



**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 4: Protected Management Frames

IEEE Computer Society

Sponsored by the
LAN/MAN Standards Committee

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

30 September 2009

IEEE Std 802.11wTM-2009
(Amendment to IEEE Std 802.11TM-2007
as amended by IEEE Std 802.11kTM-2008,
IEEE Std 802.11rTM-2008, and
IEEE Std 802.11yTM-2008)

AVA Documents
Document Sharing Hub

IEEE Std 802.11w™-2009
(Amendment to IEEE Std 802.11™-2007
as amended by IEEE Std 802.11k™-2008,
IEEE Std 802.11r™-2008, and
IEEE Std 802.11y™-2008)

**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 4: Protected Management Frames

Sponsor

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

Approved 11 September 2009

IEEE SA-Standards Board

Abstract: This amendment specifies the extensions to IEEE Std 802.11 for wireless local area networks (WLANs) providing mechanisms for protecting management frames.

Keywords: local area network (LAN)

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

Copyright © 2009 by the Institute of Electrical and Electronics Engineers, Inc.
All rights reserved. Published 30 September 2009. Printed in the United States of America.

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

PDF: ISBN 978-0-7381-6048-1 STD95962
Print: ISBN 978-0-7381-6049-8 STDPD95962

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

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

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

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

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

In publishing and making this document available, the IEEE is not suggesting or rendering professional or other services for, or on behalf of, any person or entity. Nor is the IEEE undertaking to perform any duty owed by any other person or entity to another. Any person utilizing this, and any other IEEE Standards document, should rely upon his or her 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.

Interpretations: Occasionally questions may arise regarding the meaning of portions of standards as they relate to specific applications. When the need for interpretations is brought to the attention of IEEE, the Institute will initiate action to prepare appropriate responses. Since IEEE Standards represent a consensus of concerned interests, it is important to ensure that any interpretation has also received the concurrence of a balance of interests. For this reason, IEEE and the members of its societies and Standards Coordinating Committees are not able to provide an instant response to interpretation requests except in those cases where the matter has previously received formal consideration. A statement, written or oral, that is not processed in accordance with the IEEE-SA Standards Board Operations Manual shall not be considered the official position of IEEE or any of its committees and shall not be considered to be, nor be relied upon as, a formal interpretation of the IEEE. At lectures, symposia, seminars, or educational courses, an individual presenting information on IEEE standards shall make it clear that his or her views should be considered the personal views of that individual rather than the formal position, explanation, or interpretation of the IEEE.

Comments for revision of IEEE Standards are welcome from any interested party, regardless of membership affiliation with IEEE. Suggestions for changes in documents should be in the form of a proposed change of text, together with appropriate supporting comments. Recommendations to change the status of a stabilized standard should include a rationale as to why a revision or withdrawal is required. Comments and recommendations on standards, and requests for interpretations should be addressed to:

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

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

Introduction

This introduction is not part of IEEE Std 802.11w-2009, IEEE Standard for Information technology—Telecommunications and information exchange between systems—Local and metropolitan networks—Specific requirements—Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications—Amendment 4: Protected Management Frames.

IEEE Std 802.11-2007 as amended has been used in a wide range of mainstream business and personal applications. The success of products has resulted in an increased dependency on IEEE 802.11 as a primary method for the interconnection of networking equipment. This increased dependence has resulted in a need for increased assurance that the system will not be disrupted by the actions of unauthorized equipment. Such disruption can be caused by malicious systems generating false information and impersonating valid equipment. IEEE Std 802.11-2007 as amended addresses security of data frames but systems are still vulnerable to malicious attack because management frames are unprotected. At the same time, there is an increased dependence on management frames as a result of IEEE 802.11 amendments. The purpose of this amendment is to reduce the susceptibility of systems to such attack.

Notice to users

Laws and regulations

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

Copyrights

This document is copyrighted by the IEEE. It is made available for a wide variety of both public and private uses. These include both use, by reference, in laws and regulations, and use in private self-regulation, standardization, and the promotion of engineering practices and methods. By making this document available for use and adoption by public authorities and private users, the IEEE does not waive any rights in copyright to this document.

Updating of IEEE documents

Users of IEEE standards should be aware that these documents may be superseded at any time by the issuance of new editions or may be amended from time to time through the issuance of amendments, corrigenda, or errata. An official IEEE document at any point in time consists of the current edition of the document together with any amendments, corrigenda, or errata then in effect. In order to determine whether a given document is the current edition and whether it has been amended through the issuance of amendments, corrigenda, or errata, visit the IEEE Standards Association website at <http://ieeexplore.ieee.org/xpl/standards.jsp>, or contact the IEEE at the address listed previously.

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

Errata

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

Interpretations

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

Patents

Attention is called to the possibility that implementation of this standard may require use of subject matter covered by patent rights. By publication of this standard, no position is taken with respect to the existence or validity of any patent rights in connection therewith. A patent holder or patent applicant has filed a statement of assurance that it will grant licenses under these 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. Other Essential Patent Claims may exist for which a statement 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 amendment was sent to sponsor ballot, the IEEE 802.11 Working Group had the following officers:

Bruce P. Kraemer, *Chair*
Jon Walter Rosdahl, *Vice Chair, Treasurer, and Chair, Task Group mb*
Adrian P. Stephens, *Vice Chair*
Stephen McCann, *Secretary and Chair, Publicity Standing Committee*
Terry L. Cole, *Technical Editor and Assigned Number Authority*
Teik-Kheong Tan, *Chair, Wireless Next Generation Standing Committee*

David Bagby, *Chair, Architecture Standing Committee*
Bruce P. Kraemer, *Chair, Task Group n and Co-Chair, IMT-Advanced Ad hoc Committee*
Sheung Li, *Vice Chair, Task Group n*
Lee Armstrong, *Chair, Task Group p*
Donald E. Eastlake III, *Chair, Task Group s*
Neeraj Sharma, *Chair, Task Group t*
Stephen McCann, *Chair, Task Group u*
Dorothy V. Stanley, *Chair, Task Group v and IETF Ad hoc Committee*
Jesse Walker, *Chair, JCT1 Ad hoc Committee*
Peter Ecclesine, *Chair, Task Group y*
Menzo Wentink, *Chair, Task Group z*
Ganesh Venkatesan, *Chair, Task Group aa*
Eldad Perahia, *Chair, Very High Throughput Study Group*
Darwin Engwer, *Co-Chair, IMT-Advanced Ad hoc Committee*

When the IEEE 802.11 Working Group approved this amendment, Task Group w had the following officers:

Jesse Walker, *Chair*
Nancy Cam-Winget, Jon Edney, *Technical Editors*
Sandy Turner, *Secretary*

When this amendment was sent to sponsor ballot, the IEEE 802.11 Working Group had the following membership:

Osama S. Aboulmagd	Yoshiharu Doi	Yeonkwon Jeong
Tomoko Adachi	John Dorsey	Jorjeta G. Jetcheva
Alok Aggarwal	Roger P. Durand	Lusheng Ji
Carlos H. Aldana	Srinivasa Duvvuri	Daniel Jiang
Thomas Alexander	Donald E. Eastlake III	Padam Kafle
Keith Amann	Peter Ecclesine	Carl W. Kain
Lee Armstrong	Mike Ellis	Naveen K. Kakani
Alex Ashley	Stephen P. Emeott	Masato Kato
Malik Audeh	Marc Emmelmann	Douglas Kavner
David Bagby	Darwin Engwer	John Kenney
Michael Bahr	Joseph Epstein	Stuart J. Kerry
Fan Bai	Leonid Epstein	Joonsuk Kim
Gabor Bajko	Vinko Erceg	Kyeongpyo Kim
Dennis J. Baker	Lars P. Falk	Seong S. Kim
Amit Bansal	Robert Fanfelle	Yongsun Kim
John R. Barr	Stefan Fechtel	Youjin Kim
Gal Basson	Paul H. Feinberg	Gunter Kleindl
Moussa Bavafa	Matthew J. Fischer	Jarkko Knecht
Tuncer Baykas	Wayne K. Fisher	Mark M. Kobayashi
Mathilde Benveniste	Roberta Fracchia	Fumihide Kojima
Bjorn A. Bjerke	James P. Gilb	Tom Kolze
Daniel Borges	Reinhard Gloger	Bruce P. Kraemer
Anthony Braskich	David Goodall	Johannes P. Kruys
David Britz	Tugrul Guener	Thomas Kuehnelt
G. Bumiller	Jianlin Guo	Rajendra Kumar
Nancy Cam-Winget	Pratibha Gupta	Thomas M. Kurihara
Necati Canpolat	Mark Hamilton	Joseph Kwak
Javier Cardona	Christopher J. Hansen	Edwin Kwon
Douglas S. Chan	Dan N. Harkins	Jeremy A. Landt
Lidong Chen	Brian D. Hart	Joseph P. Lauer
Nakjung Choi	Amer A. Hassan	Jin Lee
Liwen Chu	Vegard Hassel	Tae H. Lee
Terry L. Cole	Shigenori Hayase	Joseph Levy
Ryon K. Coleman	Kevin V. Hayes	Sheung Li
Charles I. Cook	Robert F. Heile	Paul Lin
Todor Cooklev	Guido R. Hiertz	Hang Liu
Xavier P. Costa	Junling Hu	Michael Livshitz
David E. Cypher	Robert Y. Huang	Peter Loc
Marc De Courville	David Hunter	Daniel Lubar
Theodorus Denteneer	Yasuhiko Inoue	Anthony F. Maida
Jeremy deVries	Akio Iso	Jakub Majkowski
Susan Dickey	Junghoon Jee	Alastair Malarky
Zhiming Ding	Hongseok Jeon	Jouni K. Malinen

Bill Marshall
 Sudheer Matta
 Stephen McCann
 Justin P. McNew
 Robert R. Miller
 Michael Montemurro
 Rajendra T. Moorti
 Hitoshi Morioka
 Peter Murray
 Andrew Myles
 Rohit Nabar
 Kengo Nagata
 Chiu Ngo
 Eero Nikula
 Erwin Noble
 Richard H. Noens
 Hideaki Odagiri
 Jisung Oh
 Chandra S. Olson
 Satoshi Oyama
 Richard H. Paine
 Arul Palanivelu
 Jungsoo Park
 Minyoung Park
 Vijaykumar Patel
 Bemini H. Peiris
 Eldad Perahia
 James E. Petranovich
 Al Petrick
 Fahd Pirzada
 Subburajan Ponnuswamy
 James D. Portaro
 Henry S. Ptasinski
 Chang W. Pyo
 Emily H. Qi
 Luke Qian
 Jim E. Raab
 Vinuth Rai

Ali Raissinia
 Stephen G. Rayment
 Leonid Razoumov
 Ivan Reede
 Joseph A. Repice
 Edward Reuss
 Randal Roebuck
 Jon Walter Rosdahl
 Richard Roy
 Alexander Safonov
 Kazuyuki Sakoda
 Nicholas Sargologos
 Katsuyoshi Sato
 Hirokazu Sawada
 Vincenzo Scarpa
 Don Schultz
 Yongho Seok
 Huairong Shao
 Neeraj Sharma
 Stephen J. Shellhammer
 Ian Sherlock
 Kai Shi
 Shusaku Shimada
 Francois Simon
 Harkirat Singh
 Graham K. Smith
 Matt Smith
 Kapil Sood
 Vinay Sridhara
 Dorothy V. Stanley
 Adrian P. Stephens
 David S. Stephenson
 Carl R. Stevenson
 Guenael T. Strutt
 Eiji Takagi
 Mineo Takai
 Teik-Kheong Tan

Allan Thomson
 Jerry Thrasher
 Alexander Tolpin
 Jason Trachewsky
 Solomon B. Trainin
 Ashley Uyehara
 Allert Van Zelst
 Mathieu Varlet-Andre
 Prabodh Varshney
 Ganesh Venkatesan
 Dalton T. Victor
 George A. Vlantis
 Jesse Walker
 Qi Wang
 Craig D. Warren
 Fujio Watanabe
 Patrick Waye
 Menzo Wentink
 Kyle Williams
 James Worsham
 Harry R. Worstell
 Songping Wu
 Pengfei Xia
 Akiyoshi Yagi
 Akira Yamada
 Takeshi Yamamoto
 Tomoya Yamaura
 Zhiyu Yang
 Peter Yee
 Su K. Yong
 Christopher Young
 Artur Zaks
 Hongyuan Zhang
 Huimin Zhang
 Meiyuan Zhao
 Jing Zhu
 Juan Zuniga
 Jonathan Zweig

Major contributions were received from the following individuals:

Clint Chaplin
 Lily Chen
 Abhijit Choudhury
 Frank Ciotti
 David E. Cypher
 Joseph Epstein
 Matthew Gast

Dan N. Harkins
 Kevin V. Hayes
 Moo Ryong Jeong
 Philip MacKenzie
 Jouni K. Malinen
 Robert Moskowitz
 Emily H. Qi

Henry S. Ptasinski
 Richard Roy
 Kapil Sood
 Fabrice Stevens
 Fujio Watanabe
 Marcus Wong
 Peter Yee

