

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 1: Fast Initial Link Setup

IEEE Computer Society

Sponsored by the
LAN/MAN Standards Committee

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

IEEE Std 802.11ai™-2016
(Amendment to
IEEE Std 802.11™-2016)

**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 1: Fast Initial Link Setup

SECOND PRINTING: 14 April 2017

Sponsor

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

Approved 7 December 2016

IEEE-SA Standards Board

Abstract: Mechanisms that provide IEEE Std 802.11 networks with fast initial link setup methods that do not degrade the security offered by Robust Security Network Association (RSNA) already defined in IEEE Std 802.11 are defined in this amendment.

Keywords: amendment, Fast Initial Link setup, FILS, IEEE 802.11ai™

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

Copyright © 2016 by The Institute of Electrical and Electronics Engineers, Inc.
All rights reserved. Published 30 December 2016. Printed in the United States of America.

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

SECOND PRINTING: 14 April 2017. Erratum included in Clause 9—Table 9-46 and Table 9-47.

PDF: ISBN 978-1-5044-3631-1 STD22359
Print: ISBN 978-1-5044-3632-8 STDPD22359

IEEE prohibits discrimination, harassment, and bullying.

For more information, visit <http://www.ieee.org/web/aboutus/whatis/policies/p9-26.html>.

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

Important Notices and Disclaimers Concerning IEEE Standards Documents

IEEE documents are made available for use subject to important notices and legal disclaimers. These notices and disclaimers, or a reference to this page, appear in all standards and may be found under the heading “Important Notices and Disclaimers Concerning IEEE Standards Documents.” They can also be obtained on request from IEEE or viewed at <http://standards.ieee.org/IPR/disclaimers.html>.

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

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

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

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

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

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

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

Translations

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

Official statements

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

Comments on standards

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

Comments on standards should be submitted to the following address:

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

Laws and regulations

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

Copyrights

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

Photocopies

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

Updating of IEEE Standards documents

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

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

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

Errata

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

Patents

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

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

Participants

At the time this standard was completed, the IEEE 802.11 Working Group had the following membership:

Adrian P. Stephens, *Chair*
Jon W. Rosdahl, *1st Vice Chair*
Dorothy V. Stanley, *2nd Vice Chair*
Stephen McCann, *Secretary*

The following were officers of Task Group ai:

Hiroshi Mano, *Chair*
Marc Emmelmann, *Vice Chair*
Hitoshi Morioka, *Secretary*
Lee R. Armstrong, *Co-Technical Editor*
Ping Fang, *Co-Technical Editor*

Osama S. Aboulmagd
Santosh P. Abraham
Roberto Aiello
Thomas Alexander
Peiman Amini
Sirikiat Lek Ariyavisitakul
Yusuke Asai
Alex Ashley
Kwok Shum Au
Vijay Auluck
Stefan Aust
David Bagby
Eugene Baik
Gabor Bajko
Raja Banerjea
Phillip Barber
Anuj Batra
Tuncer Baykas
Alan Berkema
Nehru Bhandaru
Philippe Boucachard
Andre Bourdoux
John Buffington
Lin Cai
George Calcev
Chris Calvert
Radhakrishna Canchi
Laurent Cariou
William Carney
Jaesun Cha
Romana Challans
Kim Chang
Kuor-Hsin Chang
Xin Chang
Clint F. Chaplin
Bin Chen
Jiamin Chen
Jixin Chen
Lidong Chen
Qian Chen
Xi Chen
Minho Cheong
George Cherian
Francois Chin
Rojan Chitrakar

Jinsoo Choi
Sangsung Choi
Li Chia Chia Choo
Sayantan Choudhury
Liwen Chu
Jinyoung Chun
John Coffey
Kenneth Coop
Carlos Cordeiro
Neiyer Correal
Subir Das
Hendricus De Ruijter
Rolf J. de Vegt
Yohannes Demessie
Michael Denson
Ting Dong
Xiandong Dong
Klaus Doppler
Roger P. Durand
Donald E. Eastlake
Peter Ecclesine
Richard Edgar
Amal Ekbal
Vinko Erceg
Yonggang Fang
Qin Fei
Stanislav Filin
Norman Finn
Matthew J. Fischer
George Flammer
Chittabrata Ghosh
James P. K. Gilb
Reinhard Gloger
Daning Gong
David Goodall
Elad Gottlib
Sudheer A. Grandhi
Stephen Grau
Michael Grigat
David Halasz
Mark A. Hamilton
Christopher J. Hansen
Peng Hao
Hiroshi Harada
Daniel N. Harkins

Brian D. Hart
Ahmadreza Hedayat
Robert F. Heile
Jerome Henry
Chin Keong Ho
Anh Tuan Hoang
Dien Hoang
Wei Hong
Ying-Chuan Hsiao
Jing-Rong Hsieh
David Hunter
Yasuhiko Inoue
Mitsuru Iwaoka
Wuncheol Jeong
Yangseok Jeong
Sunggeun Jin
ZhongYi Jin
Nihar Jindal
V. K. Jones
Jari Junell
Padam Kafle
Carl W. Kain
Hyunduk Kang
Mika Kasslin
Richard H. Kennedy
Stuart J. Kerry
Eunkyoung Kim
Jeongki Kim
Jinho Kim
Joo Young Kim
Joonsuk Kim
Suhwook Kim
Taejoon Kim
Youhan Kim
Youngsoo Kim
Shoichi Kitazawa
Jarkko Knecht
Gwangzeen Ko
Fumihide Kojima
Tom Kolze
Timo Koskela
Bruce P. Kraemer
Jin-Sam Kwak
Joseph Kwak
Hyounjin Kwon

Young Hoon Kwon
 Paul Lambert
 Zhou Lan
 Leonardo Lanante
 James Lansford
 Jean-Pierre Le Rouzic
 Anseok Lee
 Donghun Lee
 Jae Seung Lee
 Wookbong Lee
 Zhongding Lei
 Wai Kong Leung
 Joseph Levy
 Feng Li
 Huan-Bang Li
 Liang Li
 Lingjie Li
 Yunbo Li
 Yunzhou Li
 Zhiqiang Li
 Erik Lindskog
 Jianhan Liu
 Pei Liu
 Yong Liu
 Zongru Liu
 Peter Loc
 Su Lu
 Long Luo
 Yi Luo
 Zhendong Luo
 Kaiying Lv
 Michael Lynch
 Jouni K. Malinen
 Simone Merlin
 James Miller
 Keiichi Mizutani
 Apurva Mody
 Michael Montemurro
 Kenichi Mori
 Ronald Murias
 Andrew Myles
 Yukimasa Nagai
 Yuhei Nagao
 Hiroki Nakano
 Chiu Ngo
 Paul Nikolich
 Hiroyo Ogawa
 Minseok Oh
 Min-seok Oh
 David Olson
 Satoshi Oyama
 Michael J. Paljug
 Santos Ghanshyam Pandey
 Anna Pantelidou
 Giwon Park
 Minyoung Park
 Seung-Hoon Park
 Jaya Shankar Pathmasuntharam
 Sandhya Patil
 Xiaoming Peng
 Eldad Perahia
 James E. Petranovich

Albert Petrick
 John Petro
 Xu Ping
 Juho Pirskanen
 Khiam Boon Png
 Vishakan Ponnampalam
 Ron Porat
 Henry S. Ptasinski
 Rethnakaran Pulikkoonattu
 Chang-Woo Chang Pyo
 Emily H. Qi
 Huyu Qu
 Harish Ramamurthy
 Jayaram Ramasastry
 Ivan Reede
 Edward Reuss
 Maximilian Riegel
 Mark Rison
 Zhigang Rong
 Jon W. Rosdahl
 Cheol Ryu
 Kiseon Ryu
 Kazuyuki Sakoda
 Ruben E. Salazar Cardozo
 Hemanth Sampath
 Sigurd Schelstraete
 Jean Schwoerer
 Jonathan Segev
 Cristina Seibert
 Yongho Seok
 Kunal Shah
 Huairong Shao
 Zhenhai Shao
 Stephen J. Shellhammer
 Ian Sherlock
 Wei Shi
 Nobuhiko Shibagaki
 Shusaku Shimada
 Chang Sub Shin
 Thomas M. Siep
 Michael Sim
 Dwight Smith
 Graham Kenneth Smith
 Myung Sun Song
 Sudhir Srinivasa
 Robert Stacey
 Dorothy V. Stanley
 Lawrence Stefani
 Adrian P. Stephens
 Rene Struik
 Jung Hoon Suh
 Chin-sean Sum
 Bo Sun
 Chen Sun
 Sheng Sun
 Kazuaki Takahashi
 Mineo Takai
 Sagar Tamhane
 Joseph Teo
 Thomas Tetzlaff
 Jerry Thrasher
 Tong Tian

Jens Tingleff
 Fei Tong
 Ha Nguyen Tran
 Kazuyoshi Tsukada
 Masahiro Umehira
 Richard D. J. Van Nee
 Allert Van Zelst
 Prabodh Varshney
 Sameer Vermani
 Dalton T. Victor
 Gabriel Villardi
 George A Vlantis
 Chao Chun Wang
 Haiguang Wang
 Haiming Wang
 James June Wang
 Lei Wang
 Lin Wang
 Qi Wang
 Xiang Wang
 Xuehuan Wang
 Lisa Ward
 Zou Wei-Xia
 Lei Wen
 Menzo M. Wentink
 Harya Wicaksana
 Eric Wong
 Harry R. Worstell
 Tianyu Wu
 Zhanji Wu
 Zhenyu Xiao
 Dongmei Xu
 Quanping Xu
 Guang-Qi Yang
 Lin Yang
 Xun Yang
 Yunsong Yang
 Fan Ye
 James Yee
 Peter Yee
 Wai-Leong Yeow
 Kaoru Yokoo
 Su Khiong Khiong Yong
 Christopher Young
 Heejung Yu
 Zhan Yu
 Tevfik Yucek
 Guangrong Yue
 Katsuo D. A. Yunoki
 Hongyuan Zhang
 Hui Zhang
 Junjian Zhang
 Nianzu Zhang
 Xin Zhang
 Mu Zhao
 Jun Zheng
 Shoukang Zheng
 Mingtuo Zhou
 Yan Zhuang
 Lan Zhuo

