



**IEEE Standard for Information Technology—
Telecommunications and Information Exchange between Systems
Local and Metropolitan Area Networks—
Specific Requirements**

**Part 11: Wireless LAN Medium Access Control
(MAC) and Physical Layer (PHY) Specifications**

Amendment 3: Wake-Up Radio Operation

IEEE Computer Society

Developed by the
LAN/MAN Standards Committee

IEEE Std 802.11ba™-2021

(Amendment to IEEE Std 802.11™-2020
as amended by IEEE Std 802.11ax™-2021
and IEEE Std 802.11ay™-2021)

IEEE Std 802.11ba™-2021

(Amendment to IEEE Std 802.11™-2020
as amendment by IEEE Std 802.11ax™-2021,
and IEEE Std 802.11ay™-2021)

**IEEE Standard for Information Technology—
Telecommunications and Information Exchange between Systems
Local and Metropolitan Area Networks—
Specific Requirements**

**Part 11: Wireless LAN Medium Access Control
(MAC) and Physical Layer (PHY) Specifications**

Amendment 3: Wake-Up Radio Operation

Developed by the

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

Approved 25 March 2021

IEEE SA Standards Board

Abstract: This amendment defines modifications to both the IEEE 802.11 physical layer (PHY) and the IEEE 802.11 medium access control (MAC) sublayer for wake-up radio operation.

Keywords: IEEE 802.11™, IEEE 802.11ba™, MAC, medium access control, PHY, physical layer, power save, wake-up radio

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

Copyright © 2021 by The Institute of Electrical and Electronics Engineers, Inc.
All rights reserved. Published 8 October 2021. Printed in the United States of America.

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

PDF: ISBN 978-1-5044-7508-2 STD24663
Print: ISBN 978-1-5044-7509-9 STDPD24663

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

Important Notices and Disclaimers Concerning IEEE Standards Documents

IEEE Standards documents are made available for use subject to important notices and legal disclaimers. These notices and disclaimers, or a reference to this page (<https://standards.ieee.org/ipr/disclaimers.html>), appear in all standards and may be found under the heading “Important Notices and Disclaimers Concerning IEEE Standards Documents.”

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

IEEE Standards documents are developed within the IEEE Societies and the Standards Coordinating Committees of the IEEE Standards Association (IEEE SA) Standards Board. IEEE develops its standards through an accredited consensus development process, which brings together volunteers representing varied viewpoints and interests to achieve the final product. IEEE Standards are documents developed by volunteers with scientific, academic, and industry-based expertise in technical working groups. Volunteers are not necessarily members of IEEE or IEEE SA, 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 makes no warranties or representations concerning its standards, and expressly disclaims all warranties, express or implied, concerning this standard, including but not limited to the warranties of merchantability, fitness for a particular purpose and non-infringement. In addition, IEEE does not warrant or represent that the use of the material contained in its standards is free from patent infringement. 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: THE NEED TO PROCURE 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 is 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, nor 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 the presenter's views should be considered the personal views of that individual rather than the formal position of IEEE, IEEE SA, the Standards Committee, or the Working Group.

Comments on standards

Comments for revision of IEEE Standards documents are welcome from any interested party, regardless of membership affiliation with IEEE or IEEE SA. However, **IEEE does not provide interpretations, 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 evaluating comments or in revisions to an IEEE standard is welcome to join the relevant IEEE working group. You can indicate interest in a working group using the Interests tab in the Manage Profile & Interests area of the [IEEE SA myProject system](#). An IEEE Account is needed to access the application.

Comments on standards should be submitted using the [Contact Us](#) form.

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 constitute 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.

Data privacy

Users of IEEE Standards documents should evaluate the standards for considerations of data privacy and data ownership in the context of assessing and using the standards in compliance with applicable laws and regulations.

Copyrights

IEEE draft and approved standards are copyrighted by IEEE under US 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 licensing fees, 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; <https://www.copyright.com/>. 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 10 years. When a document is more than 10 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 [IEEE Xplore](#) or [contact IEEE](#). For more information about the IEEE SA or IEEE's standards development process, visit the IEEE SA Website.

Errata

Errata, if any, for all IEEE standards can be accessed on the [IEEE SA Website](#). Search for standard number and year of approval to access the web page of the published standard. Errata links are located under the Additional Resources Details section. Errata are also available in [IEEE Xplore](#). Users are encouraged to periodically check for errata.

Patents

IEEE Standards are developed in compliance with the [IEEE SA Patent Policy](#).

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 <https://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.

IMPORTANT NOTICE

IEEE Standards do not guarantee or ensure safety, security, health, or environmental protection, or ensure against interference with or from other devices or networks. IEEE Standards development activities consider research and information presented to the standards development group in developing any safety recommendations. Other information about safety practices, changes in technology or technology implementation, or impact by peripheral systems also may be pertinent to safety considerations during implementation of the standard. 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.

Participants

At the time this amendment was sent to the IEEE SA Board for approval, the IEEE 802.11 Working Group had the following members:

Dorothy V. Stanley, Chair
Jon Walter Rosdahl, 1st Vice Chair
Robert Stacey, 2nd Vice Chair
Stephen McCann, Secretary

Minyoung Park, IEEE 802.11ba Task Group Chair
Yunsong Yang, IEEE 802.11ba Task Group Vice Chair
Leif Wilhelmsson, IEEE 802.11ba Task Group Secretary
Po-Kai Huang, IEEE 802.11ba Task Group Technical Editor

Tomoko Adachi	Pierre Debergh	Jia Jia
Jinsoo Ahn	Donald E. Eastlake	Jinjing Jiang
Woojin Ahn	Peter Ecclesine	Liang Jin
Kosuke Aio	Richard Edgar	Allan Jones
Carlos H. Aldana	Marc Emmelmann	Vincent Knowles Jones
Yaron Alpert	Vinko Erceg	Volker Jungnickel
Song-Haur An	Andrew Estrada	Christophe Jurczak
Carol Ansley	Ping Fang	Carl W. Kain
Lee R. Armstrong	Yonggang Fang	Naveen K. Kakani
Yusuke Asai	Xiang Feng	Dzevdan Kapetanovic
Kwok Shum S. Au	Norman Finn	Assaf Y. Kasher
Vijay Auluck	Matthew J. Fischer	Oren Kedem
Geert Awater	Michael Fischer	Richard H. Kennedy
Shahnaz Azizi	Shunsuke Fujio	Stuart J. Kerry
Robert Baeten	Sho Furuichi	Evgeny Khorov
Eugene Baik	Ming Gan	Jeongki Kim
Stephane Baron	Eduard Garcia Villegas	Jin Min Kim
Anuj Batra	Chittabrata Ghosh	Suhwook Kim
Friedbert Berens	James P. Gilb	Yongho Kim
Christian Berger	Tim Godfrey	Youhan Kim
Nehru Bhandaru	Niranjan Grandhe	Jarkko Knecht
John Buffington	Michael Grigat	Geonjung Ko
George Calcev	Qiang Guo	Fumihide Kojima
Rui Cao	Yuchen Guo	Bruce P. Kraemer
Laurent Cariou	Robert Hall	Manish Kumar
William Carney	Xiao Han	Rajesh Kumar
Ricky Chair	Thomas Handte	Massinissa Lalam
Clint F. Chaplin	Christopher J. Hansen	Zhou Lan
Jiamin Chen	Chris Hartman	Leonardo Lanante
Xiaogang Chen	Victor Hayes	James Lansford
George Cherian	Allen D. Heberling	Jae Seung S. Lee
Dmitry Cherniavsky	Ahmadreza Hedayat	Sungeun Lee
Rojan Chitrakar	Robert F. Heile	Suzanne Leicht
Hangyu Cho	Guido R. Hiertz	James Lepp
Jinsoo Choi	Duncan Ho	Joseph Levy
Liwen Chu	Hanseul Hong	Dejian Li
Jinyoung Chun	Koji Horisaki	Guoqing Li
Dana Ciochina	Chunyu Hu	Huan-Bang Li
Sean Coffey	Lei Huang	Qiang Li
Claudio Da Silva	Po-Kai Huang	Yanchun Li
Subir Das	Zhiyong Huang	Yunbo Li
Rolf J. de Vegt	Sung Hyun H. Hwang	Dong Guk Lim
	Timothy Jeffries	Yingpei Lin

Der-Zheng Liu
 Jianhan Liu
 Yong Liu
 Peter Loc
 Artyom Lomayev
 Hui-Ling Lou
 Kaiying Lv
 Lily Lv
 Jing Ma
 Narendar Madhavan
 Jouni K. Malinen
 Alexander Maltsev
 Hiroshi Mano
 Roger Marks
 Simone Merlin
 Apurva Mody
 Bibhu Mohanty
 Hitoshi Morioka
 Yuichi Morioka
 Hiroyuki Motozuka
 Robert Mueller
 Yutaka Murakami
 Andrew Myles
 Patrice Nezou
 Paul Nikolich
 Yujin Noh
 John Notor
 Minseok Oh
 Oghenekome Oteri
 Kazuyuki Ozaki
 Stephen Palm
 Eunsung Park
 Minyoung Park
 Sung-jin Park
 Glenn Parsons
 Abhishek Patil
 Hakan Persson
 James E. Petranovich
 Albert Petrick
 Rethnakaran Pulikkoonattu
 Dengyu Qiao

Demir Rakanovic
 Enrico-Henrik Rantala
 Maximilian Riegel
 Mark Rison
 Zhigang Rong
 Kiseon Ryu
 Bahareh Sadeghi
 Takenori Sakamoto
 Kazuyuki Sakoda
 Sam Sambasivan
 Hemanth Sampath
 Naotaka Sato
 Sigurd Schelstraete
 Andy Scott
 Yongho Seok
 Stephen J. Shellhammer
 Ian Sherlock
 Shimi Shilo
 Graham K. Smith
 Ju-Hyung Son
 Sudhir Srinivasa
 Adrian P. Stephens
 Noel Stott
 Jung Hoon H. Suh
 Takenori Sumi
 Bo Sun
 Chen Sun
 Li-Hsiang Sun
 Sheng Sun
 Yanjun Sun
 Dennis Sundman
 Mineo Takai
 Sagar Tamhane
 Yusuke Tanaka
 Kentaro Taniguchi
 Wu Tao
 Bin Tian
 Fei Tong
 Solomon B. Trainin
 Yoshio Urabe
 Richard D. Van Nee
 Allert Van Zelst

Lorenzo Vangelista
 Jerome Vanthournout
 Prabodh Varshney
 Ganesh Venkatesan
 Lochan Verma
 Sameer Vermani
 Pascal Viger
 George A. Vlantis
 Chao Chun Wang
 Haiming Wang
 Huizhao Wang
 James June J. Wang
 Lei Wang
 Xiaofei Wang
 Xuehuan Wang
 Lisa Ward
 Julian Webber
 Menzo M. Wentink
 Leif Wilhelmsson
 Eric Wong
 Tianyu Wu
 Yan Xin
 Qi Xue
 Rui Yang
 Xun Yang
 Yunsong Yang
 Kazuto Yano
 James Yee
 Peter Yee
 Su Khiong K. Yong
 Christopher Young
 Heejung Yu
 Jian Yu
 Mao Yu
 SunWoong Yun
 Alan Zeleznikar
 Hongyuan Zhang
 Xingxin Zhang
 Yan Zhang
 Xiayu Zheng
 Lan Zhuo