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

Tomoko Adachi	Sergiu Goma	Charles Ngethe
Toru Aihara	Randall Groves	Satoshi Obara
Thomas Alexander	C. Guy	Robert O'Hara
Butch Anton	Christopher J. Hansen	Stephen Palm
Danilo Antonelli	John Hawkins	Subburajan Ponnuswamy
Matthew Ball	Russell Housley	Cam Posani
Raja Banerjea	Yasuhiko Inoue	Michael Probasco
Gennaro Boggia	Atsushi Ito	Henry S. Ptasinski
Nancy S. Bravin	Raj Jain	Maximilian Riegel
William Byrd	David Johnston	Robert Robinson
Peter J. Calderon	Bobby Jose	Jon W. Rosdahl
Edward Carley	Joe Natharoj Juisai	Richard Roy
James Carlo	Shinkyo Kaku	Herbert Ruck
Juan Carreon	Piotr Karocki	Randall Safier
Clint Chaplin	Stuart J. Kerry	Anil Sanwalka
Yung-Mu Chen	Brian Kiernan	John Sargent
Hong Cheng	Yongbum Kim	Oyama Satoshi
Keith Chow	Joseph Kubler	Kapil Sood
Ryon K. Coleman	Thomas M. Kurihara	Amjad Soomro
Charles I. Cook	Jeremy A. Landt	Dorothy V. Stanley
Todor Cooklev	Daniel Levesque	Thomas Starai
Susan Dickey	Jan-Ray Liao	Walter Struppler
Russell Dietz	Arthur Light	Alourdes Sully
Petar Djukic	Daniel Lubar	Masahiro Takagi
Sourav Dutta	William Lumpkins	Joseph Tardo
Donald E. Eastlake III	G. Luri	Solomon Trainin
Paul Eastman	Jouni K. Malinen	Mark-Rene Uchida
Richard Eckard	Peter Martini	Prabodh Varshney
Stephen P. Emeott	W. Kyle Maus	Jesse Walker
Marc Emmelmann	Stephen McCann	Stanley Wang
Joseph Epstein	Gary Michel	Fujio Watanabe
Bernard Eydt	Michael Montemurro	Stephen Webb
Matthew J. Fischer	Jose Morales	David Willow
Andre Fournier	Joseph Moran	Harry R. Worstell
Prince Francis	Andrew Myles	Xuyong Wu
Matthew Gast	Juichi Nakada	Oren Yuen
Devon Gayle	Hiroyuki Nakase	Paolo Zangheri
Michael Geipel	Michael S. Newman	Meiyuan Zhao
Mariana Goldhamer		Wenhao Zhu

When the IEEE-SA Standards Board approved this amendment on 11 September 2009, it had the following membership:

Robert M. Grow, *Chair*
Thomas Prevost, *Vice Chair*
Steve M. Mills, *Past Chair*
Judith Gorman, *Secretary*

John Barr
Karen Bartleson
Victor Berman
Ted Burse
Richard DeBlasio
Andy Drozd
Mark Epstein

Alexander Gelman
Jim Hughes
Richard H. Hulett
Young Kyun Kim
Joseph L. Koepfinger*
John Kulick
David J. Law

Ted Olsen
Glenn Parsons
Ronald C. Petersen
Narayanan Ramachandran
Jon Walter Rosdahl
Sam Sciacca
Howard L. Wolfman

*Member Emeritus

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

Satish K. Aggarwal, *NRC Representative*
Michael Janezic, *NIST Representative*

Michelle Turner
IEEE Standards Program Manager, Document Development

Michael D. Kipness
IEEE Standards Program Manager, Technical Program Development

Contents

3.	Definitions	2
4.	Abbreviations and acronyms	2
5.	General description	2
5.2	Components of the IEEE 802.11 architecture	2
5.2.3	Distribution system (DS) concepts	2
5.2.3.2	RSNA.....	2
5.4	Overview of the services.....	3
5.4.2	Services that support the distribution service	3
5.4.2.4	Disassociation	3
5.4.3	Access control and data confidentiality services	3
5.4.3.2	Deauthentication	3
5.4.3.3	Data confidentiality.....	3
5.4.3.4	Key management	4
5.4.3.5	Data origin authenticity	4
5.4.3.6	Replay detection	4
5.4.3.7	Fast BSS transition.....	4
5.4.3.8	Robust Management frame protection.....	4
5.8	IEEE Std 802.11 and IEEE Std 802.1X-2004	5
5.8.2	Infrastructure functional model overview.....	5
5.8.2.1	Authentication and key management (AKM) operations with Authentication Server (AS)	5
5.8.2.2	Operations with PSK	7
5.8.5	PMKSA caching	7
5.8.6	Protection of broadcast and multicast Robust Management frames.....	7
6.	MAC service definition	8
6.1	Overview of MAC services	8
6.1.2	Security services	8
7.	Frame formats	8
7.1	MAC Frame formats	8
7.1.3	Frame fields	8
7.1.3.1	Frame control field.....	8
7.1.3.1.8	Protected Frame field.....	8
7.2	Format of individual frame types.....	9
7.2.3	Management frames.....	9
7.2.3.3	Disassociation frame format	9
7.2.3.5	Association Response frame format	9
7.2.3.7	Reassociation Response frame format	10
7.2.3.11	Deauthentication	10
7.2.3.12	Action frame format.....	11
7.3	Management frame body components	11
7.3.1	Fields that are not information elements.....	11
7.3.1.9	Status Code field.....	11
7.3.1.11	Action field	12

7.3.2	Information elements	12
7.3.2.25	RSN information element	14
7.3.2.25.1	Cipher suites	15
7.3.2.25.2	AKM suites	17
7.3.2.25.3	RSN capabilities	17
7.3.2.48	Fast BSS transition information element (FTIE)	18
7.3.2.49	Timeout Interval information element (TIE)	19
7.3.2.54	Supported Regulatory Classes element	19
7.3.2.55	Management MIC information element	19
7.4	Action frame format details	20
7.4.5	Vendor-specific action details	20
7.4.7	Public Action details	20
7.4.7.1	Public Action frames	20
7.4.7.9	DSE Power Constraint frame format	21
7.4.7.10	Vendor Specific Public Action frame format	21
7.4.8	Action frame details	21
7.4.9	SA Query Action frame details	21
7.4.9.1	SA Query Request frame	21
7.4.9.2	SA Query Response frame	22
7.4.9a	Protected Dual of Public Action frames	22
7.4.9a.1	Protected Dual of Public Action details	22
7.4.9a.2	Protected DSE Enablement frame format	23
7.4.9a.3	Protected DSE Deenablement frame format	23
7.4.9a.4	Protected Extended Channel Switch Announcement frame format	23
7.4.9a.5	Protected DSE Measurement Request frame format	23
7.4.9a.6	Protected DSE Measurement Report frame format	23
7.4.9a.7	Protected DSE Power Constraint frame format	24
8.	Security	24
8.1	Framework	24
8.1.1	Security methods	24
8.1.3	RSNA establishment	24
8.3	RSNA data confidentiality and integrity protocols	24
8.3.1	Overview	24
8.3.3	CTR with CBC-MAC Protocol (CCMP)	25
8.3.3.1	CCMP Overview	25
8.3.3.3	CCMP cryptographic encapsulation	25
8.3.3.3.2	Construct AAD	25
8.3.3.3.3	Construct CCM nonce	26
8.3.3.3.5	CCM originator processing	26
8.3.3.4	CCMP decapsulation	26
8.3.3.4.1	CCM recipient processing	27
8.3.3.4.3	PN and replay detection	27
8.3.4	The Broadcast/Multicast integrity protocol	27
8.3.4.1	BIP overview	28
8.3.4.2	BIP MMPDU format	28
8.3.4.3	BIP AAD construction	28
8.3.4.4	BIP replay protection	28
8.3.4.5	BIP transmission	29
8.3.4.6	BIP reception	29