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

Tomoko Adachi	Werner Hoelzl	Robert O'Hara
Thomas Alexander	Russell Housley	Yoshihiro Ohba
Richard Alfvén	Noriyuki Ikeuchi	Satoshi Oyama
Nobumitsu Amachi	Yasuhiko Inoue	Stephen Palm
Carol Ansley	Akio Iso	Arumugam Paventhan
Butch Anton	Atsushi Ito	Venkatesha Prasad
Yusuke Asai	Raj Jain	Karen Randall
Alfred Asterjadhi	Adri Jovin	Maximilian Riegel
Stefan Aust	Naveen Kakani	Mark Rison
Gabor Bajko	Shinkyō Kaku	Robert Robinson
Phillip Barber	Hyunjeong Kang	Benjamin Rolfe
Harry Bims	Piotr Karocki	Jon W. Rosdahl
Gennaro Boggia	John Kenney	Osman Sakr
Nancy Bravin	Stuart Kerry	Shigenobu Sasaki
Jairo Bustos Heredia	Youhan Kim	Naotaka Sato
William Byrd	Patrick Kinney	Bartien Sayogo
Radhakrishna Canchi	Bruce Kraemer	Andy Scott
Cagatay Capar	Yasushi Kudoh	Yongho Seok
William Carney	Thomas Kurihara	Ian Sherlock
Juan Carreon	Paul Lambert	Graham Smith
Minho Cheong	Jeremy Landt	Daniel Smolinski
Paul Chiuchiolo	Hyeong Ho Lee	Ju-Hyung Son
Sayantán Choudhury	Zhongding Lei	Kapil Sood
Keith Chow	James Lepp	Thomas Starai
Charles Cook	Joseph Levy	Adrian P. Stephens
Subir Das	Arthur H. Light	Rene Struik
Patrick Diamond	William Lumpkins	Walter Struppler
Yezid Donoso	Michael Lynch	Michael Swearingen
Malcolm Dowse	Chris Lyttle	Payam Torab
Sourav Dutta	Elvis Maculuba	Kazuyoshi Tsukada
Richard Edgar	Jouni Malinen	Mark-Rene Uchida
Marc Emmelmann	Hiroshi Mano	Lorenzo Vangelista
Michael Fischer	James Marin	Dmitri Varsanofiev
Avraham Freedman	Stephen McCann	Prabodh Varshney
Devon Gayle	Michael McInnis	Ganesh Venkatesan
Joel Goergen	Filip Mestanov	George Vlantis
Randall Groves	Michael Montemurro	Khurram Waheed
Michael Gundlach	Jose Morales	Haiming Wang
Gloria Gwynne	Ronald Murias	James June Wang
Russell Haines	Rick Murphy	Lei Wang
Mark Hamilton	Andrew Myles	Xiaofei Wang
Daniel Harkins	Michael Newman	Hung-Yu Wei
Jerome Henry	Nick S.A. Nikjoo	James Yee
Marco Hernandez	John Notor	Oren Yuen
Guido Hiertz	Satoshi Obara	

When the IEEE-SA Standards Board approved this standard on 7 December 2016, it had the following membership:

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

Chuck Adams
Masayuki Ariyoshi
Stephen Dukes
Jianbin Fan
J. Travis Griffith
Gary Hoffman

Ronald W. Hotchkiss
Michael Janezic
Joseph L. Koepfinger*
Hung Ling
Kevin Lu
Annette D. Reilly
Gary Robinson

Mehmet Ulema
Yingli Wen
Howard Wolfman
Don Wright
Yu Yuan
Daidi Zhong

*Member Emeritus

Introduction

This introduction is not part of IEEE Std 802.11ai-2016, 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 1: Fast Initial Link Setup.

This amendment defines mechanisms that provide IEEE 802.11 networks with fast initial link setup methods that do not degrade the security offered by Robust Security Network Association (RSNA) already defined in IEEE Std 802.11.

Contents

2.	Normative references	18
3.	Definitions, acronyms, and abbreviations.....	20
3.1	Definitions	20
3.2	Definitions specific to IEEE Std 802.11	20
3.4	Abbreviations and acronyms	21
4.	General description	22
4.5	Overview of the services.....	22
4.5.3	Services that support the distribution service and the PCP service	22
4.5.3.3	Association.....	22
4.5.4	Access control and data confidentiality services	22
4.5.4.2	Authentication.....	22
4.5.4.3	Deauthentication	23
4.5.4.5	Key management	23
4.5.4.8	Fast BSS transition.....	24
4.10	IEEE Std 802.11 and IEEE Std 802.1X-2010	24
4.10.2	IEEE Std 802.11 usage of IEEE Std 802.1X-2010.....	24
4.10.3	Infrastructure functional model overview.....	24
4.10.3.6	AKM operations using FILS authentication	24
4.10.7	PMKSA caching	25
5.	MAC service definition	27
5.2	MAC data service specification	27
5.2.3	MA-UNITDATA.indication	27
5.2.3.3	When generated	27
6.	Layer management.....	28
6.3	MLME SAP interface	28
6.3.3	Scan.....	28
6.3.3.2	MLME-SCAN.request	28
6.3.3.3	MLME-SCAN.confirm.....	29
6.3.3.4	MLME-SCAN-STOP.request	33
6.3.5	Authenticate	33
6.3.5.2	MLME-AUTHENTICATE.request.....	33
6.3.5.3	MLME-AUTHENTICATE.confirm.....	34
6.3.5.4	MLME-AUTHENTICATE.indication	35
6.3.5.5	MLME-AUTHENTICATE.response	36
6.3.7	Associate.....	37
6.3.7.2	MLME-ASSOCIATE.request.....	37
6.3.7.3	MLME-ASSOCIATE.confirm	38
6.3.7.4	MLME-ASSOCIATE.indication	39
6.3.7.5	MLME-ASSOCIATE.response	40
6.3.8	Reassociate.....	41
6.3.8.2	MLME-REASSOCIATE.request	41
6.3.8.3	MLME-REASSOCIATE.confirm	42
6.3.8.4	MLME-REASSOCIATE.indication	43

6.3.8.5	MLME-REASSOCIATE.response	45
6.3.11	Start	46
6.3.11.2	MLME-START.request	46
6.3.105	FILS Container	48
6.3.105.1	General	48
6.3.105.2	MLME-FILSContainer.request	48
6.3.105.3	MLME-FILSContainer.confirm	49
6.3.105.4	MLME-FILSContainer.indication	49
6.3.105.5	MLME-FILSContainer.response	50
9.	Frame formats	52
9.3	Format of individual frame types	52
9.3.3	Management frames	52
9.3.3.2	Format of Management frames	52
9.3.3.3	Beacon frame format	52
9.3.3.6	Association Request frame format	53
9.3.3.7	Association Response frame format	54
9.3.3.8	Reassociation Request frame format	54
9.3.3.9	Reassociation Response frame format	55
9.3.3.10	Probe Request frame format	56
9.3.3.11	Probe Response frame format	56
9.3.3.12	Authentication frame format	57
9.4	Management and Extension frame body components	61
9.4.1	Fields that are not elements	61
9.4.1.1	Authentication Algorithm Number field	61
9.4.1.9	Status Code field	61
9.4.1.11	Action field	61
9.4.1.41	Finite field element (FFE) field	62
9.4.1.43	Finite Cyclic Group field	62
9.4.2	Elements	63
9.4.2.1	General	63
9.4.2.25	RSNE	64
9.4.2.27	Extended Capabilities element	65
9.4.2.48	Fast BSS Transition element (FTE)	65
9.4.2.171	Reduced Neighbor Report element	65
9.4.2.176	Association Delay Info element	67
9.4.2.177	CAG Number element	67
9.4.2.178	FILS Request Parameters element	68
9.4.2.179	FILS Key Confirmation element	71
9.4.2.180	FILS Session element	71
9.4.2.181	FILS Public Key element	72
9.4.2.182	AP Configuration Sequence Number (AP-CSN) element	72
9.4.2.183	FILS Indication element	72
9.4.2.184	FILS HLP Container element	75
9.4.2.185	FILS IP Address Assignment element	75
9.4.2.186	Key Delivery element	80
9.4.2.187	Differentiated Initial Link Setup element	80
9.4.2.188	FILS Wrapped Data element	82
9.4.2.189	Fragment element	82
9.4.2.190	FILS Nonce element	83
9.4.5	Access network query protocol (ANQP) elements	83
9.4.5.1	General	83
9.4.5.24	Query AP List ANQP-element	83