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

Tomoko Adachi	Lokesh Kabra	Robert Robinson
Thomas Alexander	Srinivas Kandala	Benjamin Rolfe
Nobumitsu Amachi	Piotr Karocki	Jon Walter Rosdahl
Amelia Andersdotter	Randy Kelsey	Kazuyuki Sakoda
Carol Ansley	Stuart J. Kerry	Shigenobu Sasaki
Butch Anton	Yongbum Kim	Naotaka Sato
Alfred Asterjadhi	Youhan Kim	James Schuessler
Kwok Shum S. Au	Yasushi Kudoh	Stephen J. Shellhammer
Geert Awater	Thomas Kurihara	Ian Sherlock
Harry Bims	George Kyle	Graham Smith
Nancy Bravin	Hyeong Ho Lee	Ju-Hyung Son
Vern Brethour	Frank Leong	Dorothy V. Stanley
Demetrio Bucaneg	James Lepp	Thomas Starai
William Byrd	Joseph Levy	Noel Stott
Paul Cardinal	Jeffery Maki	Walter Struppler
Juan Carreon	Jouni K. Malinen	Mark Sturza
Pin Chang	Kavita Mathur	Mitsutoshi Sugawara
Cheng Chen	Stephen McCann	Bo Sun
Rojan Chitrakar	Brett McClellan	David Tepen
Paul Chiuchiolo	Michael Montemurro	Solomon B. Trainin
Claudio Da Silva	Matthew Mora	Mark-Rene Uchida
Hendricus De Ruijter	Ronald Murias	Albert Van Zelst
Richard Edgar	Rick Murphy	Dmitri Varsanofiev
Alecsander Eitan	Andrew Myles	Prabodh Varshney
Marc Emmelmann	Paul Nikolich	George A. Vlantis
Yonggang Fang	Tetsu Nishimura	Lei Wang
Avraham Freedman	Robert O'Hara	Xiaofei Wang
David Goodall	Satoshi Obara	Lisa Ward
Mark Hamilton	Satoshi Oyama	Karl Webber
Jerome Henry	Minyoung Park	Hung-Yu Wei
Marco Hernandez	Bansi Patel	Menzo M. Wentink
Werner Hoelzl	Albert Petrick	Scott Willy
Klaus Hueske	David Piehler	Rui Yang
Oliver Holland	Clinton Powell	Yunsong Yang
Atsushi Ito	R. K. Rannow	Yu Yuan
Raj Jain	Ranga Reddy	Oren Yuen
SangKwon Jeong	Alon Regev	Daidi Zhong
Pranav Jha	Maximilian Riegel	Zhen Zhou

When the IEEE SA Standards Board approved this amendment on 25 March 2021, it had the following membership:

Gary Hoffman, *Chair*
Jon Walter Rosdahl, *Vice Chair*
John D. Kulick, *Past Chair*
Konstantinos Karachalios, *Secretary*

Edward A. Addy	Howard Li	Mehmet Ulema
Doug Edwards	Daozhuang Lin	Lei Wang
Ramy Ahmed Fathy	Kevin Lu	F. Keith Waters
J. Travis Griffith	Daleep C. Mohla	Karl Weber
Thomas Koshy	Chenhui Niu	Sha Wei
Joseph L. Koepfinger*	Damir Novosel	Howard Wolfman
David J. Law	Annette Reilly	Daidi Zhong
	Dorothy V. Stanley	

*Member Emeritus

Introduction

This introduction is not part of IEEE Std 802.11ba-2021, IEEE Standard for Information Technology—Telecommunications and Information Exchange Between Systems—Local and Metropolitan Area Networks—Specific Requirements—Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications—Amendment 3: Wake-Up Radio Operation.

This amendment defines modifications to both the IEEE 802.11 physical layer (PHY) and the IEEE 802.11 medium access control (MAC) sublayer for wake-up radio operation.

Contents

1.	Overview	21
1.3	Supplementary information on purpose.....	21
3.	Definitions, acronyms, and abbreviations.....	21
3.2	Definitions specific to IEEE 802.11	21
3.4	Abbreviations and acronyms	23
4.	General description	24
4.3	Components of the IEEE Std 802.11 architecture	24
4.3.15b	Wake-up radio (WUR) AP and WUR non-AP STA	24
4.5	Overview of the services.....	25
4.5.4	Access control and data confidentiality services	25
4.5.4.3	Deauthentication	25
4.5.11	Wake-up radio (WUR) services.....	25
4.10	IEEE Std 802.11 and IEEE Std 802.1X-2010	26
4.10.3	Infrastructure functional model overview.....	26
4.10.3.2	AKM operation with AS.....	26
4.10.3.3	AKM operations with a password or PSK.....	27
6.	Layer management.....	30
6.1	Overview of management model.....	30
6.2	Generic management primitives	30
6.3	MLME SAP interface	30
6.3.3	Scan.....	30
6.3.3.2	MLME-SCAN.request.....	30
6.3.3.2.2	Semantics of the service primitive.....	30
6.3.3.3	MLME-SCAN.confirm.....	30
6.3.3.3.2	Semantics of the service primitive.....	30
6.3.4	Synchronization	32
6.3.4.2	MLME-JOIN.request.....	32
6.3.4.2.2	Semantics of the service primitive.....	32
6.3.7	Associate.....	32
6.3.7.2	MLME-ASSOCIATE.request.....	32
6.3.7.2.2	Semantics of the service primitive.....	32
6.3.7.3	MLME-ASSOCIATE.confirm	33
6.3.7.3.2	Semantics of the service primitive.....	33
6.3.7.4	MLME-ASSOCIATE.indication	34
6.3.7.4.2	Semantics of the service primitive.....	34
6.3.7.5	MLME-ASSOCIATE.response	35
6.3.7.5.2	Semantics of the service primitive.....	35
6.3.8	Reassociate.....	36
6.3.8.2	MLME-REASSOCIATE.request	36
6.3.8.2.2	Semantics of the service primitive.....	36
6.3.8.3	MLME-REASSOCIATE.confirm	36
6.3.8.3.2	Semantics of the service primitive.....	36
6.3.8.4	MLME-REASSOCIATE.indication	37
6.3.8.4.2	Semantics of the service primitive.....	37

6.3.8.5	MLME-REASSOCIATE.response	38
6.3.8.5.2	Semantics of the service primitive	38
6.3.11	Start	39
6.3.11.2	MLME-START.request	39
6.3.11.2.2	Semantics of the service primitive	39
6.3.19	SetKeys	40
6.3.19.1	MLME-SETKEYS.request	40
6.3.19.1.2	Semantics of the service primitive	40
6.3.19.1.4	Effect of receipt	40
6.3.20	DeleteKeys	41
6.3.20.1	MLME-DELETEKEYS.request	41
6.3.20.1.2	Semantics of the service primitive	41
6.3.23	SetProtection	41
6.3.23.1	MLME-SETPROTECTION.request	41
6.3.23.1.2	Semantics of the service primitive	41
6.3.92	PN event report	42
6.3.92.2	MLME-PN-EXHAUSTION.indication	42
6.3.92.2.2	Semantics of the service primitive	42
6.3.92.3	MLME-PN-WARNING.indication	42
6.3.92.3.2	Semantics of the service primitive	42
6.3.123	WUR mode setup	43
6.3.123.1	General	43
6.3.123.2	MLME-WURMODESETUP.request	43
6.3.123.2.1	Function	43
6.3.123.2.2	Semantics of the service primitive	43
6.3.123.2.3	When generated	43
6.3.123.2.4	Effect of receipt	43
6.3.123.3	MLME-WURMODESETUP.confirm	43
6.3.123.3.1	Function	43
6.3.123.3.2	Semantics of the service primitive	44
6.3.123.3.3	When generated	44
6.3.123.3.4	Effect of receipt	44
6.3.123.4	MLME-WURMODESETUP.indication	44
6.3.123.4.1	Function	44
6.3.123.4.2	Semantics of the service primitive	45
6.3.123.4.3	When generated	45
6.3.123.4.4	Effect of receipt	45
6.3.123.5	MLME-WURMODESETUP.response	45
6.3.123.5.1	Function	45
6.3.123.5.2	Semantics of the service primitive	45
6.3.123.5.3	When generated	46
6.3.123.5.4	Effect of receipt	46
6.3.124	WUR mode teardown	46
6.3.124.1	General	46
6.3.124.2	MLME-WURMODETEARDOWN.request	46
6.3.124.2.1	Function	46
6.3.124.2.2	Semantics of the service primitive	47
6.3.124.2.3	When generated	47
6.3.124.2.4	Effect of receipt	47
6.3.124.3	MLME-WURMODETEARDOWN.indication	47
6.3.124.3.1	Function	47
6.3.124.3.2	Semantics of the service primitive	47
6.3.124.3.3	When generated	47
6.3.124.3.4	Effect of receipt	48

6.3.125	WUR Discovery.....	48
6.3.125.1	General.....	48
6.3.125.2	MLME-WURDISCOVERY.request	48
6.3.125.2.1	Function	48
6.3.125.2.2	Semantics of the service primitive.....	48
6.3.125.2.3	When generated	49
6.3.125.2.4	Effect of receipt	49
6.3.125.3	MLME-WURDISCOVERY.confirm	49
6.3.125.3.1	Function	49
6.3.125.3.2	Semantics of the service primitive.....	49
6.3.125.3.3	When generated	50
6.3.125.4	Effect of receipt	50
9.	Frame formats	51
9.2.3	General frame format.....	51
9.3	Format of individual frame types.....	51
9.3.3	(PVO) Management frames	51
9.3.3.2	Beacon frame format	51
9.3.3.5	Association Request frame format.....	52
9.3.3.6	Association Response frame format	52
9.3.3.7	Reassociation Request frame format	53
9.3.3.8	Reassociation Response frame format.....	53
9.3.3.9	Probe Request frame format	53
9.3.3.10	Probe Response frame format.....	54
9.4	Management and Extension frame body components	54
9.4.1	Fields that are not elements	54
9.4.1.11	Action field	54
9.4.2	Elements.....	55
9.4.2.1	General.....	55
9.4.2.24	RSNE	55
9.4.2.24.2	Cipher suites	55
9.4.2.47	Fast BSS Transition element (FTE).....	55
9.4.2.79	TFS Request element	56
9.4.2.241	RSN Extension element (RSNXE)	57
9.4.2.291	WUR Capabilities element	57
9.4.2.292	WUR Operation element	60
9.4.2.293	WUR Mode element	62
9.4.2.294	WUR Discovery element	67
9.4.2.295	WUR PN Update element.....	69
9.6	Action frame format details	69
9.6.33	WUR Action details.....	70
9.6.33.1	WUR Action field.....	70
9.6.33.2	WUR Mode Setup frame format.....	70
9.6.33.3	WUR Mode Teardown frame format.....	71
9.6.33.4	WUR Wake-up Indication frame format	71
9.9	MAC frame format for WUR frames	72
9.9.1	Basic components	72
9.9.2	General WUR frame format	72
9.9.2.1	General.....	72
9.9.2.2	MAC header.....	73
9.9.2.2.1	Frame Control field.....	73
9.9.2.2.2	ID field.....	74
9.9.2.2.3	Type Dependent Control field	74