8.4	RSNA security association management	30
8.4.1	Security associations	30
8.4.1.1	Security association definitions	30
8.4.1.1.3	GTKSA	30
8.4.1.1.3a	IGTKSA	30
8.4.1.2	Security association life cycle	30
8.4.1.2.1	Security association in an ESS	30
8.4.3	RSNA policy selection in an ESS	31
8.4.4	RSNA policy selection in an IBSS	32
8.4.6	RSNA authentication in an ESS	33
8.4.6.1	Preauthentication and RSNA key management	33
8.4.6.2	Cached PMKSAs and RSNA key management	33
8.4.9	RSNA key management in an IBSS	33
8.4.10	RSNA security association termination	33
8.4.11	Protection of Robust Management frames	34
8.4.12	Robust Management frame Selection Procedure	35
8.5	Keys and key distribution	35
8.5.1	Key hierarchy	35
8.5.1.1	PRF	35
8.5.1.2	Pairwise key hierarchy	36
8.5.1.3	Group key hierarchy	36
8.5.1.3a	Integrity group key hierarchy	36
8.5.1.4	PeerKey key hierarchy	36
8.5.2	EAPOL-Key frames	37
8.5.2.1	EAPOL-Key frame notation	37
8.5.3	4-Way Handshake	38
8.5.3.2	4-Way Handshake Message 2	38
8.5.3.3	4-Way Handshake Message 3	38
8.5.3.6	Sample 4-Way Handshake	38
8.5.4	Group Key Handshake	39
8.5.4.1	Group Key Handshake Message 1	40
8.5.4.4	Sample Group Key Handshake	40
8.5.5	RSNA Supplicant key management state machine	41
8.5.5.2	Supplicant state machine variables	42
8.5.5.3	Supplicant state machine procedures	42
8.5.6	RSNA Authenticator key management state machine	44
8.6	Mapping EAPOL keys to IEEE 802.11 keys	46
8.6.3	Mapping PTK to CCMP keys	46
8.6.6a	Mapping IGTK to BIP Keys	46
8.7	Per-frame pseudo-code	47
8.7.2	RSNA frame pseudo-code	47
8.7.2.1	Per-MSDU Tx pseudo-code	47
8.7.2.1a	Per-MMPDU Tx pseudo-code	47
8.7.2.2a	Per-MPDU Tx pseudo-code for MMPDU	49
8.7.2.3a	Per-MPDU Rx pseudo-code for an MMPDU	49
8.7.2.5	Per-MMPDU Rx pseudo-code	53
10.	Layer Management	54
10.3	MLME SAP interface	54
10.3.17	SetKeys	54
10.3.17.1	MLME-SETKEYS.request	54
10.3.17.1.2	Semantics of the service primitive	54

10.3.18	DeleteKeys.....	54
10.3.18.1	MLME-DELETEKEYS.request.....	54
10.3.18.1.2	Semantics of the service primitive.....	54
10.3.22	SetProtection.....	54
10.3.22.1	MLME-SETPROTECTION.request.....	54
10.3.22.1.2	Semantics of the service primitive.....	54
10.3.39	SA Query support.....	55
10.3.39.1	MLME-SAQuery.request.....	55
10.3.39.1.1	Function.....	55
10.3.39.1.2	Semantics of the service primitive.....	55
10.3.39.1.3	When generated.....	55
10.3.39.1.4	Effect of receipt.....	55
10.3.39.2	MLME-SAQuery.confirm.....	55
10.3.39.2.1	Function.....	55
10.3.39.2.2	Semantics of the service primitive.....	55
10.3.39.2.3	When generated.....	56
10.3.39.2.4	Effect of receipt.....	56
10.3.39.3	MLME-SAQuery.indication.....	56
10.3.39.3.1	Function.....	56
10.3.39.3.2	Semantics of the service primitive.....	56
10.3.39.3.3	When generated.....	57
10.3.39.3.4	Effect of receipt.....	57
10.3.39.4	MLME-SAQuery.response.....	57
10.3.39.4.1	Function.....	57
10.3.39.4.2	Semantics of the service primitive.....	57
10.3.39.4.3	When generated.....	57
10.3.39.4.4	Effect of receipt.....	57
10.3.40	Protected Extended Channel Switch Announcement.....	57
10.3.40.1	MLME-PDEXTCHANNELSWITCH.request.....	58
10.3.40.1.1	Function.....	58
10.3.40.1.2	Semantics of the service primitive.....	58
10.3.40.1.3	When generated.....	58
10.3.40.1.4	Effect of receipt.....	58
10.3.40.2	MLME-PDEXTCHANNELSWITCH.confirm.....	58
10.3.40.2.1	Function.....	58
10.3.40.2.2	Semantics of the service primitive.....	59
10.3.40.2.3	When generated.....	59
10.3.40.2.4	Effect of receipt.....	59
10.3.40.3	MLME-PDEXTCHANNELSWITCH.indication.....	59
10.3.40.3.1	Function.....	59
10.3.40.3.2	Semantics of the service primitive.....	59
10.3.40.3.3	When generated.....	60
10.3.40.3.4	Effect of receipt.....	60
10.3.40.4	MLME-PDEXTCHANNELSWITCH.response.....	60
10.3.40.4.1	Function.....	60
10.3.40.4.2	Semantics of the service primitive.....	60
10.3.40.4.3	When generated.....	61
10.3.40.4.4	Effect of receipt.....	61
10.3.41	Protected DSE Power Constraint Announcement.....	61
10.3.41.1	MLME-PDDSETPC.request.....	61
10.3.41.1.1	Function.....	61
10.3.41.1.2	Semantics of the service primitive.....	61
10.3.41.1.3	When generated.....	62
10.3.41.1.4	Effect of receipt.....	62