9.4.5.25	AP List Response ANQP-element	84
9.4.5.26	FILS Realm Information ANQP-element	85
9.4.5.27	CAG ANQP-element	85
9.6	Action frame format details	86
9.6.8	Public Action details	86
9.6.8.1	Public Action frames	86
9.6.8.36	FILS Discovery frame format	86
9.6.24	FILS Action frame details	93
9.6.24.1	General	93
9.6.24.2	FILS Container frame	93
10.	MAC sublayer functional description	94
10.5	MPDU fragmentation	94
10.6	MPDU defragmentation	94
10.27	MAC frame processing	94
10.27.1	Element fragmentation	94
10.27.12	Element defragmentation	96
11.	MLME	97
11.1	Synchronization	97
11.1.3	Maintaining synchronization	97
11.1.3.8	Multiple BSSID procedure	97
11.1.4	Acquiring synchronization, scanning	97
11.1.4.1	General	97
11.1.4.3	Active scanning	98
11.3	STA authentication and association	105
11.3.2	State transition diagram for nonmesh STAs	105
11.3.3	Frame filtering based on STA state	106
11.3.4	Authentication and deauthentication	106
11.3.4.2	Authentication—originating STA	106
11.3.4.3	Authentication—destination STA	106
11.3.5	Association, reassociation, and disassociation	107
11.3.5.1	General	107
11.3.5.2	Non-AP and non-PCP STA association initiation procedures	108
11.3.5.3	AP or PCP association receipt procedures	109
11.3.5.4	Non-AP and non-PCP STA reassociation initiation procedures	109
11.3.5.5	AP or PCP reassociation receipt procedures	109
11.25	WLAN interworking with external networks procedures	109
11.25.3.3	ANQP procedures	109
11.44	Operation under the control of a GDB	111
11.44.8	Reduced neighbor report	111
11.47	Fast Initial Link Setup (FILS) procedures	112
11.47.1	General	112
11.47.2	FILS Discovery frame generation and usage	112
11.47.2.1	FILS Discovery frame transmission	112
11.47.2.2	FILS Discovery frame reception	113
11.47.3	Higher layer setup during (re)association procedure	114
11.47.3.1	General	114
11.47.3.2	Higher layer protocol encapsulation	114
11.47.3.3	FILS IP address configuration	116
11.47.4	FILS authentication and higher layer setup capability indications	117
11.47.5	Differentiated initial link setup	118

11.47.5.1	General	118
11.47.5.2	AP procedures for differentiated initial link setup	118
11.47.5.3	Non-AP STA procedures for differentiated initial link setup	118
12.	Security	120
12.5	RSNA confidentiality and integrity protocols	120
12.5.4	Broadcast/multicast integrity protocol (BIP)	120
12.5.4.4	BIP replay protection	120
12.6	RSNA security association management	120
12.6.1	Security associations	120
12.6.1.1	Security association definitions	120
12.6.3	RSNA policy selection in an infrastructure BSS	124
12.6.10	RSNA authentication in an infrastructure BSS	124
12.6.10.1	General	124
12.6.10.3	Cached PMKSAs and RSNA key management	125
12.6.14	RSNA key management in an infrastructure BSS	126
12.6.21	RSNA rekeying	126
12.7	Keys and key distribution	126
12.7.1	Key hierarchy	126
12.7.1.2	PRF	126
12.7.1.3	Pairwise key hierarchy	127
12.7.1.7	FT key hierarchy	127
12.7.2	EAPOL-Key frames	130
12.7.4	EAPOL-Key frame notation	131
12.7.4	EAPOL-Key frame notation	131
12.7.6	4-way handshake	132
12.7.6.3	4-way handshake message 2	132
12.7.6.4	4-way handshake message 3	132
12.7.6.5	4-way handshake message 4	133
12.7.7.2	Group key handshake message 1	134
12.7.7.3	Group key handshake message 2	134
12.7.8	PeerKey handshake	135
12.7.8.5	Error reporting	138
12.7.9	TDLS PeerKey (TPK) security protocol	139
12.7.9.7	Supplicant PeerKey state machine variables	139
12.7.10	RSNA Supplicant key management state machine	139
12.7.10.3	Supplicant state machine variables	139
12.7.11	RSNA Authenticator key management state machine	139
12.7.11.3	Authenticator state machine variables	139
12.7.11.4	Authenticator state machine procedures	139
12.12	Authentication for FILS	140
12.12.1	General	140
12.12.2	FILS authentication protocol	140
12.12.2.1	General	140
12.12.2.2	Discovery of a FILS capable AP	140
12.12.2.3	Key establishment with FILS Shared Key authentication	141
12.12.2.4	Key establishment with FILS Public Key authentication	145
12.12.2.5	Key establishment with FILS authentication	147
12.12.2.6	Key confirmation with FILS authentication	148
12.12.2.7	AEAD cipher mode for FILS	152
13.	Fast BSS transition	153

13.2 Key holders	153
13.2.2 Authenticator key holders	153
13.2.3 Supplicant key holders	153
13.2.4 FT initial mobility domain association over FILS in an RSN	153
Annex B (normative) Protocol Implementation Conformance Statement (PICS) proforma	156
B.2.2 General abbreviations for Item and Support columns	156
B.4.3 IUT configuration	156
B.4.27 FILS features	156
Annex C (normative) ASN.1 encoding of the MAC and PHY MIB	158
C.3 MIB detail	158

Tables

Table 9-27—Beacon frame body	52
Table 9-27—Beacon frame body	53
Table 9-29—Association Request frame body	53
Table 9-30—Association Response frame body	54
Table 9-31—Reassociation Request frame body	54
Table 9-32—Reassociation Response frame body	55
Table 9-33—Probe Request frame body	56
Table 9-34—Probe Response frame body	56
Table 9-34—Probe Response frame body	56
Table 9-35—Authentication frame body	57
Table 9-35—Authentication frame body	58
Table 9-36—Presence of fields and elements in Authentication frames	59
Table 9-46—Status codes	61
Table 9-47—Category values	61
Table 9-77—Element IDs	63
Table 9-133—AKM suite selectors	64
Table 9-135—Extended Capabilities field	65
Table 9-258a—TBTT Information field	66
Table 9-262a—BSS Delay Criterion subfield	70
Table 9-262b—PHY Support Criterion subfield	70
Table 9-262c—Key Type and Public Key Indicator subfields	74
Table 9-262d—IPv4 subfield settings	76
Table 9-262e—IPv6 subfield settings	76
Table 9-262f—IP Address Response Control subfield with B0 = 0	78
Table 9-262g—IP Address Response Control subfield with B0 = 1	78
Table 9-262h—DNS Info Control subfield settings	79
Table 9-262i—MAC Address Filter field	82
Table 9-271—ANQP-element definitions	83
Table 9-307—Public Action field values	86
Table 9-325a—FILS Discovery frame format	86
Table 9-325b—BSS Operating Channel Width	89
Table 9-325c—Maximum Number of Spatial Streams	90
Table 9-325d—PHY Index subfield	90
Table 9-325e—FILS Minimum Rate	91
Table 9-325f—Cipher suite selector definitions	92
Table 9-325g—AKM suite selector definitions	92
Table 9-421a—FILS Action frame values	93
Table 11-15—ANQP usage	110
Table 12-8—Integrity and key-wrap algorithms	131

Figures

Figure 4-29a—FILS authentication using Authentication Server	25
Figure 9-583—TBTT Information field format	66
Figure 9-589a—Association Delay Info element format	67
Figure 9-589b—CAG Number element format	68
Figure 9-589c—CAG Tuple field.....	68
Figure 9-589d—FILS Request Parameters element format	68
Figure 9-589e—Parameter Control Bitmap field	69
Figure 9-589f—FILS Criteria field.....	69
Figure 9-589g—FILS Key Confirmation element format	71
Figure 9-589h—FILS Session element format	71
Figure 9-589i—FILS Public Key element format	72
Figure 9-589j—AP-CSN element format	72
Figure 9-589l—FILS Information field definition	73
Figure 9-589k—FILS Indication element format	73
Figure 9-589m—Realm Identifier field	74
Figure 9-589n—Public Key Identifier field	74
Figure 9-589o—FILS HLP Container element format	75
Figure 9-589p—FILS IP Address Assignment element format	75
Figure 9-589q— IP Address Data field for request format	76
Figure 9-589r—IP Address Request Control subfield format	76
Figure 9-589s—IP Address Data field format for response	77
Figure 9-589t—DNS Info Control subfield format	79
Figure 9-589u—Key Delivery element format.....	80
Figure 9-589v—Differentiated Initial Link Setup element format.....	80
Figure 9-589w—FILSC Type field format	81
Figure 9-589x—FILS User Priority field format	81
Figure 9-589y—MAC Address Filter field	81
Figure 9-589z—FILS Wrapped Data element format	82
Figure 9-589aa—Fragment element format	82
Figure 9-589ab—FILS Nonce element format.....	83
Figure 9-628a—Query AP List ANQP-element format.....	84
Figure 9-628b—AP List field format	84
Figure 9-628c—AP List Response ANQP-element format.....	84
Figure 9-628d—FILS Realm Information ANQP-element format	85
Figure 9-628e—CAG ANQP-element format	85
Figure 9-687a—FILS Discovery Information field format	87
Figure 9-687b—FILS Discovery Frame Control subfield format	87
Figure 9-687c—FD Capability subfield format	89
Figure 9-687d—Format of the FD RSN Information subfield	91
Figure 9-687e—Mobility Domain subfield format	92
Figure 9-740a—FILS Container frame format	93
Figure 10-40a—Example of the element fragmentation without Element ID Extension	95
Figure 10-40b—Example of the element fragmentation with Element ID Extension	95
Figure 11-4a—Active scanning by a non-DMG STA with a probe request addressed to an individual address	100
Figure 11-4b —Active scanning by a non-DMG STA with a probe request addressed to wildcard BSSID	100
Figure 11-13—Relationship between state and services between a given pair of nonmesh STAs	105
Figure 12-31—FT key hierarchy at an Authenticator	129
Figure 12-54—FILS Shared Key authentication	142
Figure 13-1a—FT initial mobility domain association using FILS authentication in an RSN	154

**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 1: Fast Initial Link Setup

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 instructions specify the location of the change and describes what is being changed by using ~~striketrough~~ (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.

2. Normative references

Insert the following references into Clause 2 in alphanumeric order:

FIPS 186-4, Digital Signature Standard (DSS).