9.9.2.3	Frame Body field	74
9.9.2.4	Frame Check Sequence (FCS) field.....	75
9.9.2.4.1	General.....	75
9.9.2.4.2	Cyclic Redundancy Check (CRC) for WUR frames	75
9.9.3	Format of individual WUR frame types	76
9.9.3.1	WUR Beacon frame format	76
9.9.3.2	WUR Wake-up frame format	76
9.9.3.3	WUR Discovery frame format.....	78
9.9.3.4	WUR Vendor Specific frame format	79
9.9.3.5	WUR Short Wake-up frame format.....	79
10.	MAC sublayer functional description.....	81
10.2	MAC architecture	81
10.2.1	General.....	81
11.	MLME	82
11.2	Power management.....	82
11.2.1	General.....	82
11.3	STA authentication and association.....	82
11.3.3	Frame filtering based on STA state	82
11.3.4	Authentication and deauthentication	82
11.3.4.4	Deauthentication-originating STA.....	82
11.3.4.5	Deauthentication-destination STA.....	82
11.3.5	Association, reassociation, and disassociation	83
11.3.5.2	Non-AP and non-PCP STA association initiation procedures.....	83
11.3.5.3	AP or PCP association receipt procedures.....	83
11.3.5.4	Non-AP and non-PCP STA reassociation initiation procedures	83
11.3.5.5	AP or PCP reassociation receipt procedures.....	83
11.3.5.6	Non-AP and non-PCP STA disassociation initiation procedures.....	83
11.3.5.7	Non-AP and non-PCP STA disassociation receipt procedures	83
11.3.5.8	AP or PCP disassociation initiation procedure	84
11.3.5.9	AP or PCP disassociation receipt procedure.....	84
12.	Security	85
12.2	Framework	85
12.2.4	RSNA establishment.....	85
12.5	RSNA confidentiality and integrity protocols	85
12.5.1	Overview.....	85
12.5.4	Broadcast/multicast integrity protocol (BIP).....	85
12.5.4.1	BIP overview	85
12.6	RSNA security association management.....	86
12.6.1	Security associations.....	86
12.6.1.1	Security association definitions	86
12.6.1.1.1	General.....	86
12.6.1.1.6	PTKSA.....	86
12.6.1.1.1a	WIGTKSA	87
12.6.1.3	Security association life cycle.....	87
12.6.1.3.2	Security association in an ESS.....	87
12.6.2	RSNA selection.....	87
12.6.3	RSNA policy selection in an infrastructure BSS	87
12.6.14	RSNA key management in an infrastructure BSS	88

12.6.18	RSNA security association termination.....	88
12.6.21	RSNA rekeying.....	88
12.7	Keys and key distribution.....	88
12.7.1	Key hierarchy.....	88
12.7.1.1	General.....	88
12.7.1.3	Pairwise key hierarchy.....	89
12.7.1.6	FT key hierarchy.....	90
12.7.1.6.5	PTK.....	90
12.7.1.7a	Wake-up radio integrity group temporal key (WIGTK) hierarchy.....	91
12.7.2	EAPOL-Key frames.....	92
12.7.4	EAPOL-KEY frame notation.....	92
12.7.6	4-way handshake.....	92
12.7.6.1	General.....	92
12.7.6.2	4-way handshake message 1.....	92
12.7.6.4	4-way handshake message 3.....	93
12.7.6.5	4-way handshake message 4.....	93
12.7.6.6	4-way handshake implementation considerations.....	93
12.7.7	Group key handshake.....	94
12.7.7.1	General.....	94
12.7.7.2	Group key handshake message 1.....	94
12.7.7.4	Group key handshake implementation considerations.....	94
12.7.9.4	Supplicant state machine procedures.....	95
12.8	Mapping EAPOL keys to IEEE 802.11 keys.....	95
12.8.10a	Mapping WTK to BIP key.....	95
12.8.10b	Mapping WIGTK to BIP key.....	95
12.11	Authentication for FILS.....	95
12.11.2	FILS authentication protocol.....	95
12.11.2.1	General.....	95
12.11.2.5.3	PTKSA Key derivation with FILS authentication.....	95
12.11.2.6	Key confirmation with FILS authentication.....	97
12.11.2.6.3	(Re)Association Response for FILS key confirmation.....	97
13.	Fast BSS transition.....	98
13.2	Key holders.....	98
13.2.2	Authenticator key holders.....	98
13.2.3	Supplicant key holders.....	98
13.4	FT initial mobility domain association.....	98
13.4.2	FT initial mobility domain association in an RSN.....	98
13.5	FT protocol.....	99
13.5.1	Overview.....	99
13.6	FT resource request protocol.....	99
13.6.2	Over-the-air fast BSS transition with resource request.....	99
13.6.3	Over-the-DS fast BSS transition with resource request.....	99
13.7	FT reassociation.....	99
13.7.1	FT reassociation in an RSN.....	99
13.8	FT authentication sequence.....	99
13.8.5	FT authentication sequence: contents of fourth message.....	99
29.	Wake-Up Radio (WUR) MAC specification.....	101
29.1	Introduction.....	101
29.2	WUR channel, WUR primary channel, and WUR discovery channel.....	101
29.3	Channel access.....	102

29.4	Discarding a WUR frame	102
29.5	Setting the identifiers of WUR frames	103
29.5.1	General.....	103
29.5.2	Compressed BSSID	103
29.5.3	Transmitter ID.....	103
29.5.4	WUR Group ID.....	104
29.5.5	WUR ID	104
29.5.6	Nontransmitter ID	105
29.6	Synchronization using WUR Beacon frame	105
29.6.1	General.....	105
29.6.2	WUR Beacon frame generation	105
29.6.3	Maintaining TSF timer synchronization with WUR Beacon frame	107
29.7	WUR duty cycle operation	107
29.8	WUR power management procedure.....	109
29.8.1	General.....	109
29.8.2	WUR mode setup	110
29.8.3	WUR power management operation for a WUR AP.....	113
29.8.4	WUR power management operation for a WUR non-AP STA	114
29.9	Wake-up operation.....	115
29.9.1	General.....	115
29.9.2	WUR Short Wake-up frame operation	116
29.9.3	WUR AP operation.....	117
29.9.4	WUR non-AP STA operation	119
29.10	WUR frame protection.....	119
29.10.1	General.....	119
29.10.2	Protected WUR frame transmission	121
29.10.3	Protected WUR frame reception.....	122
29.10.4	Generation and construction of PN for WUR frames	123
29.10.4.1	Generation of the PN by a WUR AP	123
29.10.4.2	Construction of the PN by a WUR non-AP STA	124
29.10.4.3	WUR PN update procedure	125
29.11	WUR FDMA operation	125
29.11.1	WUR FDMA channel access	126
29.12	WUR discovery.....	127
30.	Wake-Up Radio (WUR) PHY specification	129
30.1	Introduction.....	129
30.2	WUR PHY service interface.....	130
30.2.1	Introduction.....	130
30.2.2	TXVECTOR and RXVECTOR parameters	130
30.2.3	PHY-CONFIG_VECTOR parameters.....	133
30.3	WUR PHY	134
30.3.1	Introduction.....	134
30.3.2	WUR Basic PPDU format	134
30.3.3	WUR FDMA PPDU format.....	135
30.3.4	Transmitter block diagram.....	135
30.3.4.1	WUR Basic PPDU waveform generation for WUR-Sync field and WUR-Data field with WUR HDR	137
30.3.4.2	WUR Basic PPDU waveform generation for WUR-Data field with WUR LDR	138
30.3.4.3	WUR FDMA PPDU WUR-Data field waveform generation.....	139
30.3.4.4	Symbol Randomizer and Per-transmit chain Cyclic Shift	139
30.3.5	Overview of the PPDU encoding process.....	140

30.3.5.1	General.....	140
30.3.5.2	Construction of the L-STF	140
30.3.5.3	Construction of the L-LTF	140
30.3.5.4	Construction of the L-SIG	141
30.3.5.5	Construction of the BPSK-Mark1.....	141
30.3.5.6	Construction of the BPSK-Mark2.....	142
30.3.5.7	Construction of the WUR-Sync for a single 20 MHz channel	142
30.3.5.8	Construction of the WUR-Data for a single 20 MHz channel.....	142
30.3.5.9	Construction of the WUR-Sync and WUR-Data for the FDMA transmission	143
30.3.6	WUR data rates	143
30.3.7	Timing related parameters	143
30.3.8	Mathematical description of signals	145
30.3.9	WUR preamble	148
30.3.9.1	Introduction.....	148
30.3.9.2	Non-WUR portion of WUR PHY preamble.....	149
30.3.9.2.1	L-STF Definition	149
30.3.9.2.2	L-LTF Definition	149
30.3.9.2.3	L-SIG Definition.....	150
30.3.9.2.4	BPSK-Mark1 Definition.....	151
30.3.9.2.5	BPSK-Mark2 Definition.....	151
30.3.9.3	WUR-Sync field	152
30.3.9.3.1	Introduction.....	152
30.3.9.3.2	Cyclic Shift for WUR-Sync field.....	152
30.3.9.3.3	WUR-Sync field for WUR LDR	152
30.3.9.3.4	WUR-Sync field for WUR HDR	152
30.3.10	WUR-Data field.....	152
30.3.10.1	Cyclic Shift for WUR-Data field	152
30.3.10.2	WUR-Data field for WUR LDR and WUR HDR	153
30.3.11	WUR Padding field for a WUR FDMA PPDU	153
30.3.12	WUR transmit specification.....	154
30.3.12.1	Transmit spectrum mask	154
30.3.12.2	Spectral flatness	157
30.3.12.3	Transmit center frequency and symbol clock frequency tolerance	157
30.3.12.4	Transmit On and Off Symbols power ratio	157
30.3.12.5	Correlation test on MC-OOK symbols	157
30.3.13	WUR receiver specification.....	158
30.3.13.1	Receiver minimum input sensitivity	158
30.3.13.2	Adjacent channel rejection.....	158
30.3.13.3	Nonadjacent channel rejection.....	158
30.3.13.4	Receiver maximum input level	159
30.3.13.5	CCA sensitivity.....	159
30.3.14	WUR transmit procedure	159
30.3.15	WUR receive procedure.....	162
30.4	WUR PLME	165
30.4.1	TXTIME and PSDU length calculation.....	165
30.4.2	Table of time and length characteristics	166
30.5	Parameters for WUR Data Rates	166
Annex B (normative) Protocol Implementation Conformance Statement (PICS) proforma.....		167
Annex C (normative) ASN.1 encoding of the MAC and PHY MIB.....		171
Annex AC (informative) Examples of WUR MC-OOK Symbol Design and CSD Design.....		176