10.3.41.2	MLME-PDDSETPC.confirm	62
10.3.41.2.1	Function	62
10.3.41.2.2	Semantics of the service primitive	62
10.3.41.2.3	When generated	63
10.3.41.2.4	Effect of receipt	63
10.3.41.3	MLME-PDDSETPC.indication	63
10.3.41.3.1	Function	63
10.3.41.3.2	Semantics of the service primitive	63
10.3.41.3.3	When generated	63
10.3.41.3.4	Effect of receipt	63
10.3.41.4	MLME-PDDSETPC.response	64
10.3.41.4.1	Function	64
10.3.41.4.2	Semantics of the service primitive	64
10.3.41.4.3	When generated	64
10.3.41.4.4	Effect of receipt	64
10.3.42	Protected Enablement	64
10.3.42.1	MLME-PDENABLEMENT.request	64
10.3.42.1.1	Function	64
10.3.42.1.2	Semantics of the service primitive	64
10.3.42.1.3	When generated	65
10.3.42.1.4	Effect of receipt	65
10.3.42.2	MLME-PDENABLEMENT.confirm	65
10.3.42.2.1	Function	65
10.3.42.2.2	Semantics of the service primitive	65
10.3.42.2.3	When generated	66
10.3.42.2.4	Effect of receipt	66
10.3.42.3	MLME-PDENABLEMENT.indication	66
10.3.42.3.1	Function	66
10.3.42.3.2	Semantics of the service primitive	66
10.3.42.3.3	When generated	67
10.3.42.3.4	Effect of receipt	67
10.3.42.4	MLME-PDENABLEMENT.response	67
10.3.42.4.1	Function	67
10.3.42.4.2	Semantics of the service primitive	67
10.3.42.4.3	When generated	68
10.3.42.4.4	Effect of receipt	68
10.3.43	Protected Deenablement	68
10.3.43.1	MLME-PDDEENABLEMENT.request	68
10.3.43.1.1	Function	68
10.3.43.1.2	Semantics of the service primitive	68
10.3.43.1.3	When generated	68
10.3.43.1.4	Effect of receipt	68
10.3.43.2	MLME-PDDEENABLEMENT.confirm	69
10.3.43.2.1	Function	69
10.3.43.2.2	Semantics of the service primitive	69
10.3.43.2.3	When generated	69
10.3.43.2.4	Effect of receipt	69
10.3.43.3	MLME-PDDEENABLEMENT.indication	69
10.3.43.3.1	Function	69
10.3.43.3.2	Semantics of the service primitive	70
10.3.43.3.3	When generated	70
10.3.43.3.4	Effect of receipt	70

10.3.44	Vendor Specific Public Action	70
10.3.44.1	MLME-PVSPECIFIC.request	70
10.3.44.1.1	Function	70
10.3.44.1.2	Semantics of the service primitive	70
10.3.44.1.3	When generated	71
10.3.44.1.4	Effect of receipt	71
10.3.44.2	MLME-PVSPECIFIC.confirm	71
10.3.44.2.1	Function	71
10.3.44.2.2	Semantics of the service primitive	71
10.3.44.2.3	When generated	72
10.3.44.2.4	Effect of receipt	72
10.3.44.3	MLME-PVSPECIFIC.indication	72
10.3.44.3.1	Function	72
10.3.44.3.2	Semantics of the service primitive	72
10.3.44.3.3	When generated	72
10.3.44.3.4	Effect of receipt	72
11.	MLME	73
11.3	STA authentication and association	73
11.3.1	Authentication and deauthentication	73
11.3.1.1	Authentication—originating STA	73
11.3.1.2	Authentication—destination STA	73
11.3.2	Association, reassociation, and disassociation	73
11.3.2.2	AP association procedures	73
11.3.2.4	AP reassociation procedures	74
11.11	DSE procedures	74
11.11.1	General	74
11.12	Broadcast and multicast Robust Management frame procedures	75
11.13	SA Query procedures	75
11A.	Fast BSS Transition	75
11A.2	Key holders	75
11A.2.2	Authenticator key holders	75
11A.4	FT initial mobility domain association	76
11A.4.2	FT initial mobility domain association in an RSN	76
11A.5	FT protocol	77
11A.5.2	Over-the-air FT protocol authentication in an RSN	77
11A.5.3	Over-the-DS FT Protocol authentication in an RSN	78
11A.6	FT Resource Request Protocol	79
11A.6.2	Over-the-air fast BSS transition with resource request	79
11A.6.3	Over-the-DS fast BSS transition with resource request	79
11A.7	FT reassociation	80
11A.7.1	FT reassociation in an RSN	80
11A.8	FT authentication sequence	80
11A.8.5	FT authentication sequence: contents of fourth message	80
11A.9	FT security architecture state machines	81
11A.9.3	R1KH state machine	81
Annex A (normative)	Protocol Implementation Conformance Statement (PICS) proforma	83
A.4	PICS proforma—IEEE Std 802.11-2007	83
A.4.4	MAC protocol	83
A.4.4.1	MAC protocol capabilities	83

Annex D (normative) ASN.1 encoding of the MAC and PHY MIB.....	85
Annex H (informative) RSNA reference implementations and test vectors.....	90
H.8 Test vectors for AES-128-CMAC	90
H.9 Management Frame Protection test vectors	90
H.9.1 BIP with broadcast Deauthentication frame.....	90
H.9.2 CCMP with unicast Deauthentication frame.....	91

List of figures

Figure 5-13—Establishing pairwise and group keys	6
Figure 5-14—Delivery of subsequent group keys	7
Figure 7-72—RSN Information Element format	14
Figure 7-74—RSN Capabilities field format	17
Figure 7-95o6a—IGTK sub-element format	18
Figure 7-95o15—Management MIC information element format	19
Figure 7-95o16—Vendor Specific Public Action frame format	21
Figure 7-101m—SA Query Request frame details	22
Figure 7-101n—SA Query Response frame details	22
Figure 8-17—AAD construction	25
Figure 8-18—Nonce construction	26
Figure 8-19a—BIP Encapsulation	28
Figure 8-19b—BIP AAD Construction	28
Figure 8-32a—IGTK KDE format	37
Figure 8-33—Sample 4-Way Handshake	39
Figure 8-34—Sample Group Key Handshake	41
Figure 8-35—RSNA Supplicant key management state machine	41
Figure 8-37—Authenticator state machines, part 1	45
Figure 8-40—Authenticator state machines, part 4	46
Figure 11A-2—FT Initial Mobility Domain Association in an RSN	76
Figure 11A-4—Over-the-air FT Protocol in an RSN	77
Figure 11A-5—Over-the-DS FT Protocol in an RSN	78
Figure 11A-9—Over-the-air FT Resource Request Protocol in an RSN	79
Figure 11A-14—R1KH state machine, including portions of the SME (part 1)	81
Figure 11A-15—R1KH state machine, including portions of the SME (part 2)	82

List of tables

Table 7-9—Disassociation frame body	9
Table 7-13—Reassociation Response frame body	10
Table 7-11—Association Response frame body	10
Table 7-18—Deauthentication frame body	11
Table 7-19—Action frame body	11
Table 7-23—Status codes	11
Table 7-24—Category values	12
Table 7-26—Element IDs	13
Table 7-32—Cipher suite selectors	16
Table 7-33—Cipher suite usage	16
Table 7-34—AKM suite selectors	17
Table 7-43g—Sub-element IDs	18
Table 7-43h—Timeout Interval Type field value	19
Table 7-57e—Public Action field values	20
Table 7-57l—SA Query Action fields	21
Table 7-57m—Protected Dual of Public Action field values	23
Table 8-1a—Robust Management frame selection in an ESS	31
Table 8-1b—Robust Management frame selection in an IBSS	32
Table 8-2—Cipher suite key lengths	37
Table 8-4—KDE	37

**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 4: Protected Management Frames

(This amendment is based on IEEE Std 802.11TM-2007, as amended by IEEE Std 802.11kTM-2008, IEEE Std 802.11rTM-2008, and IEEE Std 802.11yTM-2008.)