IETF RFC 2131, Dynamic Host Configuration Protocol, March 1997.

IETF RFC 3279, Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, April 2002.

IETF RFC 3315, Dynamic Host Configuration Protocol for IPv6 (DHCPv6), July 2003.

IETF RFC 3447, Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specification Version 2.1, February 2003.

IETF RFC 3490, Internationalizing Domain Names in Applications (IDNA), March 2003.

IETF RFC 4862, IPv6 Stateless Address Autoconfiguration, September 2007.

IETF RFC 5116, An Interface and Algorithms for Authenticated Encryption, January 2008.

IETF RFC 5280, Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, May 2008.

IETF RFC 5295, Specification for the Derivation of Root Keys from an Extended Master Session Key (EMSK), August 2008.

IETF RFC 5480, Elliptic Curve Cryptography Subject Public Key Information, March 2009.

IETF RFC 6696, EAP Extensions for the EAP Re-authentication Protocol (ERP), July 2012.

IETF RFC 6942, Diameter Support for the EAP Re-authentication Protocol (ERP), May 2013.

ISO/IEC 14888-3:2006, Information technology - Security techniques-Digital signatures with appendix-Part 3: Discrete logarithm based mechanisms.

NIST Special Publication 800-56A R2, Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography, May 2013.

3. Definitions, acronyms, and abbreviations

3.1 Definitions

Insert the following new definitions into 3.1 in alphabetic order:

authenticated encryption with associated data (AEAD): A cipher mode that performs authenticated encryption of a plain text, with associated data that is authenticated but not encrypted.

certificate authority (CA): An entity that vouches for the binding between a device's identity, its public key, and associated keying material (such as key validity period and key usage).

perfect forward secrecy (PFS): A property of a key agreement protocol that protects a session key derived from a set of long-term public and private keys from being compromised if one of the (long-term) private keys is compromised in the future.

trusted third party (TTP): An entity that is relied upon to vouch for two parties in a pairwise authentication protocol.

3.2 Definitions specific to IEEE Std 802.11

Insert the following new definitions into 3.2 in alphabetic order:

Extensible Authentication Protocol (EAP) reauthentication protocol (EAP-RP): A protocol, using the EAP framework, that allows single round trip reauthentication with an Authentication Server after an initial EAP authentication.

NOTE—IETF RFC 6696 uses “ERP” for the abbreviation of EAP reauthentication protocol; whereas, IEEE Std 802.11 uses “EAP-RP” because “ERP” stands for “Extended Rate PHY” in IEEE Std 802.11.

fast initial link setup (FILS): A collection of mechanisms that enable IEEE Std 802.11 networks to minimize initial link setup time.

fast initial link setup category (FILSC): A value that indicates the priority category of the station (STA) for fast initial link setup.

fast initial link setup station (FILS STA): A station that implements fast initial link setup (FILS) and for which dot11FILSActivated is true.

fast initial link setup (FILS) association: A type of association used in fast initial link setup.

fast initial link setup (FILS) authentication: A type of authentication used in fast initial link setup.

integrity check key (ICK): A key used to integrity check FILS Authentication frames.

link setup: The process of discovering an extended service set (ESS), (secure) association and authentication, and gaining the ability to send higher layer [e.g., Internet Protocol (IP)] traffic with a valid higher layer address through an access point (AP).

upstream network: An integrated local area network (LAN) to which an access point (AP) is connected through a portal.

Change the following definitions in 3.2:

group temporal key security association (GTKSA): The context resulting from a successful group temporal key (GTK) distribution exchange via either a group key handshake, ~~or a 4-way handshake,~~ or fast initial link setup (FILS) authentication.

pairwise transient key security association (PTKSA): The context resulting from a successful 4-way handshake between a peer and Authenticator or from a successful fast initial link setup (FILS) authentication.

pre-robust security network association (pre-RSNA): The type of association used by a pair of stations (STAs) if the procedure for establishing authentication or association between them did not include the 4-way handshake, was not fast initial link setup (FILS) authentication, and did not use FT protocol.

robust security network association (RSNA): The type of association used by a pair of stations (STAs) if the procedure to establish authentication or association between them includes the 4-way handshake or FT protocol, or is fast initial link setup (FILS) authentication. Note that existence of an RSNA between two STAs does not of itself provide robust security. Robust security is provided when all STAs in the network use RSNAs.

robust security network association (RSNA) key management: Key management that includes the 4-way handshake, the group key handshake, authenticated mesh peering exchange, mesh group key handshake, and the PeerKey handshake. If fast basic service set (BSS) transition (FT) is enabled, the FT 4-way handshake and FT authentication sequence are also included. If fast initial link setup (FILS) is enabled, FILS authentication is also included.

3.4 Abbreviations and acronyms

Insert the following new abbreviations/acronyms into 3.4:

AEAD	authenticated encryption with associated data
ANO	access network options
AP-CSN	AP configuration sequence number
CA	certificate authority
CAG	Common Advertisement Group
EAP-RP	EAP reauthentication protocol
FD	FILS discovery
FILS	fast initial link setup
FILSC	fast initial link setup category
HLP	higher layer protocol
ICK	FILS integrity check key
PFS	perfect forward secrecy
TTP	trusted third party

4. General description

4.5 Overview of the services

4.5.3 Services that support the distribution service and the PCP service

4.5.3.3 Association

Change the last paragraph of 4.5.3.3 as follows:

A STA learns what APs are present and what operational capabilities are available from each of those APs and then invokes the association service to establish an association. A FILS STA is able to discover, authenticate and associate with the AP with reduced number of frame transmissions. For details of how a STA learns about what APs are present, see 11.1.4.

4.5.4 Access control and data confidentiality services

4.5.4.2 Authentication

Change 4.5.4.2 as follows:

IEEE 802.11 authentication operates at the link level between IEEE 802.11 STAs. IEEE Std 802.11 does not provide either end-to-end (MSDU origin to MSDU destination) or user-to-user authentication.

IEEE Std 802.11 attempts to control LAN access via the authentication service. IEEE 802.11 authentication is an SS. This service might be used by all STAs to establish their identity to STAs with which they communicate, in both ESSs and IBSSs. If a mutually acceptable level of authentication has not been established between two STAs, an association is not established.

IEEE Std 802.11 defines ~~five~~^{four} IEEE 802.11 authentication methods: Open System authentication, Shared Key authentication, FT authentication, ~~and simultaneous authentication of equals (SAE), and FILS authentication.~~ Open System authentication admits any STA to the DS. Shared Key authentication relies on WEP to demonstrate knowledge of a WEP encryption key. FT authentication relies on keys derived during the initial mobility domain association to authenticate the stations as defined in Clause 13. SAE authentication uses finite field cryptography to prove knowledge of a shared password. FILS authentication allows for faster connection to the network for FILS non-AP STAs by providing authentication, association, and key confirmation information in an efficient number of frame exchanges (see 4.10.3.6). The IEEE 802.11 authentication mechanism also allows definition of new authentication methods.

An RSNA might support SAE authentication, FILS authentication, or both. An RSNA also supports authentication based on IEEE Std 802.1X-2010, or preshared keys (PSKs) after Open System authentication. IEEE 802.1X authentication utilizes the EAP to authenticate STAs and the AS with one another. This standard does not specify an EAP method that is mandatory to implement. See 12.6.5 for a description of the IEEE 802.1X authentication and PSK usage within an IEEE 802.11 IBSS.

In an RSNA, IEEE 802.1X Supplicants and Authenticators exchange protocol information via the IEEE 802.1X Uncontrolled Port. The IEEE 802.1X Controlled Port is blocked from passing general data traffic between two STAs until an IEEE 802.1X authentication procedure completes successfully over the IEEE 802.1X Uncontrolled Port.

SAE authentication ~~or~~ and Open System IEEE 802.11 authentication ~~is~~ are used by non-DMG STAs in an RSN for an infrastructure BSS. ~~FILS authentication may be used by FILS STAs in an RSN for an infrastructure BSS.~~ SAE authentication, Open System IEEE 802.11 authentication, or no IEEE 802.11 authentication is used in an RSN for an IBSS. SAE authentication is used ~~in~~ for an MBSS. ~~In a An RSNA, disallows the use of Shared Key authentication is not used.~~ In an RSN for DMG BSS, Open System IEEE 802.11 authentication is not used (12.2.4).

4.5.4.3 Deauthentication

Change 4.5.4.3 as follows:

The deauthentication service is invoked when an existing Open System, Shared Key, ~~FT, or SAE, or FILS~~ authentication is to be terminated. Deauthentication is a SS.

In an ESS, because authentication is a prerequisite for association, the act of deauthentication causes the STA to be disassociated. The deauthentication service can be invoked by either authenticated party (non-AP STA or AP). Deauthentication is not a request; it is a notification. The association at the transmitting STA is terminated when the STA sends a deauthentication notice to an associated STA. Deauthentication, and if associated, disassociation can not be refused by the receiving STA except when management frame protection is negotiated and the message integrity check fails.

~~In an RSN ESS, Open System IEEE Std 802.11 authentication is required.~~ In an RSN ESS, deauthentication results in termination of any association for the deauthenticated STA. It also results in the IEEE 802.1X Controlled Port for that STA, if used for this association, being disabled and deletes the pairwise transient key security association (PTKSA). The deauthentication notification is provided to IEEE Std 802.1X-2010 via the MAC layer.

In an RSNA, deauthentication also destroys any related pairwise transient key security association (PTKSA), group temporal key security association (GTKSA), station-to-station link (STSL) master key security association (SMKSA), STSL transient key security association (STKSA), TPK security association (TPKSA), integrity group temporal key security association (IGTKSA), 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.