Tables

Table 9-32—Beacon frame body	51
Table 9-34—Association Request frame body	52
Table 9-35—Association Response frame body	52
Table 9-36—Reassociation Request frame body	53
Table 9-37—Reassociation Response frame body	53
Table 9-38—Probe Request frame body	53
Table 9-39—Probe Response frame body	54
Table 9-51—Category values	54
Table 9-92—Element IDs	55
Table 9-222—TFS Action Code field values	56
Table 9-321—Extended RSN Capabilities field	57
Table 9-322af—Subfields of the WUR Capabilities Information field	59
Table 9-322ag—Action Type definitions	62
Table 9-322ah—WUR Mode Response Status Definition	63
Table 9-322ai—Subfields of WUR Parameters field from WUR AP	64
Table 9-322aj—WUR Channel Offset subfield encoding	65
Table 9-322ak—Subfields of the WUR Parameters field from WUR non-AP STA	66
Table 9-526h—WUR Action field values	70
Table 9-526i—WUR Mode Setup frame Action field format	70
Table 9-526j—WUR Mode Teardown frame Action field format	71
Table 9-526k—WUR Wake-up Indication frame Action field format	71
Table 9-526l—WUR Wake-up Indication field values	72
Table 9-539a—WUR frame types	73
Table 9-539b—Identifiers of WUR frames	74
Table 29-1—Settings for WUR mode setup frame exchange - Request and Response	110
Table 29-2—WUR Mode Setup frame or WUR Mode Teardown frame transmission	111
Table 30-1—TXVECTOR and RXVECTOR parameters	131
Table 30-2—Fields of the WUR Basic PPDU	134
Table 30-3—Timing-related constants	144
Table 30-4—Frequently used parameters	144
Table 30-5—Field specific parameter values for the MC-OOK symbols in WUR-Sync and WUR-Data fields	147
Table 30-6—Values of pseudorandom cyclic shift with cyclic shift index n for the WUR-Sync field and WUR-Data field with WUR HDR	147
Table 30-7—Values of pseudorandom cyclic shift with cyclic shift index n for the WUR-Data field with WUR LDR	148
Table 30-8—The states of the LFSR, the values of the bits b_2 , b_1 , b_0 , the value of n , and the pseudorandom cyclic shift with cyclic shift index n for the first seven MC-OOK symbols in the WUR-Sync field	148
Table 30-9—WUR encoded bits for WUR LDR	153
Table 30-10—WUR encoded bits for WUR HDR	153
Table 30-11—Receiver minimum input level sensitivity	158
Table 30-12—Minimum required adjacent and nonadjacent channel rejection levels	158
Table 30-13—WUR PPDU Time and Length Characteristics	166
Table 30-14—WUR PPDU data rates	166
Table AC-1—Example Values for the Sequence S^{HDR} used for the Construction of the 2 μs duration MC-OOK On Symbol	176
Table AC-2—Example Values for the Sequence S^{LDR} used for the Construction of the 4 μs duration MC-OOK On Symbol	177
Table AC-3—Recommended CSD values for the WUR-Sync field and WUR-Data field with WUR HDR	178
Table AC-4—Recommended CSD values for the WUR-Data field with WUR LDR	179

Figures

Figure 4-32—Establishing pairwise and group keys	28
Figure 4-33—Delivery of subsequent group keys	29
Figure 9-363a—WIGTK subelement format.....	56
Figure 9-788dm—WUR Capabilities element format.....	57
Figure 9-788dn—Supported Bands field format	58
Figure 9-788do—WUR Capabilities Information field format	58
Figure 9-788dp—WUR Operation element format.....	60
Figure 9-788dq—WUR Operation Parameters field format.....	61
Figure 9-788dr—WUR Mode element format	62
Figure 9-788ds—WUR Parameters Control field format.....	63
Figure 9-788dt—WUR Parameters field format from WUR AP	64
Figure 9-788du—WUR Group ID List subfield format	65
Figure 9-788dv—WUR Parameters field format from WUR non-AP STA	66
Figure 9-788dw—Proposed WUR Parameters subfield format	66
Figure 9-788dx—WUR Discovery element format.....	67
Figure 9-788dy—WUR AP Information subfield format.....	67
Figure 9-788dz—WUR AP Parameters subfield format	68
Figure 9-788ea—WUR AP Parameters Control field format.....	68
Figure 9-788eb—WUR PN Update element format.....	69
Figure 9-788ec—Key Info field format.....	69
Figure 9-788ed—PN field format.....	69
Figure 9-993a—WUR frame format.....	72
Figure 9-993b—MAC header field format of the WUR frame	73
Figure 9-993c—Frame Control field format of WUR frame	73
Figure 9-993d—CRC-16 implementation for WUR frames	76
Figure 9-993e—Type Dependent Control field of WUR Wake-up frame	77
Figure 9-993f—Miscellaneous subfield format.....	78
Figure 9-993g—STA Info field format	78
Figure 9-993h—Frame Body Field format of WUR Discovery frame	79
Figure 9-993i—WUR Short Wake-up frame format.....	79
Figure 10-1—Non-DMG non-CMMG non-S1G STA MAC architecture	81
Figure 12-30—Pairwise key hierarchy	89
Figure 12-47a—WIGTK KDE	92
Figure 29-1—State transition diagram of WUR power state of a WUR non-AP STA in WUR mode.....	108
Figure 29-2—WUR Duty Cycle	108
Figure 29-3—AAD construction for WUR frames	121
Figure 30-1—WUR Basic PPDU format.....	134
Figure 30-2—An example of a WUR FDMA PPDU for 40 MHz channel widths.....	135
Figure 30-3—An example of a WUR FDMA PPDU for 80 MHz channel widths.....	135
Figure 30-4—An example of a WUR signal generator for the WUR-Sync field.....	136
Figure 30-5—An example of a WUR signal generator for the WUR-Data field.....	136
Figure 30-6—An example of an On-WG for the WUR-Sync and WUR-Data fields with WUR HDR	137
Figure 30-7—An example of an On-WG for the WUR-Data fields with WUR LDR	138
Figure 30-8—An example of a WUR-Data field signal generator for the FDMA transmission.....	139
Figure 30-9—Symbol Randomizer.....	140
Figure 30-10—Timing boundaries for the WUR Basic PPDU Fields.....	145
Figure 30-11—Transmit spectrum mask for WUR-Sync and WUR-Data fields of WUR Basic PPDU transmission	155
Figure 30-12—Transmit spectrum mask for WUR-Sync and WUR-Data fields of 40 MHz WUR FDMA PPDU transmission.....	156
Figure 30-13—Transmit spectrum mask for WUR-Sync and WUR-Data fields of 80 MHz WUR FDMA PPDU transmission.....	156

Figure 30-14—PHY transmit procedure for a WUR Basic PPDU 160

Figure 30-15—PHY transmit procedure for a WUR FDMA PPDU 160

Figure 30-16—PHY transmit state machine..... 162

Figure 30-17—PHY receiver procedure for WUR Basic PPDU 163

Figure 30-18—PHY receive state machine 164

**IEEE Standard for Information Technology—
Telecommunications and Information Exchange between Systems
Local and Metropolitan Area Networks—
Specific Requirements**

**Part 11: Wireless LAN Medium Access Control
(MAC) and Physical Layer (PHY) Specifications**

Amendment 3: Wake-Up Radio Operation

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. Editorial 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. Overview

1.3 Supplementary information on purpose

Insert the following to the end of the list:

Specifically, in the context of IEEE 802.11™-compliant devices, this standard

....

- Defines mechanisms to enable delivery of preassociation service discovery information to IEEE 802.11 stations (STAs).
- Defines a mechanism to enable IEEE 802.11 STAs to operate at extremely low power consumption and to react to incoming traffic with low latency through a wake-up signal.

3. Definitions, acronyms, and abbreviations

3.2 Definitions specific to IEEE 802.11

Insert the following definitions maintaining alphabetical order:

broadcast wake-up radio (WUR) wake-up frame: A WUR Wake-up frame with the ID field set to transmitter identifier (ID) or nontransmitter ID.

compressed basic service set identifier (BSSID): A 32-bit Basic Service Set (BSS) identifier derived from a BSSID or a transmitted BSSID as defined in 29.5.2.

group addressed wake-up radio (WUR) wake-up frame: A WUR Wake-up frame with the ID field set to group identifier (ID).

transmitter identifier (ID): An identifier that identifies a wake-up radio (WUR) access point (AP) and used in broadcast WUR frames that are addressed to all WUR non-AP stations (STAs) associated with the WUR AP when multiple BSSID operation is not supported or that are addressed to all WUR non-AP STAs associated with the transmitted basic service set identifier (BSSID) of a multiple BSSID set when multiple BSSID operation is supported or that are addressed to all WUR non-AP STAs that intend to discover or synchronize with the WUR AP.

multicarrier on-off keying (MC-OOK) symbol: A MC-OOK symbol is either an MC-OOK On Symbol where the multicarrier signal is present or an MC-OOK Off Symbol where no signal is present.

multicarrier signal: A multicarrier signal is a signal that is constructed with multiple subcarriers that carry energy.

identifier (ID): An identifier used by a wake-up radio (WUR) access point (AP) to identify broadcast WUR frames that are addressed to all WUR non-AP stations (STAs) associated with an AP corresponding to a nontransmitted basic service set identifier (BSSID) from the multiple BSSID set when multiple BSSID operation is supported.

wake-up radio (WUR) basic physical layer (PHY) protocol data unit (PPDU): A PPDU transmitted with the TXVECTOR parameter FORMAT equal to WUR_BASIC and TXVECTOR parameter CH_BANDWIDTH equal to WUR_CBW_20.

wake-up radio (WUR) channel: A channel in which a WUR access point (AP) transmits WUR Short Wake-up frames, WUR Wake-up frames, and WUR Vendor Specific frames.

wake-up radio (WUR) discovery channel: The channel used by a WUR access point (AP) to transmit WUR Discovery frames.

wake-up radio (WUR) duty cycle period: The interval between the starting time of two successive WUR duty cycle service periods.

wake-up radio (WUR) duty cycle service period: A period of time of an established WUR duty cycle operation between a WUR access point (AP) and a WUR non-AP station (STA) during which one or more WUR frames can be transmitted to the WUR non-AP STA from the WUR AP.