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

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

The editing instructions contained in this amendment define how to merge the material contained herein into the existing base standard and its amendments to form the comprehensive standard.¹

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 ~~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 instructions. ***Replace*** is used to make changes in figures or equations by removing the existing figure or equation and replacing it with a new one. Editing instructions, change markings, and this NOTE will not be carried over into future editions because the changes will be incorporated into the base standard.

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

3. Definitions

Insert the following definitions alphabetically into Clause 3, renumbering as necessary:

3.223 Integrity GTK (IGTK): A random value, assigned by the broadcast/multicast source STA, which is used to protect group addressed medium access control (MAC) management protocol data units (MMPDUs) from that source STA.

3.224 Protected Dual of Public Action frame: Protected Dual of Public Action frames are defined as Action frames with the category value specified in 7.3.1.11 Table 7-24. For each Protected Dual of Public Action frame, there is a dual Action frame in a category that is specified with “No” in the “Robust” column of Table 7-24.

3.225 Robust Action frame: Robust Action frames are defined as Action frames with category values specified in 7.3.1.11 Table 7-24 with “Yes” in the “Robust” column.

3.226 Robust Management frame: A management frame that is eligible for protection.

4. Abbreviations and acronyms

Insert the following new abbreviations and acronyms in alphabetical order:

BIP	Broadcast/Multicast Integrity Protocol
IGTK	Integrity GTK
IPN	IGTK packet number
MFPC	Management Frame Protection Capable
MFPR	Management Frame Protection Required
MMIE	Management MIC Information Element
SA Query	Security Association Query

5. General description

5.2 Components of the IEEE 802.11 architecture

5.2.3 Distribution system (DS) concepts

5.2.3.2 RSNA

Insert the following item at the end of the dashed list in 5.2.3.2:

- Enhanced cryptographic encapsulation mechanisms for Robust Management frames

5.4 Overview of the services

5.4.2 Services that support the distribution service

5.4.2.4 Disassociation

Change the third paragraph of 5.4.2.4 as follows:

The disassociation service may be invoked by either party to an association (non-AP STA or AP). Disassociation is a notification, not a request. Disassociation cannot be refused by ~~either party to the association.~~ the receiving STA except when Management Frame Protection is negotiated and the message integrity check fails.

5.4.3 Access control and data confidentiality services

5.4.3.2 Deauthentication

Change the second paragraph of 5.4.3.2 as follows:

In an ESS, because authentication is a prerequisite for association, the act of deauthentication shall cause the station to be disassociated. The deauthentication service may be invoked by either authenticated party (non-AP STA or AP). Deauthentication is not a request; it is a notification. ~~Deauthentication shall not be refused by either party. When an AP sends a deauthentication notice to an associated STA, the association shall also be terminated. 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.~~

Change the fourth paragraph of 5.4.3.2 as follows:

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), and STSL transient key security association (STKSA), and integrity group temporal key security association (IGTKSA) that exist in the STA and closes the associated IEEE 802.1X Controlled Port. If pairwise master key (PMK) caching is not enabled, deauthentication also destroys the pairwise master key security association (PMKSA) from which the deleted PTKSA was derived.

5.4.3.3 Data confidentiality

Change 5.4.3.3 by inserting a new fourth paragraph and changing the last paragraph as follows:

IEEE Std 802.11 provides one security protocol, CCMP, for protection of unicast Robust Management frames. This standard does not provide data confidentiality for group addressed Robust Management frames.

The default data confidentiality state for all IEEE 802.11 STAs is “in the clear.” If the data confidentiality service is not invoked, all ~~messages frames~~ shall be sent unprotected. If this policy is unacceptable to the sender, it shall not send data frames; and if the policy is unacceptable to the receiver, it shall discard any received data frames. Unprotected data frames and unprotected Robust Management frames received at a STA configured for mandatory data confidentiality, as well as protected data frames and protected Robust Management frames using a key not available at the receiving STA, are discarded without an indication to LLC (or without indication to distribution services in the case of “To DS” frames received at an AP). These frames are acknowledged on the WM [if received without frame check sequence (FCS) error] to avoid wasting WM bandwidth on retries of frames that are being discarded.

5.4.3.4 Key management

Change the text of 5.4.3.4 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 protocols called the 4-Way Handshake, FT 4-Way Handshake, FT Protocol, FT Resource Request Protocol, and Group Key Handshake.

5.4.3.5 Data origin authenticity

Change the text of 5.4.3.5 as follows:

The data origin authenticity mechanism defines a means by which a STA that receives a data or protected Robust Management frame can determine which STA transmitted the MAC protocol data unit (MPDU). This feature is required in an RSNA to prevent one STA from masquerading as a different STA. ~~This mechanism is provided for STAs that use CCMP or TKIP.~~

Data origin authenticity is only applicable to unicast data frames, and unicast Robust Management frames. The protocols do not guarantee data origin authenticity for broadcast/multicast ~~data~~ frames, as this cannot be accomplished using symmetric keys and public key methods are too computationally expensive.

5.4.3.6 Replay detection

Change the text of 5.4.3.6 as follows:

The replay detection mechanism defines a means by which a STA that receives a data or protected Robust Management frame from another STA can detect whether the received data-frame is an unauthorized retransmission. This replay protection mechanism is provided for data frames for STAs that use CCMP or TKIP. The replay protection mechanism is also provided for Robust Management frames for STAs that use CCMP and Broadcast/Multicast Integrity Protocol (BIP).

5.4.3.7 Fast BSS transition

Insert the following new subclause (5.4.3.8) after 5.4.3.7 as follows:

5.4.3.8 Robust Management frame protection

Robust Management frames are a set of management frames that can be protected by the Management Frame Protection service. The Robust Management frames are Disassociation, Deauthentication, and Robust Action frames. Action frames specified with “No” in the “Robust” column of Table 7-24 are not Robust Management frames and shall not be protected.

Management Frame Protection protocols apply to Robust Management frames after RSNA PTK establishment for protection of unicast frames is completed and after delivery of the IGTK to protect group addressed frames. Robust Management frame protection is implemented by the CCMP and BIP protocols and the SA Query procedure.

5.8 IEEE Std 802.11 and IEEE Std 802.1X-2004

5.8.2 Infrastructure functional model overview

5.8.2.1 Authentication and key management (AKM) operations with Authentication Server (AS)

Change the second paragraph of 5.8.2.1 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.
- Install the pairwise encryption and integrity keys into IEEE Std 802.11.
- 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.
- Verify that the RSN capabilities negotiated are valid as defined in 7.3.2.25.3.
- Confirm the cipher suite selection.

Insert the following paragraph at the end of 5.8.2.1:

When Management Frame Protection is negotiated, the Authenticator also uses the Group Key Handshake with all associated STAs to change the IGTK. The Authenticator encrypts the GTK and IGTK values in the EAPOL-Key frame as described in 8.5.