In an RSN IBSS, Open System authentication is optional, but a STA is required to recognize Deauthentication frames. Deauthentication results in the IEEE 802.1X Controlled Port for that STA being disabled and deletes the PTKSA.

4.5.4.5 Key management

Change 4.5.4.5 as follows:

The enhanced data confidentiality, data authentication, and replay protection mechanisms require fresh cryptographic keys and corresponding security associations. The procedures defined in this standard provide fresh keys by means of various protocols and handshakes, ~~called the 4-way handshake, FT 4-way handshake, FT protocol, FT resource request protocol, and group key handshake.~~

4.5.4.8 Fast BSS transition

Change 4.5.4.8 as follows:

The FT mechanism defines a means for a STA to set up security and QoS parameters prior to reassociation to a new AP. This mechanism allows time-consuming operations to be removed from the time-critical reassociation process. When FILS authentication is used during a handover across mobility domains, the overhead incurred during the FT initial mobility domain association in an RSN is further reduced.

4.10 IEEE Std 802.11 and IEEE Std 802.1X-2010

4.10.2 IEEE Std 802.11 usage of IEEE Std 802.1X-2010

Change the second paragraph of 4.10.2 as follows:

IEEE Std 802.11 depends upon IEEE Std 802.1X-2010 and various IEEE 802.11 protocols and handshakes ~~the 4-way handshake, FT 4-way handshake, FT protocol, FT resource request protocol, and group key handshake,~~ described in Clause 12 and Clause 13, to establish and change cryptographic keys. Keys are established after authentication has completed. Keys might change for a variety of reasons, including expiration of an IEEE 802.1X authentication timer, key compromise, danger of compromise, or policy.

4.10.3 Infrastructure functional model overview

Insert new subclause 4.10.3.6 as follows:

4.10.3.6 AKM operations using FILS authentication

4.10.3.6.1 General

FILS authentication allows faster link setup to the network by performing authentication, association, and key confirmation using four frames—two Authentication frames, one (Re)Association Request frame, and one (Re)Association Response frame.

The following three FILS authentication methods are defined:

- a) FILS Shared Key authentication performed without perfect forward security (PFS)
- b) FILS Shared Key authentication performed with PFS
- c) FILS Public Key authentication with PFS

FILS Shared Key authentication with and without PFS is described in 4.10.3.6.2.

FILS Public Key authentication exchange is described in 4.10.3.6.3.

4.10.3.6.2 AKM operations using FILS Shared Key authentication

A non-AP STA and an Authentication Server (AS) using FILS Shared Key authentication verify mutual possession of a shared key (rRK) (as defined in IETF RFC 5295 and IETF RFC 6696) using Extensible Authentication Protocol (EAP) reauthentication protocol (EAP-RP) signaling. EAP-RP signaling is encapsulated using FILS wrapped data in an Authentication frame as shown in Figure 4-29a. A valid rRK is derived using

a prior full authentication using the full EAP as defined in 4.10.3.2. This rRK can be used for multiple runs of EAP-RP authentications as specified in IETF RFC 5295 and IETF RFC 6696.

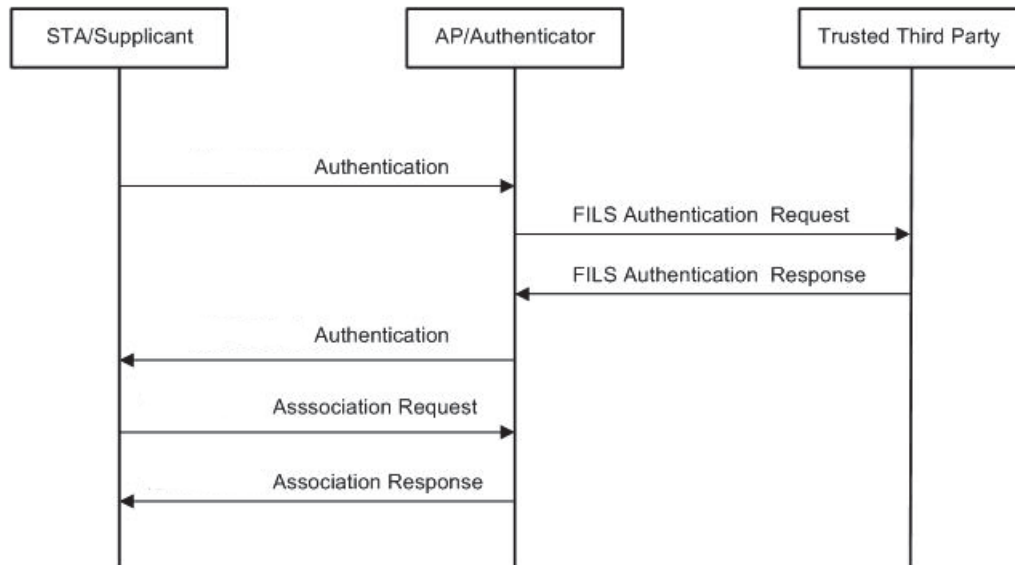


Figure 4-29a—FILS authentication using Authentication Server

4.10.3.6.3 AKM operations using FILS Public Key authentication

When using FILS Public Key authentication, it is assumed that both STAs using FILS have either:

- Obtained a public key certificate from a certificate authority (CA) and are capable of verifying each other's certificate during execution of FILS authentication procedures; or
- A priori knowledge of, and trust in, an uncertified public key.

The manner in which trust is obtained in certificates is outside the scope of this standard.

4.10.7 PMKSA caching

Change 4.10.7 as follows:

The Authenticator and Supplicant can cache PMKSAs, which include the IEEE 802.1X state. A PMKSA can be deleted from the cache for any reason and at any time.

The STA can supply a list of PMK identifiers in the (Re)Association Request frame or first FILS Authentication frame. Each key identifier names a PMKSA; the PMKSA can contain a single PMK. The Authenticator can specify the selected PMK key identifier in message 1 of the 4-way handshake or the second FILS Authentication frame. The selection of the key identifiers to be included by the STA and Authenticator within the (Re)Association Request frame and message 1 of the 4-Way handshake is out of the scope of this standard.

A FILS STA performing FILS authentication can supply a list of PMK identifiers in its initial Authentication frame. Each PMK identifier names a PMKSA; the PMKSA contains a single PMK. If the AP has retained an identified PMKSA, it can facilitate a faster connection by identifying a single PMKSA in the Authentication frame it transmits. The STA and AP can then use the PMK from the cached PMKSA to authenticate. FILS APs that support PMK caching may identify themselves using a cache identifier. A FILS STA that has successfully established a PMKSA at an AP identifying a particular cache identifier can attempt to use PMK caching in a subsequent attempt with any AP that uses the same cache identifier.

5. MAC service definition

5.2 MAC data service specification

5.2.3 MA-UNITDATA.indication

5.2.3.3 When generated

Change 5.2.3.3 as follows:

The MA-UNITDATA.indication primitive is passed from the MAC sublayer entity to the LLC sublayer entity or entities to indicate the arrival of a frame at the local MAC sublayer entity. Frames are reported only if they are validly formatted at the MAC sublayer, received without error, received with valid (or null) security and integrity information, and their destination address designates the local MAC sublayer entity. The MA-UNITDATA.indication primitive might also be passed from the MAC sublayer entity, in coordination with the MAC sublayer management entity, to the LLC sublayer entity to indicate the arrival of a FILS higher layer protocol (HLP) Container element.

6. Layer management

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 parameter list in 6.3.3.2.2 as follows:

The primitive parameters are as follows:

```
MLME-SCAN.request(  
    BSSType,  
    BSSID,  
    SSID,  
    ScanType,  
    ProbeDelay,  
    ChannelList,  
    MinChannelTime,  
    MaxChannelTime,  
    RequestInformation,  
    SSID List,  
    ChannelUsage,  
    AccessNetworkType,  
    HESSID,  
    MeshID,  
    DiscoveryMode,  
    FILSRequestParameters,  
    ReportingOption,  
    APConfigurationSequenceNumber,  
    VendorSpecificInfo  
)
```

Insert the following rows before the VendorSpecificInfo row in the parameter table in 6.3.3.2.2:

Name	Type	Valid range	Description
FILSRequestParameters	As defined in 9.4.2.178	As defined in 9.4.2.178	Used in determining whether to transmit a Probe Response frame. This parameter is optionally present if dot11FILSActivated is true; otherwise not present.
ReportingOption	Enumeration	IMMEDIATE, CHANNEL_SPECIFIC, AT_END	Indicates the result reporting mode as described in 11.1.4. This parameter is optionally present if dot11FILSActivated is true; otherwise not present.
APConfigurationSequenceNumber	Integer	As defined in 9.4.2.182	Indicates the configuration sequence number for the static information fields and elements as described in 11.1.4.3.7. This parameter is optionally present if dot11FILSActivated is true and BSSID is an individual MAC address; otherwise not present.

6.3.3.3 MLME-SCAN.confirm

6.3.3.3.1 Function

Change the first paragraph of 6.3.3.1 as follows:

This primitive returns the descriptions of the set of BSSs detected by the scan process. Multiple MLME-SCAN.confirm primitives can be issued when the value of the ReportingOption parameter in the MLME-SCAN.request primitive is CHANNEL_SPECIFIC or IMMEDIATE. When the value of the ReportingOption parameter is AT_END, or the ReportingOption parameter is not present, a single MLME-SCAN.confirm primitive is issued.