wake-up radio (WUR) 80 MHz channel: The 80 MHz channel that is used to transmit 80 MHz WUR Frequency Division Multiple Access (FDMA) physical layer (PHY) protocol data units (PPDUs).

wake-up radio (WUR) frequency division multiple access (FDMA) physical layer (PHY) protocol data unit (PPDU): A PPDU transmitted with the TXVECTOR parameter FORMAT equal to WUR_FDMA and TXVECTOR parameter CH_BANDWIDTH equal to WUR_CBW_40 or WUR_CBW_80 or WUR_CBW_PUNC80-PRI or WUR_CBW_PUNC80-SEC or WUR_CBW_PUNC80-PRI-SEC-1 or WUR_CBW_PUNC80-PRI-SEC-2.

wake-up radio (WUR) integrity group temporal key (WIGTK): A random value, assigned by a WUR access point (AP) that is used to protect broadcast and group addressed WUR frames from that AP.

wake-up radio (WUR) mode: A negotiation status between a WUR access point (AP) and a WUR non-AP station (STA) in which the WUR power state of the WUR non-AP STA in power save mode alternates between the WUR awake state and the WUR doze state or stays in the WUR awake state based on the negotiated WUR parameters.

wake-up radio (WUR) primary channel: The channel used by a WUR access point (AP) to transmit WUR Beacon frames.

wake-up radio (WUR) primary 40 MHz channel: The 40 MHz channel that is used to transmit 40 MHz WUR Frequency Division Multiple Access (FDMA) physical layer (PHY) protocol data units (PPDUs).

wake-up radio (WUR) scanning: The process of scanning WUR discovery channels for WUR Discovery frames.

wake-up radio (WUR) secondary channel: The 20 MHz channel adjacent to the WUR primary channel that together form the WUR primary 40 MHz channel.

wake-up radio (WUR) secondary 40 MHz channel: The 40 MHz channel adjacent to the WUR primary 40 MHz channel that together form the WUR 80 MHz channel.

wake-up radio (WUR) temporal key (WTK): A temporal key used to protect individually addressed WUR Wake-up frames.

3.4 Abbreviations and acronyms

Insert the following acronym definitions (maintaining alphabetical order):

FDMA	frequency division multiple access
FL	fixed-length
HDR	high data rate
KDK	key derivation key
LDR	low data rate
MC-OOK	multicarrier on-off keying
PPN	partial packet number
VL	variable-length
WIGTK	wake-up radio integrity group temporal key
WIGTKSA	wake-up radio integrity group temporal key security association
WIPN	wake-up radio IGTK packet number
WTK	wake-up radio temporal key
WTPN	wake-up radio TK packet number
WUR	wake-up radio

4. General description

4.3 Components of the IEEE Std 802.11 architecture

Insert a new subclause after subclause 4.3.15 as follows

4.3.15b Wake-up radio (WUR) AP and WUR non-AP STA

A WUR non-AP STA is a non-HT, HT, VHT, or HE non-AP STA that is capable of receiving WUR PPDU and supports the WUR operation. A WUR non-AP STA has a capability to receive a WUR PPDU at a power consumption of less than 1 milliwatt.

A WUR AP is a non-HT, HT, VHT, or HE AP that is capable of transmitting WUR PPDU and supports the WUR operation.

A WUR Basic PPDU carries a WUR frame. A WUR FDMA PPDU carries more than one WUR frame. A WUR AP transmits a WUR PPDU to an intended recipient WUR non-AP STA or multiple intended recipient WUR non-AP STAs. There are five types of WUR frames that provide the following functions:

- WUR Beacon frames are transmitted by a WUR AP and used by a WUR non-AP STA to maintain timing synchronization to support the WUR duty cycle operation.
- WUR Wake-up frames provide notification to one or more WUR non-AP STA(s) that a WUR AP has buffered data and/or critical update of BSS parameters for the WUR non-AP STA(s), which enables the WUR non-AP STAs to remain in power save when there is no data to receive and enables the WUR non-AP STAs to react promptly to incoming traffic and critical update of BSS parameters.
- WUR Short Wake-up frames are shortened version of the WUR Wake-up frames.
- WUR Discovery frames support the discovery of WUR APs by a WUR non-AP STA at low power consumption.
- WUR Vendor Specific frames support vendor specific operations.

WUR PPDU are either WUR Basic PPDU or WUR FDMA PPDU. The transmission and reception of WUR PPDU is defined for the 2.4 GHz and 5 GHz bands. The transmission of 40 MHz WUR FDMA PPDU is defined for the 2.4 GHz and 5 GHz bands and the transmission of 80 MHz WUR FDMA PPDU is defined for the 5 GHz band.

The details of the WUR power management procedure are defined in 29.8.

A WUR AP has the following mandatory main features:

- Transmission of a WUR Basic PPDU on a 20 MHz channel at low data rate (LDR).
- Transmission of a WUR Basic PPDU on a 20 MHz channel at high data rate (HDR).
- Support of the WUR power management procedure.
- Support of the WUR wake-up operation.
- Support of the WUR duty cycle operation.
- Transmission of an individually addressed fixed-length (FL) WUR Wake-up frame.
- Transmission of a broadcast FL WUR Wake-up frame.
- WUR Beacon frame generation.

A WUR AP has the following optional main features:

- Transmission of a WUR FDMA PPDU on a 40 MHz or 80 MHz channel.
- Transmission of a variable-length (VL) WUR frame.
- Support for WUR frame protection.
- Transmission of a WUR Wake-up frame with a WUR group ID.
- Transmission of a WUR Short Wake-up frame.
- Support for WUR Discovery.

A WUR non-AP STA has the following mandatory main features:

- Reception of a WUR Basic PPDU on a 20 MHz channel at LDR.
- Support of the WUR power management procedure.
- Support of the WUR wake-up operation.
- Reception of an individually addressed FL WUR Wake-up frame.
- Reception of a broadcast FL WUR Wake-up frame.
- Synchronization using WUR Beacon frame.

A WUR non-AP STA has the following optional main features:

- Reception of a WUR Basic PPDU on a 20 MHz channel at HDR.
- Support of the WUR FDMA operation (see 29.11).
- Support of the WUR duty cycle operation (see 29.7).
- Reception of a VL WUR frame.
- Support for WUR frame protection.
- Reception of a WUR Wake-up frame with a WUR group ID.
- Reception of a WUR Short Wake-up frame.
- Support for WUR Discovery.

4.5 Overview of the services

4.5.4 Access control and data confidentiality services

4.5.4.3 Deauthentication

Change the 4th paragraphs as follows:

In an RSNA, deauthentication also deletes any related pairwise transient key security association (PTKSA), group temporal key security association (GTKSA), TPK security association (TPKSA), integrity group temporal key security association (IGTKSA)), beacon integrity group temporal key security association (BIGTKSA), wake-up radio integrity group temporal key security association (WIGTKSA), mesh GTKSA, and mesh TKSA that exist in the STA and closes the associated IEEE 802.1X Controlled Port, if used for this association. If pairwise master key security association (PMKSA) caching is not enabled, deauthentication also deletes the PMKSA or mesh PMKSA.

4.5.11 Wake-up radio (WUR) services

The WUR service allows non-AP STAs to have access to basic services provided by a BSS while operating at very low power. The basic WUR services that the BSS might provide to non-AP STAs include discovery, synchronization, and wake up instructions (scheduled or unscheduled).

4.10 IEEE Std 802.11 and IEEE Std 802.1X-2010

4.10.3 Infrastructure functional model overview

4.10.3.2 AKM operation with AS

Change the 2nd paragraphs as follows:

A 4-way handshake or FT 4-way handshake utilizing EAPOL-Key frames is initiated by the Authenticator to do the following:

- Confirm that a live peer holds the PMK.
- Confirm that the PMK is current.
- In the case of fast BSS transition, derive PMK-R0s and PMK-R1s.
- Derive a fresh pairwise transient key (PTK) from the PMK or, in the case of fast BSS transition, from the PMK-R1, the derived PTK including the key derivation key (KDK) if WUR frame protection is negotiated.
- If WUR frame protection is negotiated, derive a fresh WTK from the KDK.
- Install the pairwise encryption and integrity keys, and if WUR frame protection is negotiated, the WTK.
- Transport the group temporal key (GTK) and GTK sequence number from Authenticator to Supplicant and install the GTK and GTK sequence number in the STA and, if not already installed, in the AP.
- If management frame protection is negotiated, transport the IGTK and the IGTK packet number (IPN) from the Authenticator to the Supplicant and install these values in the STA and, if not already installed, in the AP.
- If beacon protection is enabled, transport the BIGTK and the BIGTK packet number (BIPN) from the Authenticator to the Supplicant and install these values in the STA and, if not already installed, in the AP.
- If WUR frame protection is negotiated, transport the wake-up radio integrity group temporal key (WIGTK) and the WIGTK packet number (WIPN) from the Authenticator to the Supplicant and install these values in the STA and, if not already installed, in the AP.
- Verify that the RSN capabilities negotiated are valid as defined in 9.4.2.24.4.
- Confirm the cipher suite selection.

Change the 3rd paragraphs as follows:

Installing the PTK, and where applicable the GTK and, if management frame protection is negotiated, the IGTK, causes the MAC to encrypt and decrypt all subsequent MSDUs irrespective of their path through the controlled or uncontrolled ports. Installing the WTK when WUR frame protection is negotiated also causes the MAC to integrity protect subsequent individually addressed WUR Wake-up frames at the AP or to validate subsequent individually addressed WUR Wake-up frames at the non-AP STA. Installing the BIGTK when beacon protection is enabled causes the MAC to integrity protect at the AP or validate subsequent Beacon frames at the non-AP STA. Installing the WIGTK when WUR frame protection is negotiated causes the MAC to integrity protect subsequent broadcast or group addressed WUR Wake-up frames at the AP or to validate subsequent broadcast or group addressed WUR Wake-up frames at the non-AP STA.

Change the 6th paragraphs as follows:

When management frame protection is negotiated, the Authenticator also uses the group key handshake with all associated STAs to change the IGTK, ~~and~~ BIGTK if beacon protection is enabled, and WIGTK if WUR

frame protection is negotiated. The Authenticator encrypts the GTK, IGTK, ~~and~~ BIGTK, and WIGTK values in the EAPOL-Key frame as described in 12.7.

4.10.3.3 AKM operations with a password or PSK

Change the 1st paragraphs as follows:

The following AKM operations are carried out when authentication is accomplished using a Password or PSK:

- A STA discovers the AP's security policy through passively monitoring the Beacon frames or through active probing. After discovery the STA performs SAE authentication using Authentication frames with the AP (see Figure 4-34).
- Upon the successful conclusion of SAE, both the STA and AP generate a PMK. The STA then associates to an AP and negotiates security policy. The AKM in the Association Request and Response frames is confirmed to be the AKM of SAE or of fast BSS transition.
- The PMK generated by SAE is used in a 4-way handshake using EAPOL-Key frames, just as with IEEE 802.1X authentication when an AS is present. See Figure 4-32.
- The GTK and GTK sequence number are sent from the Authenticator to the Supplicant just as in the AS case. See Figure 4-32 and Figure 4-33.
- If WUR frame protection is negotiated, the WIGTK and WIPN are sent from the Authenticator to the Supplicant just as in the AS case. See Figure 4-32 and Figure 4-33.