Replace Figure 5-13 with the following figure:

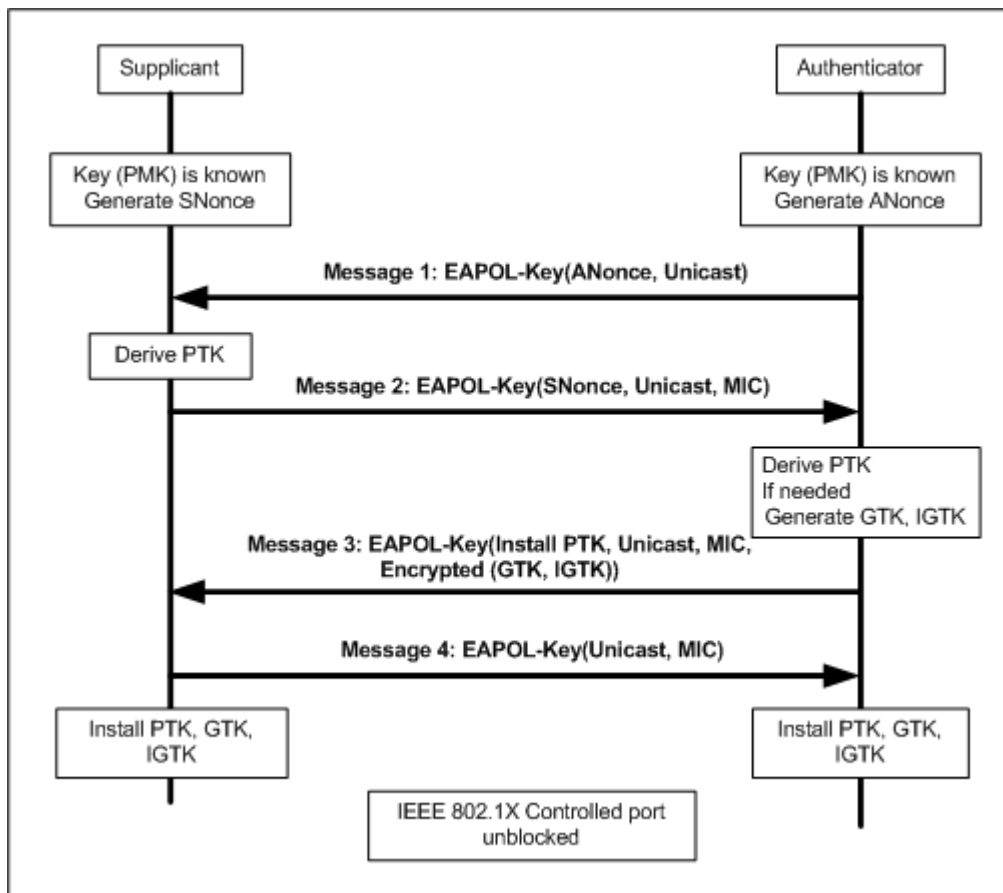


Figure 5-13—Establishing pairwise and group keys

Replace Figure 5-14 with the following figure:

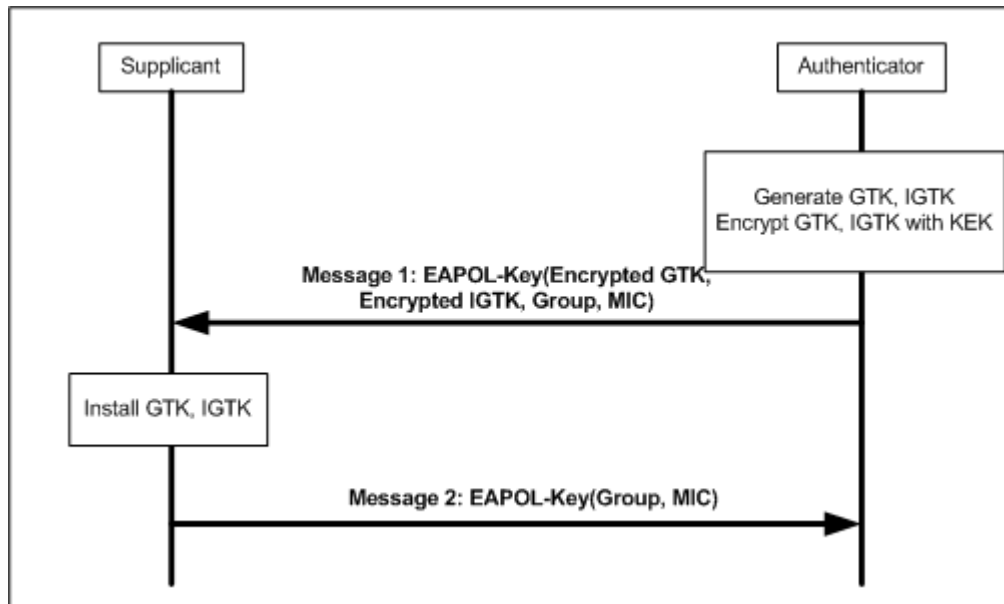


Figure 5-14—Delivery of subsequent group keys

5.8.2.2 Operations with PSK

Insert a new item after the third item in 5.8.2.2 as follows:

- If Management Frame Protection is negotiated, the IGTK and IGTK packet number are sent from the Authenticator to the Supplicant just as in the AS case. See Figure 5-13 and Figure 5-14.

5.8.5 PMKSA caching

Insert a new subclause (5.8.6) after 5.8.5 as follows:

5.8.6 Protection of broadcast and multicast Robust Management frames

When Management Frame Protection is negotiated, all group addressed Robust Management frames shall be encapsulated using the procedures defined in 11.12. This service provides integrity protection of group addressed Robust Management frames using BIP.

6. MAC service definition

6.1 Overview of MAC services

6.1.2 Security services

Change the text of 6.1.2 as follows:

Security services in IEEE Std 802.11 are provided by the authentication service and the TKIP, ~~and CCMP, and BIP~~ mechanisms. The scope of the security services provided is limited to station-to-station data and Robust Management frame transmissions-exchange. The data confidentiality service offered by an IEEE 802.11 TKIP ~~and CCMP~~ implementation is the protection of the MSDU. When CCMP is used, the data confidentiality service is provided for data frames and unicast Robust Management frames. For the purposes of this standard, TKIP and CCMP are viewed as logical services located within the MAC sublayer as shown in the reference model, Figure 5-10 (in 5.7). Actual implementations of the TKIP and CCMP services are transparent to the LLC and other layers above the MAC sublayer.

The security services provided by TKIP and CCMP in IEEE Std 802.11 are as follows:

- a) Data Confidentiality;
- b) Authentication; and
- c) Access control in conjunction with layer management.

BIP provides message integrity and access control for group addressed Robust Management frames.

During the authentication exchange, both parties exchange authentication information as described in Clause 8 and Clause 11A.

The MAC sublayer security services provided by TKIP, ~~and CCMP, and BIP~~ rely on information from nonlayer-2 management or system entities. Management entities communicate information to TKIP, ~~and CCMP, and BIP~~ through a set of MAC sublayer management entity (MLME) interfaces and MIB attributes; in particular, the decision tree for TKIP, ~~and CCMP, and BIP~~ defined in 8.7 is driven by MIB attributes.