6.3.3.3.2 Semantics of the service primitive

Change the primitive parameter list in 6.3.3.3.2 as follows:

The primitive parameters are as follows:

```
MLME-SCAN.confirm(
    BSSDescriptionSet,
    BSSDescriptionFromMeasurementPilotSet,
    BSSDescriptionFromFDSet,
    ResultCode,
    VendorSpecificInfo
)
```

Change the table in 6.3.3.3.2 as follows:

Name	Type	Valid range	Description
BSSDescriptionSet	Set of BSSDescriptions	N/A	The BSSDescriptionSet is returned to indicate the results of the scan request. It is a set containing zero or more instances of a BSSDescription.
BSSDescriptionFromMeasurementPilotSet	Set of BSSDescriptionFromMeasurementPilots	N/A	The BSSDescriptionFromMeasurementPilotSet is returned to indicate the results of the scan request derived from measurement pilots. It is a set containing zero or more instances of a BSSDescriptionFromMeasurementPilot. Present if dot11RMMeasurementPilotActivated is nonzero; otherwise not present.
<u>BSSDescriptionFromFDSet</u>	<u>Set of BSSDescriptionFromFDs</u>	<u>N/A</u>	<u>The BSSDescriptionFromFDSet is returned to indicate the results of the scan request derived from FILS Discovery frames. It is a set containing zero or more instances of a BSSDescriptionFromFD. Present if dot11FILSActivated is true; otherwise not present.</u>
ResultCode	Enumeration	SUCCESS, <u>INTERMEDIATE_SCAN_RESULT</u> , NOT_SUPPORTED	Indicates the result of the MLME-SCAN.confirm primitive. <u>The INTERMEDIATE_SCAN_RESULT is used to report the discovered BSSs when the value of the ReportingOption parameter in the MLME-SCAN.request primitive is CHANNEL_SPECIFIC or IMMEDIATE and is valid if dot11FILSActivated is true.</u>
VendorSpecificInfo	A set of elements	As defined in 9.4.2.26	Zero or more elements.

Insert the following rows at the end of the second table in 6.3.3.3.2:

Name	Type	Valid range	Description	IBSS adoption
CAG Number	As defined in 9.4.2.177	As defined in 9.4.2.177	One or more Common Advertisement Group (CAG) tuples. Each CAG Tuple describes the CAG Version, Scope, and Partial Advertisement Protocol ID. This parameter is optionally present when dot11FILSActivated is true; otherwise not present.	Do not adopt.
Differentiated Initial Link Setup	As defined in 9.4.2.187	As defined in 9.4.2.187	Contains the values from the Differentiated Initial Link Setup element. It is optionally present when dot11FILSActivated is true and if such an element was present in the Probe Response or Beacon frame; otherwise not present.	Do not adopt.

Insert the following text and table to the end of 6.3.3.3.2:

The BSSDescriptionFromFDSet parameter is present if dot11FILSActivated is true; otherwise, it is not present. Each BSSDescriptionFromFD consists of the parameters shown in the following table:

Name	Type	Valid range	Description
BSSID	MAC address	N/A	The BSSID of the found BSS.
SSID	Octet String	As defined in 9.4.2.2	The SSID of the found BSS. This parameter is present if the Short SSID Indicator in the received FILS Discovery frame is equal to 0.
Short SSID	Integer	As defined in the 9.4.2.171	The Short SSID of the found BSS. This parameter is present if the Short SSID Indicator in the received FILS Discovery frame is equal to 1.
FD Capability	As defined in 9.6.8.36	As defined in 9.6.8.36	The FD Capability contains the capabilities and operational indications of the BSS. This parameter is optional.
Operating class	Integer	As defined in 9.4.1.37	The operating class of the advertised BSS.
Access Network Options	As defined in 8.4.2.91	As defined in 8.4.2.91	The advertised access network options of the BSS. This parameter is optional.

Name	Type	Valid range	Description
Primary Channel	Integer	1–255	The Primary Channel of the advertised BSS. The Primary Channel is defined within the indicated Operating Class as shown in Annex E. This parameter is optional.
FD RSN Information	As defined in 9.6.8.36	As defined in 9.6.8.36	The information for robust security network. This parameter is optional.
Channel Center Frequency Segment 1	Integer	1–255	The channel frequency index of the 80 MHz channel of frequency segment 1 when the BSS operates on an 80+80 MHz operating channel width. This parameter is optional.
AP-CSN	Integer	As defined in 9.4.2.182	The value of the Configuration Sequence Number in the found BSS. This parameter is optional.
AP's next TBTT Offset	Integer	As defined in 9.6.8.36	The information of next target beacon transmission time of the found BSS. This parameter is optional.
Reduced Neighbor Report	As defined in 9.4.2.171	As defined in 9.4.2.171	The information of the Reduced Neighbor Information field of the received FILS Discovery frame. This parameter is optional.
FILS Indication	As defined in 9.4.2.183	As defined in 9.4.2.183	The information related to FILS authentication and upper layer set up capabilities of the found AP. This parameter is optional.

6.3.3.3.3 When generated

Change 6.3.3.3.3 as follows:

This primitive is generated by the MLME to report the operating environment of the STA. It is issued after receiving an MLME-SCAN.request primitive or, if dot11FILSActivated is true, after receiving an MLME-SCAN-STOP.request primitive following an MLME-SCAN.request primitive. as a result of an MLME-SCAN.request primitive to ascertain the operating environment of the STA.

6.3.3.3.4 Effect of receipt

Change 6.3.3.3.4 as follows:

The SME is notified of the results of the scan procedure. If dot11FILSActivated is true, these results might be intermediate results, according to the value of ResultCode.

Insert new subclause 6.3.3.4 as follows:

6.3.3.4 MLME-SCAN-STOP.request

6.3.3.4.1 Function

This primitive terminates any ongoing scan.

6.3.3.4.2 Semantics of the service primitive

The primitive has no parameters.

6.3.3.4.3 When generated

This primitive is generated by the SME in order to stop all ongoing active or passive scan processes in the STA.

6.3.3.4.4 Effect of receipt

This request terminates all ongoing scan procedures.

6.3.5 Authenticate

6.3.5.2 MLME-AUTHENTICATE.request

6.3.5.2.2 Semantics of the service primitive

Change the primitive parameter list in 6.3.5.2.2 as follows:

The primitive parameters are as follows:

```
MLME-AUTHENTICATE.request(  
    PeerSTAAddress,  
    AuthenticationType,  
    AuthenticateFailureTimeout,  
    Content of FT Authentication elements,  
    Content of SAE Authentication frame,  
    Multi-band local,  
    Multi-band peer,  
    Content of FILS Authentication frame,  
    VendorSpecificInfo  
)
```

Change one row and insert one new row before the VendorSpecificInfo row in the parameter table in 6.3.5.2.2 as follows:

Name	Type	Valid range	Description
AuthenticationType	Enumeration	OPEN_SYSTEM, SHARED_KEY, FAST_BSS_TRANSITION, SAE, <u>FILS_SHARED_KEY_WITHOUT_PFS,</u> <u>FILS_SHARED_KEY_WITH_PFS,</u> <u>FILS_PUBLIC_KEY</u>	Specifies the type of authentication algorithm to use during the authentication process.
<u>Content of FILS Authentication frame</u>	<u>Sequence of elements and fields</u>	<u>As defined in 9.4.1.43,</u> <u>9.4.1.41, 9.4.2.25,</u> <u>9.4.2.180, 9.4.2.188,</u> <u>and 9.4.2.190</u>	<u>The set of elements and fields to be included in the first message of the FILS authentication sequence, as described in 12.12. Present if AuthenticationType indicates FILS_SHARED_KEY WITHOUT PFS, FILS_SHARED_KEY WITH PFS, or FILS_PUBLIC_KEY; otherwise not present.</u>

6.3.5.3 MLME-AUTHENTICATE.confirm

6.3.5.3.2 Semantics of the service primitive

Change the primitive parameter list in 6.3.5.3.2 as follows:

The primitive parameters are as follows:

```
MLME-AUTHENTICATE.confirm(
    PeerSTAAddress,
    AuthenticationType,
    ResultCode,
    Content of FT Authentication elements,
    Content of SAE Authentication frame,
    Multi-band local,
    Multi-band peer,
    Content of FILS Authentication frame,
    VendorSpecificInfo
)
```

Change one row and insert a new row before the VendorSpecificInfo row in the parameter table in 6.3.5.3.2 as follows:

Name	Type	Valid range	Description
AuthenticationType	Enumeration	OPEN_SYSTEM, SHARED_KEY, FAST_BSS_TRANSITION, SAE_FILS_SHARED_KEY_WITHOUT_PFS, FILS_SHARED_KEY_WITH_PFS, FILS_PUBLIC_KEY	Specifies the type of authentication algorithm to use during the authentication process.
<u>Content of FILS Authentication frame</u>	<u>Sequence of elements and fields</u>	<u>As defined in 9.4.1.43, 9.4.1.41, 9.4.2.25, 9.4.2.176, 9.4.2.180, 9.4.2.188, and 9.4.2.190</u>	<u>The set of elements and fields included in the second message of the FILS authentication sequence, as described in 12.12. Present if AuthenticationType indicates FILS_SHARED_KEY_WITHOUT_PFS, FILS_SHARED_KEY_WITH_PFS, or FILS_PUBLIC_KEY; otherwise not present.</u>

6.3.5.4 MLME-AUTHENTICATE.indication

6.3.5.4.2 Semantics of the service primitive

Change the primitive parameter list in 6.3.5.4.2 as follows:

The primitive parameters are as follows:

```
MLME-AUTHENTICATE.indication(
    PeerSTAAddress,
    AuthenticationType,
    Content of FT Authentication elements,
    Content of SAE Authentication frame,
    Multi-band local,
    Multi-band peer,
    Content of FILS Authentication frame.
    VendorSpecificInfo
)
```

Change one row and insert a new row before the VendorSpecificInfo row in the parameter table in 6.3.5.4.2 as follows:

Name	Type	Valid range	Description
AuthenticationType	Enumeration	OPEN_SYSTEM, SHARED_KEY, FAST_BSS_TRANSITION, SAE, <u>FILS_SHARED_KEY_WITHOUT_PFS,</u> <u>FILS_SHARED_KEY_WITH_PFS,</u> <u>FILS_PUBLIC_KEY</u>	Specifies the type of authentication algorithm that was used during the authentication process.
<u>Content of FILS Authentication frame</u>	<u>Sequence of elements and fields</u>	<u>As defined in 9.4.1.43,</u> <u>9.4.1.41, 9.4.2.25, 9.4.2.176,</u> <u>9.4.2.180, 9.4.2.188, and</u> <u>9.4.2.190</u>	<u>The set of elements and fields included in the first message of the FILS authentication sequence, as described in 12.12. Present if AuthenticationType indicates FILS_SHARED_KEY_WITHOUT_PFS, FILS_SHARED_KEY_WITH_PFS, or FILS_PUBLIC_KEY; otherwise not present.</u>

6.3.5.5 MLME-AUTHENTICATE.response

6.3.5.5.2 Semantics of the service primitive

Change the primitive parameter list in 6.3.5.5.2 as follows:

The primitive parameters are as follows:

```
MLME-AUTHENTICATE.response(
    PeerSTAAddress,
    ResultCode,
    Content of FT Authentication elements,
    Content of SAE Authentication frame,
    Multi-band local,
    Multi-band peer,
    Content of FILS Authentication frame,
    VendorSpecificInfo
)
```

Insert a new row before the VendorSpecificInfo row in the parameter table in 6.3.5.5.2 as follows:

Name	Type	Valid range	Description
<u>Content of FILS Authentication frame</u>	<u>Sequence of elements and fields</u>	<u>As defined in 9.4.1.43, 9.4.1.41, 9.4.2.25, 9.4.2.180, 9.4.2.188, and 9.4.2.190</u>	<u>The set of elements and fields to be included in the second message of the FILS authentication sequence, as described in 12.12. Present if AuthenticationType indicates FILS SHARED KEY WITHOUT PFS, FILS SHARED KEY WITH PFS, or FILS PUBLIC KEY; otherwise not present.</u>

6.3.7 Associate

6.3.7.2 MLME-ASSOCIATE.request

6.3.7.2.2 Semantics of the service primitive

Change the primitive parameter list in 6.3.7.2.2 as follows:

The primitive parameters are as follows:

```
MLME-ASSOCIATE.request(
    PeerSTAAddress,
    ListenInterval,
    Supported Channels,
    RSN,
    QoSCapability,
    Content of FT Authentication elements,
    SupportedOperatingClasses,
    SM Power Save,
    QoSTrafficCapability,
    TIMBroadcastRequest,
    EmergencyServices,
    DMG Capabilities,
    Multi-band local,
    Multi-band peer,
    MMS,
    FILSHLPContainer,
    FILSIPAddressAssignment,
    VendorSpecificInfo
)
```

Insert two new rows before the VendorSpecificInfo row in the parameter table in 6.3.7.2.2 as follows:

Name	Type	Valid range	Description
FILSHLPContainer	As defined in 9.4.2.184	As defined in 9.4.2.184	A set of elements containing encapsulated data of higher layer protocol frames (e.g., DHCP message) that is transported in FILS association. The parameter is optionally present if dot11FILSActivated is true; otherwise not present.
FILSIPAddressAssignment	As defined in 9.4.2.185	As defined in 9.4.2.185	An explicit request for an IP address. The request is either for a new IP address or for a specified IP address. The parameter is optionally present if dot11FILSActivated is true; otherwise not present.

6.3.7.3 MLME-ASSOCIATE.confirm

6.3.7.3.2 Semantics of the service primitive

Change the primitive parameter list in 6.3.7.3.2 as follows:

The primitive parameters are as follows:

MLME-ASSOCIATE.confirm(
 ResultCode,
 CapabilityInformation,
 AssociationID,
 EDCAPParameterSet,
 RCPI of Request,
 RSNI of Request,
 RCPI of Response,
 RSNI of Response,
 RMEnabledCapabilities,
 Content of FT Authentication elements,
 SupportedOperatingClasses,
 Extended Capabilities,
 20/40 BSS Coexistence,
 TimeoutInterval,
 BSSMaxIdlePeriod,
 TIMBroadcastResponse,
 QoSMapSet,
 QMFPolicy,
 DMG Capabilities,
 Multi-band local,
 Multi-band peer,
 MMS,
 FILSHLPContainer,
 FILSIPAddressAssignment,
 KeyDelivery.

VendorSpecificInfo
)

Insert three new rows before the VendorSpecificInfo row in the parameter table in 6.3.7.3.2 as follows:

Name	Type	Valid range	Description
FILSHLPContainer	As defined in 9.4.2.184	As defined in 9.4.2.184	A set of elements containing encapsulated data of higher layer protocol (HLP) frames (e.g., DHCP message) that is transported in FILS association. The parameter is optionally present if dot11-FILSActivated is true; otherwise not present.
FILSIPAddressAssignment	As defined in 9.4.2.185	As defined in 9.4.2.185	Contains the IP address of a network layer entity associated with the STA. The parameter is optionally present if dot11-FILSActivated is true; otherwise not present.
KeyDelivery	As defined in 9.4.2.186	As defined in 9.4.2.186	Contains the KDE(s) and the Key RSC. The parameter is present if dot11FILSActivated is true; otherwise not present.

6.3.7.4 MLME-ASSOCIATE.indication

6.3.7.4.2 Semantics of the service primitive

Change the primitive parameter list in 6.3.7.4.2 as follows:

The primitive parameters are as follows:

MLME-ASSOCIATE.indication(
PeerSTAAddress,
CapabilityInformation,
ListenInterval,
SSID,
OperationalRateSet,
BSSMembershipSelectorSet,
RSN,
QoSCapability,
RCPI,
RSNI,
RMEnabledCapabilities,
Content of FT Authentication elements,
SupportedOperatingClasses,
DSERegisteredLocation,
HT Capabilities,
Extended Capabilities,
20/40 BSS Coexistence,
QoSTrafficCapability,
TIMBroadcastRequest,
EmergencyServices,
DMG Capabilities,

Multi-band local,
 Multi-band peer,
 MMS,
 VHT Capabilities,
FILSHLPContainer,
FILSIPAddressAssignment,
 VendorSpecificInfo
)

Insert two new rows before the VendorSpecificInfo row in the parameter table in 6.3.7.4.2 as follows:

Name	Type	Valid range	Description
FILSHLPContainer	As defined in 9.4.2.184	As defined in 9.4.2.184	A set of elements containing encapsulated data of higher layer protocol frames (e.g., DHCP message) that is transported in FILS association. The parameter is optionally present if dot11FILSActivated is true; otherwise not present.
FILSIPAddressAssignment	As defined in 9.4.2.185	As defined in 9.4.2.185	An explicit request for an IP address. The request is for a new IP address or a specified IP address. The parameter is optionally present if dot11FILSActivated is true; otherwise not present.

6.3.7.5 MLME-ASSOCIATE.response

6.3.7.5.2 Semantics of the service primitive

Change the primitive parameter list in 6.3.7.5.2 as follows:

The primitive parameters are as follows:

MLME-ASSOCIATE.response(
 PeerSTAAddress,
 ResultCode,
 AssociationID,
 RCPI,
 RSNI,
 RMEnabledCapabilities,
 Content of FT Authentication elements,
 SupportedOperatingClasses,
 TimeoutInterval,
 BSSMaxIdlePeriod,

TIMBroadcastResponse,
 QoSMapSet,
 Multi-band peer,
FILSHLPContainer,
FILSIPAddressAssignment,
KeyDelivery,
 VendorSpecificInfo
)

Insert three new rows before the VendorSpecificInfo row in the parameter table in 6.3.7.5.2 as follows:

Name	Type	Valid range	Description
FILSHLPContainer	As defined in 9.4.2.184	As defined in 9.4.2.184	A set of elements containing encapsulated data of higher layer protocol frames (e.g., a DHCP message) transported in FILS association. The parameter is optionally present if dot11FILSActivated is true; otherwise not present.
FILSIPAddressAssignment	As defined in 9.4.2.185	As defined in 9.4.2.185	Contains the IP address of a network layer entity associated with the STA. The parameter is optionally present if dot11FILSActivated is true; otherwise not present.
KeyDelivery	As defined in 9.4.2.186	As defined in 9.4.2.186	Contains KDE(s) and the current Key RSC. The parameter is present if dot11FILSActivated is true; otherwise 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 parameter list in 6.3.8.2.2 as follows:

The primitive parameters are as follows:

MLME-REASSOCIATE.request(
 NewPCPorAPAddress,
 ListenInterval,
 Supported Channels,
 RSN,
 QoSCapability,

Content of FT Authentication elements,
 SupportedOperatingClasses,
 SM Power Save,
 QoS Traffic Capability,
 TIM Broadcast Request,
 FMS Request,
 DMS Request,
 Emergency Services,
 DMG Capabilities,
 Multi-band local,
 Multi-band peer,
 MMS,
FILSHLPContainer,
FILSIPAddressAssignment,
 VendorSpecificInfo
)

Insert two new rows before the VendorSpecificInfo row in the parameter table in 6.3.8.2.2 as follows:

Name	Type	Valid range	Description
FILSHLPContainer	As defined in 9.4.2.184	As defined in 9.4.2.184	A set of elements containing encapsulated data of higher layer protocol frames (e.g., a DHCP message) that is transported in FILS association. The parameter is optionally present if dot11FILSActivated is true; otherwise not present.
FILSIPAddressAssignment	As defined in 9.4.2.185	As defined in 9.4.2.185	An explicit request for an IP address. The request may be for a new IP address or a specified IP address. The parameter is optionally present if dot11FILSActivated is true; otherwise not present.