Replace Figure 4-32—Establishing pairwise and group keys with the following:

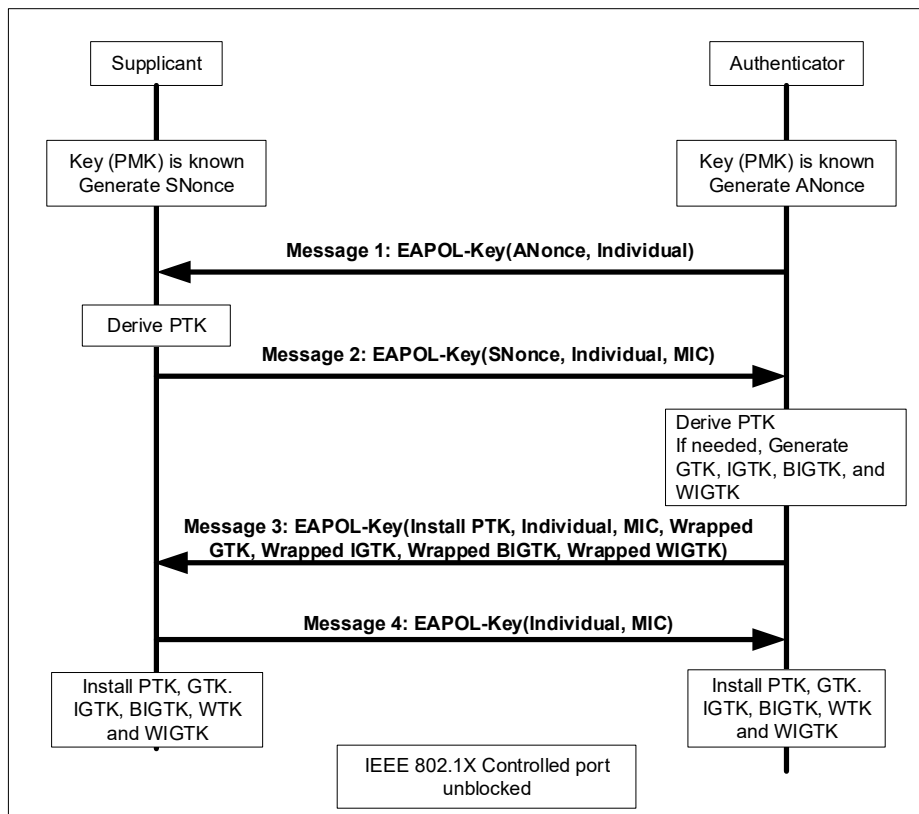


Figure 4-32—Establishing pairwise and group keys

Replace Figure 4-33—Delivery of subsequent group keys with the following:

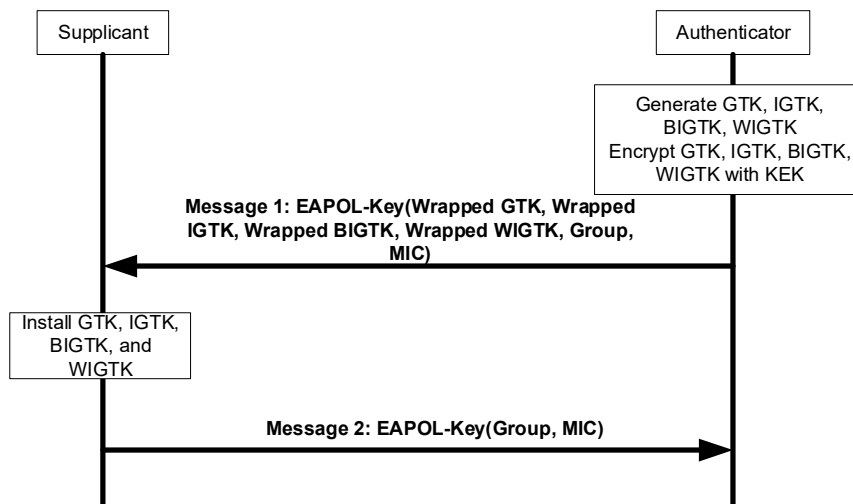


Figure 4-33—Delivery of subsequent group keys

6. Layer management

6.1 Overview of management model

6.2 Generic management primitives

6.3 MLME SAP interface

6.3.3 Scan

6.3.3.2 MLME-SCAN.request

6.3.3.2.2 Semantics of the service primitive

Change the primitive parameters as follows (not all existing parameters in the baseline are shown):

The primitive parameters are as follows:

```
MLME-SCAN.request(
    ...
    WUR Capabilities,
    VendorSpecificInfo
)
```

Insert the following entry into the unnumbered table in this subclause maintaining the primitive order above:

Name	Type	Valid range	Description
WUR Capabilities	As defined in WUR Capabilities element	As defined in 9.4.2.291	Specifies the parameters within the WUR Capabilities element that are supported by the STA. The parameter is present if dot11WUROptionImplemented is true and ScanType = ACTIVE; otherwise, this parameter is not present.

6.3.3.3 MLME-SCAN.confirm

6.3.3.3.2 Semantics of the service primitive

Insert the following rows at the end of the table that lists the BSSDescription parameters:

Name	Type	Valid range	Description	IBSS adoption
WUR Capabilities	As defined in frame format	As defined in 9.4.2.291	The value from WUR Capabilities element. The parameter is present if dot11WUROptionImplemented is true and a WUR Capabilities element was present in the Probe Response or Beacon frame from which the BSSDescription was determined; otherwise, the parameter is not present.	Do not adopt
WUR Operation	As defined in frame format	As defined in 9.4.2.292	The value from WUR Operation element. The parameter is present if dot11WUROptionImplemented is true and a WUR Operation element was present in the Probe Response or Beacon frame from which the BSSDescriptionSet was determined; otherwise, the parameter is not present.	Do not adopt
WUR Discovery	As defined in frame format	As defined in 9.4.2.294	The value from WUR Discovery element. The parameter is present if dot11WUROptionImplemented is true and a WUR Discovery element was present in the Probe Response or Beacon frame from which the BSSDescriptionSet was determined; otherwise, the parameter is not present.	Do not adopt

6.3.4 Synchronization

6.3.4.2 MLME-JOIN.request

6.3.4.2.2 Semantics of the service primitive

Change the primitive parameters as follows (not all existing parameters in the baseline are shown):

The primitive parameters are as follows:

```
MLME-JOIN.request(  
    ...,  
    WUR Capabilities,  
    VendorSpecificInfo  
)
```

Insert the following entry into the unnumbered table in this subclause maintaining the primitive order above:

Name	Type	Valid range	Description
WUR Capabilities	As defined in WUR Capabilities element	As defined in 9.4.2.291	Specifies the parameters within the WUR Capabilities element that are supported by the STA. The parameter is present if dot11WUROptionImplemented is true; otherwise, this parameter is not present.

6.3.7 Associate

6.3.7.2 MLME-ASSOCIATE.request

6.3.7.2.2 Semantics of the service primitive

Change the primitive parameters as follows (not all parameters are shown):

The primitive parameters are as follows:

```
MLME-ASSOCIATE.request(  
    ...,  
    WUR Mode,  
    VendorSpecificInfo  
)
```

Insert the following entry into the unnumbered table in this subclause maintaining the primitive order above:

Name	Type	Valid range	Description
WUR Mode	WUR Mode element	As defined in 9.4.2.293	Specifies the proposed service parameters for the WUR Mode Setup request. The parameter is optionally present if dot11WUROptionImplemented is true; otherwise, this parameter is not present.

6.3.7.3 MLME-ASSOCIATE.confirm

6.3.7.3.2 Semantics of the service primitive

Change the primitive parameters as follows (not all parameters are shown):

The primitive parameters are as follows:

```
MLME-ASSOCIATE.confirm(
    ...,
    WUR Capabilities,
    WUR Operation,
    WUR Mode,
    VendorSpecificInfo
)
```

Insert the following entries into the unnumbered table in this subclause maintaining the primitive order above:

Name	Type	Valid range	Description
WUR Capabilities	As defined in WUR Capabilities element	As defined in 9.4.2.291	Specifies the parameters within the WUR Capabilities element that are supported by the WUR AP. The parameter is present if dot11WUROptionImplemented is true; otherwise, this parameter is not present.
WUR Operation	As defined in WUR Operation element	As defined in 9.4.2.292	Provides additional information for WUR operation. The parameter is present if dot11WUROptionImplemented is true; otherwise, this parameter is not present.
WUR Mode	As defined in WUR Mode element	As defined in 9.4.2.293	Specifies the proposed service parameters for the WUR Mode Setup request. The parameter is present if dot11WUROptionImplemented is true and the WUR Mode element is present in the Association Response frame received from the AP; otherwise, this parameter is not present.

6.3.7.4 MLME-ASSOCIATE.indication

6.3.7.4.2 Semantics of the service primitive

Change the primitive parameters as follows (not all existing parameters in the baseline are shown):

The primitive parameters are as follows:

```
MLME-ASSOCIATE.indication(
    ...
    WUR Capabilities,
    WUR Mode,
    VendorSpecificInfo
)
```

Insert the following entry into the unnumbered table in this subclause maintaining the primitive order above:

Name	Type	Valid range	Description
WUR Capabilities	As defined in WUR Capabilities element	As defined in 9.4.2.291	Specifies the parameters within the WUR Capabilities element that are supported by the peer STA. The parameter is present if it is present in the Association Request frame received from the STA; otherwise, this parameter is not present.
WUR Mode	As defined in WUR Mode element	As defined in 9.4.2.293	Specifies the proposed service parameters for the WUR Mode Setup request. The parameter is present if dot11WUROptionImplemented is true and the WUR Mode element is present in the Association Request frame received from the STA; otherwise, this parameter is not present.

6.3.7.5 MLME-ASSOCIATE.response

6.3.7.5.2 Semantics of the service primitive

Change the primitive parameters as follows (not all existing parameters in the baseline are shown):

The primitive parameters are as follows:

```
MLME-ASSOCIATE.response(
    ...,
    WUR Capabilities,
    WUR Operation,
    WUR Mode,
    VendorSpecificInfo
)
```

Insert the following entries into the unnumbered table in this subclause maintaining the primitive order above:

Name	Type	Valid range	Description
WUR Capabilities	As defined in WUR Capabilities element	As defined in 9.4.2.291	Specifies the parameters within the WUR Capabilities element that are supported by the STA. The parameter is present if dot11WUROptionImplemented is true; otherwise, this parameter is not present.

WUR Operation	As defined in WUR Operation element	As defined in 9.4.2.292	Provides additional information for WUR operation. The parameter is present if dot11WUROptionImplemented is true; otherwise not present.
WUR Mode	As defined in WUR Mode element	As defined in 9.4.2.293	Specifies the proposed service parameters for the WUR Mode Setup request. The parameter is optionally present if dot11WUROptionImplemented is true; otherwise, this parameter is not present.

6.3.8 Reassociate

6.3.8.2 MLME-REASSOCIATE.request

6.3.8.2.2 Semantics of the service primitive

Change the primitive parameters as follows (not all existing parameters in the baseline are shown):

The primitive parameters are as follows:

```
MLME-REASSOCIATE.request(
    ...,
    WUR Mode,
    VendorSpecificInfo
)
```

Insert the following entries into the unnumbered table in this subclause maintaining the primitive order above:

Name	Type	Valid range	Description
WUR Mode	As defined in WUR Mode element	As defined in 9.4.2.293	Specifies the proposed service parameters for the WUR Mode Setup request. The parameter is optionally present if dot11WUROptionImplemented is true; otherwise, this parameter is not present.

6.3.8.3 MLME-REASSOCIATE.confirm

6.3.8.3.2 Semantics of the service primitive

Change the primitive parameters as follows (not all existing parameters in the baseline are shown):

The primitive parameters are as follows:

MLME-REASSOCIATE.confirm(

...,
WUR Capabilities,
WUR Operation,
WUR Mode,
VendorSpecificInfo
)

Insert the following entries into the unnumbered table in this subclause maintaining the primitive order above:

Name	Type	Valid range	Description
WUR Capabilities	As defined in WUR Capabilities element	As defined in 9.4.2.291	Specifies the parameters within the WUR Capabilities element that are supported by the WUR AP. The parameter is present if dot11WUROptionImplemented is true; otherwise, this parameter is not present.
WUR Operation	As defined in WUR Operation element	As defined in 9.4.2.292	Provides additional information for WUR operation. The parameter is present if dot11WUROptionImplemented is true; otherwise not present.
WUR Mode	As defined in WUR Mode element	As defined in 9.4.2.293	Specifies the proposed service parameters for the WUR Mode Setup request. The parameter is present if dot11WUROptionImplemented is true and the WUR Mode element is present in the Reassociation Response frame received from the AP; otherwise, this parameter is not present.

6.3.8.4 MLME-REASSOCIATE.indication

6.3.8.4.2 Semantics of the service primitive

Change the primitive parameters as follows (not all parameters are shown):

The primitive parameters are as follows:

MLME-REASSOCIATE.indication(
...,
WUR Capabilities,
WUR Mode,
VendorSpecificInfo
)

Insert the following entry into the unnumbered table in this subclause maintaining the primitive order above:

Name	Type	Valid range	Description
WUR Capabilities	As defined in WUR Capabilities element	As defined in 9.4.2.291	Specifies the parameters within the WUR Capabilities element that are supported by the peer STA. The parameter is present if it is present in the Association Request frame received from the STA; otherwise, this parameter is not present.
WUR Mode	As defined in WUR Mode element	As defined in 9.4.2.293	Specifies the proposed service parameters for the WUR Mode Setup request. The parameter is present if dot11WUROptionImplemented is true and the WUR Mode element is present in the Reassociation Request frame received from the STA; otherwise, this parameter is not present.

6.3.8.5 MLME-REASSOCIATE.response

6.3.8.5.2 Semantics of the service primitive

Change the primitive parameters as follows (not all existing parameters in the baseline are shown):

The primitive parameters are as follows:

```
MLME-REASSOCIATE.response(
    ...,
    WUR Capabilities,
    WUR Operation,
    WUR Mode,
    VendorSpecificInfo
)
```

Insert the following entries into the unnumbered table in this subclause maintaining the primitive order above:

Name	Type	Valid range	Description
WUR Capabilities	As defined in WUR Capabilities element	As defined in 9.4.2.291	Specifies the parameters within the WUR Capabilities element that are supported by the STA. The parameter is present if dot11WUROptionImplemented is true; otherwise, this parameter is not present.

WUR Operation	As defined in WUR Operation element	As defined in 9.4.2.292	Provides additional information for WUR operation. The parameter is present if dot11WUROptionImplemented is true; otherwise not present.
WUR Mode	As defined in WUR Mode element	As defined in 9.4.2.293	Specifies the proposed service parameters for the WUR Mode Setup request. The parameter is optionally present if dot11WUROptionImplemented is true; otherwise, this parameter is not present.

6.3.11 Start

6.3.11.2 MLME-START.request

6.3.11.2.2 Semantics of the service primitive

Change the primitive parameters as follows (not all existing parameters in the baseline are shown):

```
MLME-START.request(
    ...
    WUR Capabilities,
    WUR Operation,
    WUR Discovery,
    VendorSpecificInfo
)
```

Insert the following entry into the unnumbered table in this subclause maintaining the primitive order above:

Name	Type	Valid range	Description
WUR Capabilities	As defined in WUR Capabilities element	As defined in 9.4.2.291	Specifies the parameters within the WUR Capabilities element that are supported by the STA. The parameter is present if dot11WUROptionImplemented is true; otherwise, this parameter is not present.
WUR Operation	As defined in WUR Operation element	As defined in 9.4.2.292	Provides additional information for WUR operation. The parameter is present if dot11WUROptionImplemented is true; otherwise not present.

WUR Discovery	A defined in WUR Discovery element	As defined in 9.4.2.294	Specifies the parameters used for transmission of WUR Discovery frames. The parameter is present if <code>dot11WUROptionImplemented</code> is true and <code>dot11WURDiscoveryImplemented</code> is true; otherwise, this parameter is not present.
---------------	------------------------------------	-------------------------	---

6.3.19 SetKeys

6.3.19.1 MLME-SETKEYS.request

6.3.19.1.2 Semantics of the service primitive

Change the 2nd table as follows:

Name	Type	Valid range	Description
Key	Bit string	N/A	The temporal key value
Length	Integer	N/A	The number of bits in the Key to be used.
Key ID	Integer	0–3 shall be used with WEP, TKIP, CCMP, and GCMP; 4–5 with BIP for IGTK; 6–7 with BIP for BIGTK; ~~8–9~~ with BIP for <u>WIGTK</u> ; and ~~810–4095~~ are reserved	Key identifier
Key Type	Integer	Group, Pairwise, PeerKey, IGTK, BIGTK, <u>WIGTK</u>	Defines whether this key is a group key, pairwise key, PeerKey, or Integrity Group key, ~~or beacon protection key, or wake-up radio integrity group temporal key.~~
Address	MACAddress	Any valid individual MAC address	This parameter is valid only when the Key Type value is Pairwise, when the Key Type value is Group and the STA is in IBSS, or when the Key Type value is PeerKey.
Receive Sequence Count	8 octets	N/A	Value to which the RSC(s) is initialized. This parameter is valid only when the Key Type is Group, IGTK, ~~or BIGTK, or~~ <u>WIGTK</u> .

6.3.19.1.4 Effect of receipt

Change the 1st paragraph as follows:

When the Key Type is Group, IGTK, ~~or BIGTK, or~~ WIGTK, and the key matches the existing GTK, IGTK, ~~or BIGTK, or~~ WIGTK, installed as a result of exiting WNM sleep mode (see 11.2.3.16.1), if any, or matches the existing GTK or IGTK installed as a result of receipt of EAPOL-Key frames (see 12.7.7.4) receipt of this primitive shall have no effect. Otherwise, receipt of this primitive causes the MAC to apply the keys as follows, subject to the MLME-SETPROTECTION.request primitive:

6.3.20 DeleteKeys

6.3.20.1 MLME-DELETEKEYS.request

6.3.20.1.2 Semantics of the service primitive

Change the 2nd table as follows:

Name	Type	Valid range	Description
Key ID	Integer	0–3 shall be used with WEP, TKIP, CCMP, and GCMP; 4–5 with BIP; 6–7 with BIP for BIGTK; <u>8–9 with BIP for WIGTK</u> ; and ~~8~~ <u>10–4095</u> are reserved	Key identifier.
Key Type	Integer	Group, Pairwise, PeerKey, IGTK, BIGTK, <u>WIGTK</u>	Defines whether this key is a group key, pairwise key, PeerKey, Integrity Group key, ~~or~~ <u>beacon integrity group temporal key, or wake-up radio integrity group temporal key.</u>
Address	MACAddress	Any valid individual MAC address	This parameter is valid only when the Key Type value is Pairwise, or when the Key Type value is Group and is from an IBSS STA, or when the Key Type value is PeerKey.

6.3.23 SetProtection

6.3.23.1 MLME-SETPROTECTION.request

6.3.23.1.2 Semantics of the service primitive

Change the 2nd table as follows:

Name	Type	Valid range	Description
Address	MACAddress	Any valid individual MAC address	This parameter is valid only when the Key Type value is Pairwise or when the Key Type value is Group and is from an IBSS STA or PeerKey.
ProtectType	Enumeration	None, Rx, Tx, Rx_Tx	The protection value for this MAC.
Key Type	Integer	Group, Pairwise, PeerKey, IGTK, BIGTK, <u>WIGTK</u>	Defines whether this key is a group key, pairwise key, PeerKey, Integrity Group key, ~~or~~ <u>beacon integrity group temporal key, or wake-up radio integrity group temporal key.</u>

6.3.92 PN event report

6.3.92.2 MLME-PN-EXHAUSTION.indication

6.3.92.2.2 Semantics of the service primitive

Change the 1st table as follows:

Name	Type	Valid range	Description
Key ID	Integer	0–3 shall be used with WEP, TKIP, CCMP, and GCMP; 4–5 with BIP; 6–7 with BIP for BIGTK; <u>8–9 with BIP for WIGTK;</u> and ~~810–4095~~ are reserved	Key identifier.
Key Type	Integer	Group, Pairwise, PeerKey, IGTK, BIGTK, <u>WIGTK</u>	Defines whether this key is a group key, pairwise key, PeerKey, Integrity Group key, ~~or beacon integrity group temporal key,~~ <u>or wake-up radio integrity group temporal key.</u>
Address	MAC address	Any valid individual MAC address	This parameter is valid only when the Key Type value is Pairwise, or when the Key Type value is Group and is from an IBSS STA, or when the Key Type value is PeerKey.

6.3.92.3 MLME-PN-WARNING.indication

6.3.92.3.2 Semantics of the service primitive

Change the 1st table as follows:

Name	Type	Valid range	Description
Key ID	Integer	0–3 shall be used with WEP, TKIP, CCMP, and GCMP; 4–5 with BIP; 6–7 with BIP for BIGTK; <u>8–9 with BIP for WIGTK;</u> and ~~810–4095~~ are reserved	Key identifier.
Key Type	Integer	Group, Pairwise, PeerKey, IGTK, BIGTK, <u>WIGTK</u>	Defines whether this key is a group key, pairwise key, PeerKey, Integrity Group key, ~~or beacon integrity group temporal key,~~ <u>or wake-up radio integrity group temporal key.</u>
Address	MAC address	Any valid individual MAC address	This parameter is valid only when the Key Type value is Pairwise, or when the Key Type value is Group and is from an IBSS STA, or when the Key Type value is PeerKey.