6.3.8.3 MLME-REASSOCIATE.confirm

6.3.8.3.2 Semantics of the service primitive

Change the primitive parameter list in 6.3.8.3.2 as follows:

The primitive parameters are as follows:

MLME-REASSOCIATE.confirm(
 ResultCode,
 CapabilityInformation,
 AssociationID,
 EDCAPParameterSet,
 RCPI of Request,
 RSNI of Request,
 RCPI of Response,

RSNI of Response,
 RMEnabledCapabilities,
 Content of FT Authentication elements,
 SupportedOperatingClasses,
 Extended Capabilities,
 20/40 BSS Coexistence,
 TimeoutInterval,
 BSSMaxIdlePeriod,
 TIMBroadcastResponse,
 FMSResponse,
 DMSResponse,
 QoSMapSet,
 QMFPolicy,
 DMG Capabilities,
 Multi-band local,
 Multi-band peer,
 MMS,
FILSHLPContainer,
FILSIPAddressAssignment,
KeyDelivery,
 VendorSpecificInfo
)

Insert three new rows before the VendorSpecificInfo row in the parameter table in 6.3.8.3.2 as follows:

Name	Type	Valid range	Description
FILSHLPContainer	As defined in 9.4.2.184	As defined in 9.4.2.184	A set of elements containing encapsulated dataset of higher layer protocol frames (e.g., a DHCP message) that is transported in FILS association. The parameter is present if dot11FILSActivated is true; otherwise not present.
FILSIPAddressAssignment	As defined in 9.4.2.185	As defined in 9.4.2.185	Contains the IP address assigned to the STA for higher layer communication. The parameter is present if dot11FILSActivated is true; otherwise not present.
KeyDelivery	As defined in 9.4.2.186	As defined in 9.4.2.186	Contains KDE(s) and the current Key RSC. The parameter is present if dot11FILSActivated is true; otherwise not present.

6.3.8.4 MLME-REASSOCIATE.indication

6.3.8.4.2 Semantics of the service primitive

Change the primitive parameter list in 6.3.8.4.2 as follows:

The primitive parameters are as follows:

MLME-REASSOCIATE.indication(
 PeerSTAAddress,
 CurrentAPAddress,
 CapabilityInformation,
 ListenInterval,
 SSID,
 OperationalRateSet,
 BSSMembershipSelectorSet,
 RSN,
 QoSCapability,
 RCPI,
 RSNI,
 RMEnabledCapabilities,
 Content of FT Authentication elements,
 SupportedOperatingClasses,
 DSERegisteredLocation,
 HT Capabilities,
 Extended Capabilities,
 20/40 BSS Coexistence,
 QoSTrafficCapability,
 TIMBroadcastRequest,
 FMSRequest,
 DMSRequest,
 EmergencyServices,
 DMG Capabilities,
 Multi-band local,
 Multi-band peer,
 MMS,
 VHT Capabilities,
 FILSHLPContainer,
 FILSIPAddressAssignment,
 VendorSpecificInfo
)

Insert two new rows before the VendorSpecificInfo row in the parameter table in 6.3.8.4.2 as follows:

Name	Type	Valid range	Description
FILSHLPContainer	As defined in 9.4.2.184	As defined in 9.4.2.184	A set of elements containing encapsulated data of higher layer protocol frames (e.g., a DHCP message) that is transported in FILS reassociation. The parameter is optionally present if dot11FILSActivated is true; otherwise not present.
FILSIPAddressAssignment	As defined in 9.4.2.185	As defined in 9.4.2.185	An explicit request for an IP address. The request may be for a new IP address or a specified IP address. The parameter is optionally present if dot11FILSActivated is true; otherwise not present.

6.3.8.5 MLME-REASSOCIATE.response

6.3.8.5.2 Semantics of the service primitive

Change the primitive parameter list in 6.3.8.5.2 as follows:

The primitive parameters are as follows:

```
MLME-REASSOCIATE.response(
    PeerSTAAddress,
    ResultCode,
    AssociationID,
    RCPI,
    RSNI,
    RMEnabledCapabilities,
    Content of FT Authentication elements,
    SupportedOperatingClasses,
    TimeoutInterval,
    BSSMaxIdlePeriod,
    TIMBroadcastResponse,
    FMSResponse,
    DMSResponse,
    QoSMapSet,
    Multi-band peer,
    FILSHLPContainer,
    FILSIPAddressAssignment,
    KeyDelivery,
    VendorSpecificInfo
)
```

Insert three new rows before the VendorSpecificInfo row in the parameter table in 6.3.8.5.2 as follows:

Name	Type	Valid range	Description
FILSHLPContainer	As defined in 9.4.2.184	As defined in 9.4.2.184	A set of elements containing encapsulated data of higher layer protocol frames (e.g., a DHCP message) that is transported in FILS reassociation. The parameter is optionally present if dot11-FILSActivated is true; otherwise not present.
FILSIPAddressAssignment	As defined in 9.4.2.185	As defined in 9.4.2.185	Contains the IP address of a network layer entity associated with the STA. The parameter is optionally present if dot11-FILSActivated is true; otherwise not present.
KeyDelivery	As defined in 9.4.2.186	As defined in 9.4.2.186	Contains KDE(s) and the current Key RSC. The parameter is present if dot11-FILSActivated is true; otherwise 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 parameter list in 6.3.11.2.2 as follows:

The primitive parameters are as follows:

```
MLME-START.request(
    SSID,
    BSSType,
    BeaconPeriod,
    DTIMPeriod,
    CF parameter set,
    PHY parameter set,
    IBSS parameter set,
    NAVSyncDelay,
    CapabilityInformation,
    BSSBasicRateSet,
    OperationalRateSet,
    Country,
    IBSS DFS Recovery Interval,
    EDCAPParameterSet,
    DSERegisteredLocation,
    HT Capabilities,
    HT Operation,
```

BSSMembershipSelectorSet,
 Extended Capabilities,
 20/40 BSS Coexistence,
 Overlapping BSS Scan Parameters,
 MultipleBSSID,
 InterworkingInfo,
 AdvertisementProtocolInfo,
 RoamingConsortiumInfo,
 Mesh ID,
 Mesh Configuration,
 QMFPolicy,
 DMG Capabilities,
 Multi-band,
 MMS,
 DMG Operation,
 Clustering Control,
 CBAP Only,
 PCP Association Ready,
 VHT Capabilities,
 VHT Operation,
Known OUIs,
 VendorSpecificInfo
)

Change the following row in the parameter table in 6.3.11.2.2:

Name	Type	Valid range	Description
MultipleBSSID	As defined in Multiple BSSID Element in 9.4.2.46	As defined in Multiple BSSID Element in 9.4.2.46	This element is optionally present when dot11RM-MeasurementPilotActivated is a value between 2 and 7 and the AP is a member of a Multiple BSSID Set (see 11.11.14) with two or more members, or if dot11MultiBSSIDActivated is true. <u>This element is present when dot11FILSActivated is true and the AP is a member of a Multiple BSSID Set with two or more members.</u>

Insert one new row before the VendorSpecificInfo row in the parameter table in 6.3.11.2.2 as follows:

Name	Type	Valid range	Description
Known OUIs	A set of OUIs, each of which is as defined in 9.4.1.32	N/A	Zero or more OUIs that specify the OUIs known by the AP. The AP uses the known OUIs to determine if it should respond to the Probe Request frame as defined in 11.1.4.3.4.

Insert new subclause 6.3.105 as follows:

6.3.105 FILS Container

6.3.105.1 General

This mechanism supports the process of IP address setup with a peer MAC entity.

6.3.105.2 MLME-FILSContainer.request

6.3.105.2.1 Function

This primitive requests transmission of the FILS Container frame with a specified peer MAC entity.

6.3.105.2.2 Semantics of the service primitive

The primitive parameters are as follows:

```
MLME-FILSContainer.request(
    Peer MAC Address,
    FILSIPAddressAssignment,
    VendorSpecificInfo
)
```

Name	Type	Valid range	Description
Peer MAC Address	MACAddress	Any valid individual MAC address	Specifies the address of the peer MAC entity.
FILSIPAddressAssignment	FILS IP Address Assignment element	As defined in 9.4.2.185	The request may be for a new IP address or a specified IP address.
VendorSpecificInfo	A set of elements	As defined in 9.4.2.26	Zero or more elements.

6.3.105.2.3 When generated

This primitive is generated by the SME for a STA to request IP Address setup from the AP.

6.3.105.2.4 Effect of receipt

This primitive requests IP Address setup. In the case that a response is received from the AP, the MLME subsequently issues an MLME-FILSContainer.confirm primitive that reflects the results.

6.3.105.3 MLME-FILSContainer.confirm

6.3.105.3.1 Function

This primitive reports the results of an IP Address setup with an AP.

6.3.105.3.2 Semantics of the service primitive

The primitive parameters are as follows:

```
MLME-FILSContainer.confirm(  

    Peer MAC Address,  

    FILSIPAddressAssignment,  

    VendorSpecificInfo  

)
```

Name	Type	Valid range	Description
Peer MAC Address	MACAddress	Any valid individual MAC address	Specifies the address of the peer MAC entity.
FILSIPAddressAssignment	FILS IP Address Assignment element	As defined in 9.4.2.185	IP address information.
VendorSpecificInfo	A set of elements	As defined in 9.4.2.26	Zero or more elements.

6.3.105.4 MLME-FILSContainer.indication

6.3.105.4.1 Function

This primitive indicates receipt of a request of IP Address setup.

6.3.105.4.2 Semantics of the service primitive

The primitive parameters are as follows:

```
MLME-FILSContainer.indication(  

    Peer MAC Address,  

    FILSIPAddressAssignment,  

    VendorSpecificInfo  

)
```