Insert the following subclauses at the end of Clause 6:

6.3.123 WUR mode setup

6.3.123.1 General

The following MLME primitives support the signaling of WUR mode setup procedure described in 29.8.2.

6.3.123.2 MLME-WURMODESETUP.request

6.3.123.2.1 Function

This primitive requests that a WUR Mode Setup frame be sent as specified in 29.8.2.

6.3.123.2.2 Semantics of the service primitive

The primitive parameters are as follows:

MLME-WURMODESETUP.request(
PeerSTAAddress,
DialogToken,
WURMode,
WURPNUpdate)

Name	Type	Valid range	Description
PeerSTAAddress	MAC Address	Any valid individual MAC Address	Specifies the address of the peer MAC entity with which to perform the WUR mode setup request/response procedure.
DialogToken	Integer	0–255	The dialog token to identify the WUR Mode Setup request/response transaction.
WURMode	WUR Mode element	As defined in 9.4.2.293	Specifies the proposed service parameters for the WUR mode setup request
WURPNUpdate	WUR PN Update element	One or more WUR PN Update elements as defined in 9.4.2.295	Provides information related to update of WUR PNs. The parameter is optionally present if dot11RSNAWURFrameProtectionActivated is true; otherwise not present.

6.3.123.2.3 When generated

This primitive is generated by the SME to request that a WUR Mode Setup frame be sent.

6.3.123.2.4 Effect of receipt

On receipt of this primitive, the MLME constructs a WUR Mode Setup frame. The STA then attempts to transmit this WUR Mode Setup frame.

6.3.123.3 MLME-WURMODESETUP.confirm

6.3.123.3.1 Function

This primitive reports the result of a WUR Setup request/response procedure in 29.8.2.

6.3.123.3.2 Semantics of the service primitive

The primitive parameters are as follows:

MLME-WURMODESETUP.confirm(
PeerSTAAddress,
DialogToken,
WURMode,
WUR Operation,
WURPNUpdate)

Name	Type	Valid range	Description
PeerSTAAddress	MAC Address	Any valid individual MAC Address	Specifies the address of the peer MAC entity with which to perform the WUR mode setup request/response procedure.
DialogToken	Integer	0–255	The dialog token to identify the WUR mode setup request/response transaction.
WURMode	WUR Mode element	As defined in 9.4.2.293	Specifies the proposed service parameters for the WUR Mode Setup request
WUR Operation	As defined in WUR Operation element	As defined in 9.4.2.292	Provides additional information for WUR operation. The parameter is optionally present if dot11WUROptionImplemented is true; otherwise not present.
WURPNUpdate	WUR PN Update element	One or more WUR PN Update elements as defined in 9.4.2.295	Provides information related to update of WUR PNs. The parameter is optionally present if dot11RSNAWURFrameProtectionActivated is true; otherwise not present.

6.3.123.3.3 When generated

This primitive is generated by the MLME as a result of an MLME-WURMODESETUP.request primitive and indicates the results of the request. This primitive is generated when the STA receives a WUR Mode Setup frame from its associated AP in response to a WUR Mode Setup frame transmitted by the STA.

6.3.123.3.4 Effect of receipt

On receipt of this primitive, the SME should operate according to the procedure in 29.8.2.

6.3.123.4 MLME-WURMODESETUP.indication

6.3.123.4.1 Function

This primitive indicates that a WUR Mode Setup frame was received from an associated non-AP STA.

6.3.123.4.2 Semantics of the service primitive

The primitive parameters are as follows:

MLME-WURMODESETUP.indication(
PeerSTAAddress,
DialogToken,
WURMode,
WURPNUpdate)

Name	Type	Valid range	Description
PeerSTAAddress	MAC Address	Any valid individual MAC Address	Specifies the address of the peer MAC entity from which a WUR Mode Setup frame was received.
DialogToken	Integer	0–255	The dialog token to identify the WUR mode setup request/response transaction.
WURMode	WUR Mode element	As defined in 9.4.2.293	Specifies the proposed service parameters for the WUR mode setup request.
WURPNUpdate	WUR PN Update element	One or more WUR PN Update elements as defined in 9.4.2.295	Provides information related to update of WUR PNs. The parameter is optionally present if dot11RSNAWURFrameProtectionActivated is true; otherwise not present.

6.3.123.4.3 When generated

This primitive is generated by the MLME when a WUR Mode Setup frame is received from an associated non-AP STA.

6.3.123.4.4 Effect of receipt

On receipt of this primitive, the SME should operate according to the procedure in 29.8.2.

6.3.123.5 MLME-WURMODESETUP.response

6.3.123.5.1 Function

This primitive is used to send a WUR Mode Setup frame, in response to a received WUR Mode Setup frame.

6.3.123.5.2 Semantics of the service primitive

The primitive parameters are as follows:

MLME-WURMODESETUP.response(
PeerSTAAddress,
DialogToken,
WURMode,
WUR Operation,

WURPNUpdate)

Name	Type	Valid range	Description
PeerSTAAddress	MAC Address	Any valid individual MAC Address	Specifies the address of the peer MAC entity from which a WUR Mode Setup frame was received.
DialogToken	Integer	0–255	The dialog token to identify the WUR mode setup request/response transaction.
WURMode	WUR Mode element	As defined in 9.4.2.293	Specifies the proposed service parameters for the WUR mode setup response.
WUR Operation	As defined in WUR Operation element	As defined in 9.4.2.292	Provides additional information for WUR operation. The parameter is optionally present if dot11WUROptionImplemented is true; otherwise not present.
WURPNUpdate	WUR PN Update element	One or more WUR PN Update elements as defined in 9.4.2.295	Provides information related to update of WUR PNs. The parameter is optionally present if dot11RSNAWURFrameProtectionActivated is true; otherwise not present.

6.3.123.5.3 When generated

This primitive is generated by the SME to request that a WUR Mode Setup frame be sent to a peer entity to convey the WUR parameter information.

6.3.123.5.4 Effect of receipt

On receipt of this primitive, the MLME constructs a WUR Mode Setup frame. The STA then attempts to transmit this frame to the non-AP STA indicated by the PeerSTAAddress parameter in 29.8.2.

6.3.124 WUR mode teardown

6.3.124.1 General

The following MLME primitives support the signaling of WUR mode teardown procedure described in 29.8.2.

6.3.124.2 MLME-WURMODETEARDOWN.request

6.3.124.2.1 Function

This primitive requests that a WUR Mode Teardown frame be sent as specified in 29.8.2.

6.3.124.2.2 Semantics of the service primitive

The primitive parameters are as follows:

```
MLME-WURMODETEARDOWN.request(  

    PeerSTAAddress  

)
```

Name	Type	Valid range	Description
PeerSTAAddress	MAC Address	Any valid individual MAC Address	Specifies the address of the peer MAC entity with which to perform the WUR mode teardown procedure.

6.3.124.2.3 When generated

This primitive is generated by the SME to request that a WUR Mode Teardown frame be sent to the peer entity.

6.3.124.2.4 Effect of receipt

On receipt of this primitive, the MLME constructs a WUR Mode Teardown frame. The STA then attempts to transmit this frame to the peer entity with which it performed the WUR Mode Setup request/response procedure.

6.3.124.3 MLME-WURMODETEARDOWN.indication

6.3.124.3.1 Function

This primitive indicates that a WUR Mode Teardown frame was received.

6.3.124.3.2 Semantics of the service primitive

The primitive parameters are as follows:

```
MLME-WURMODETEARDOWN.indication(  

    PeerSTAAddress  

)
```

Name	Type	Valid range	Description
PeerSTAAddress	MAC Address	Any valid individual MAC Address	Specifies the address of the peer MAC entity with which to perform the WUR mode teardown procedure.

6.3.124.3.3 When generated

This primitive is generated by the MLME when a WUR Mode Teardown frame is received.

6.3.124.3.4 Effect of receipt

On receipt of this primitive, the SME should operate according to the procedure in 29.8.2.

6.3.125 WUR Discovery

6.3.125.1 General

The following MLME primitives support the WUR discovery procedure described in 29.12.

6.3.125.2 MLME-WURDISCOVERY.request

6.3.125.2.1 Function

This primitive requests to initiate WUR scanning.

6.3.125.2.2 Semantics of the service primitive

This primitive parameters are as follows:

MLME-WURDISCOVERY.request(

WURDiscoveryChannelList,
MinChannelTime,
MaxChannelTime,
Transmitter ID,
CompressedBSSID_MSB,
Compressed SSID)

Name	Type	Valid range	Description
WURDiscoveryChannelList	A set of operating class and channel information as defined in 9.4.1.22.	Each channel is selected from the valid channel range for the appropriate PHY and carrier set.	Specifies the WUR discovery channels that are examined when scanning for a WUR Discovery frame.
MinChannelTime	Integer	N/A	The minimum time (in TU) to spend on each WUR discovery channel when scanning for WUR Discovery frames.
MaxChannelTime	Integer	$\geq \text{MinChannelTime}$	The maximum time (in TU) to spend on each WUR discovery channel when scanning for WUR Discovery frames.
Transmitter ID	Integer	As defined in 29.5.3	The Transmitter ID of the WUR AP to be discovered. This parameter is optionally present.

CompressedBSSID_MSB	Integer	As defined in 9.9.3.3	The 12 MSBs of the compressed BSSID of the WUR AP to be discovered. This parameter is optionally present.
Compressed SSID	Integer	As defined in 9.9.3.3	The 16 LSBs of the short SSID of the WUR AP to be discovered. This parameter is optionally present.

6.3.125.2.3 When generated

This primitive is generated by the SME for a WUR non-AP STA to determine if there are other BSSs that it can join.

6.3.125.2.4 Effect of receipt

This request initiates the WUR discovery procedure.

6.3.125.3 MLME-WURDISCOVERY.confirm

6.3.125.3.1 Function

This primitive indicates the receipt of a WUR Discovery frame during WUR discovery procedure.

6.3.125.3.2 Semantics of the service primitive

The primitive parameters are as follows:

MLME-WURDISCOVERY.confirm(

BSSDescriptionFromWDSets,

ResultCode)

Name	Type	Valid range	Description
BSSDescription-FromWDSets	Set of BSSDescription-FromWDSets	N/A	The BSSDescriptionFromWDSets is returned to indicate the results of the WUR discovery derived from WUR Discovery frames. It is a set containing zero or more instances of a BSSDescriptionFromWD. Present if both dot11WUROptionImplemented and dot11WURDiscoveryImplemented are true; otherwise, not present.
ResultCode	Enumeration	SUCCESS, NOT_SUPPORTED	Indicates the result of the MLME-WURDISCOVERY.confirm primitive.