The use of WEP for confidentiality, authentication, or access control is deprecated. The WEP algorithm is unsuitable for the purposes of this standard.

A STA that has associated with Management Frame Protection enabled shall not use pairwise cipher suite selectors WEP-40, WEP-104, TKIP, or "Use Group cipher suite."

7. Frame formats

7.1 MAC Frame formats

7.1.3 Frame fields

7.1.3.1 Frame control field

7.1.3.1.8 Protected Frame field

Change the text of 7.1.3.1.8 as follows:

The Protected Frame field is 1 bit in length. The Protected Frame field is set to 1 if the Frame Body field contains information that has been processed by a cryptographic encapsulation algorithm. The Protected Frame field is set to 1 only within data frames and within management frames of subtype Authentication, and unicast Robust Management frames. The Protected Frame field is set to 0 in all other frames. When the Protected Frame field is set to 1, the Frame Body field is protected utilizing the cryptographic encapsulation algorithm and expanded as defined in Clause 8. The Protected Frame field is set to 0 in Data frames of subtype Null Function, CF-ACK (no data), CF-Poll (no data), and CF-ACK+CF-Poll (no data) (see 8.3.2.2 and 8.3.3.1 that , which show that the frame body must be one octet or longer to apply the encapsulation).

7.2 Format of individual frame types

7.2.3 Management frames

7.2.3.3 Disassociation frame format

Change Table 7-9 and insert a NOTE at the end of the table as follows:

The frame body of a management frame of subtype Disassociation contains the information shown in Table 7-9.

Table 7-9—Disassociation frame body

Order	Information
1	Reason Code
2 — (Last – 1)	One or more vendor-specific information elements may appear in this frame.
Last	<u>The Management MIC IE (MMIE) is present when Management Frame Protection is enabled at the AP and the frame is a group addressed frame.</u>
NOTE—The MMIE appears after all fields that it protects. Therefore, it appears last in the frame body to protect the frames as specified in 8.3.4.	

7.2.3.5 Association Response frame format

Insert order 13 into Table 7-11 as follows:

The frame body of a management frame of subtype Association Response contains the information shown in Table 7-11.

Table 7-11—Association Response frame body

Order	Information	Notes
<u>13</u>	<u>Timeout Interval (Association Comeback time)</u>	<u>A Timeout Interval information element containing the Association Comeback time is present when dot11RSNAEnabled is true.</u> <u>dot11RSNAProtectedManagementFramesEnabled is true and the association request is rejected with a status code 30.</u>
Last	Vendor Specific	One or more vendor-specific information elements may appear in this frame. This information element follows all other information elements.

7.2.3.7 Reassociation Response frame format

Insert order 15 into Table 7-13 as follows:

The frame body of a management frame of subtype Association Response contains the information shown in Table 7-13.

Table 7-13—Reassociation Response frame body

Order	Information	Notes
<u>15</u>	<u>Timeout Interval (Association Comeback time)</u>	<u>A Timeout Interval information element containing the Association Comeback time is present when dot11RSNAEnabled is true.</u> <u>dot11RSNAProtectedManagementFramesEnabled is true and the reassociation is rejected with status code 30.</u>
Last	Vendor Specific	One or more vendor-specific information elements may appear in this frame. This information element follows all other information elements.

7.2.3.11 Deauthentication

Change Table 7-18 and insert a NOTE at the end of the table as follows:

The frame body of a management frame of subtype Deauthentication contains the information shown in Table 7-18.

Table 7-18—Deauthentication frame body

Order	Information
1	Reason code
2 — (Last – 1)	One or more vendor-specific information elements may appear in this frame. ~~This information element follows all other information elements.~~
Last	<u>The Management MIC IE (MMIE) is present when Management Frame Protection is enabled at the AP and the frame is a group addressed frame.</u>
NOTE—The MMIE appears after all fields that it protects. Therefore, it appears last in the frame body to protect the frames as specified in 8.3.4.	

7.2.3.12 Action frame format

Change Table 7-19 and insert a NOTE at the end of the table as follows:

The frame body of a management frame of subtype Action contains the information shown in Table 7-19.

Table 7-19—Action frame body

Order	Information
1	Action
2 — (Last – 1)	One or more vendor-specific information elements may appear in this frame. ~~This information element follows all other information elements.~~
Last	<u>The Management MIC IE (MMIE) is present when Management Frame Protection is enabled at the AP and the frame is a group addressed Robust Action frame.</u>
NOTE—The MMIE appears after any fields that it protects. Therefore, it appears last in the frame body to protect the frames as specified in 8.3.4.	

7.3 Management frame body components**7.3.1 Fields that are not information elements****7.3.1.9 Status Code field**

Change Table 7-23 as follows:

Table 7-23—Status codes

Status code	Meaning
29–34	Reserved
30	<u>Association request rejected temporarily; try again later</u>
31	<u>Robust Management frame policy violation</u>

7.3.1.11 Action field

Change Table 7-24 as follows:

Table 7-24—Category values

Code	Meaning	See subclause	<u>Robust</u>
0	Spectrum management	7.4.1	<u>Yes</u>
1	QoS	7.4.2	<u>Yes</u>
2	DLS	7.4.3	<u>Yes</u>
3	Block Ack	7.4.4	<u>Yes</u>
4	Public	7.4.7	<u>No</u>
5	Radio measurement	7.4.6	<u>Yes</u>
6	Fast BSS Transition	7.4.8	<u>Yes</u>
~~7~~	<u>Reserved</u>	—	—
~~8~~	<u>SA Query</u>	<u>7.4.9</u>	<u>Yes</u>
~~9~~	<u>Protected Dual of Public Action</u>	<u>7.4</u>	<u>Yes</u>
10–125 ~~6–126~~	Reserved	—	—
~~126~~	<u>Vendor-specific Protected</u>	<u>7.4.5</u>	<u>Yes</u>
127	Vendor-specific	7.4.5	<u>No</u>
128–255	Error	—	—

7.3.2 Information elements

Change the second to last paragraph in 7.3.2 as follows:

A STA that encounters an unknown or reserved element ID value in a management frame received without error shall ignore that element and shall parse any remaining management frame body for additional information elements with recognizable element ID values. The frame body components specified for many management subtypes result in elements ordered by ascending element ID, with the exception of the MIC Management IE (7.3.2.55). If present, the MIC Management IE appears at the end of the Robust Management frame body.

Change Table 7-26 as follows (note that the entire table is not shown):

Table 7-26—Element IDs

Information Element	Element ID	Length (in octets)	Extensible
Fast BSS Transition (FTIE) (see 7.3.2.48)	55	84 to 257	Yes
Timeout interval (see 7.3.2.49)	56	7	
RIC Data (RDIE) (see 7.3.2.50)	57	6	
DSE Registered Location (see 7.3.2.52)	58	22	
Supported Regulatory Classes (see 7.3.2.54)	59	4 to 255	
Extended Channel Switch Announcement (see 7.3.2.53)	60	6	
Reserved	61–62		
BSS Average Access Delay (see 7.3.2.39)	63	3	Yes
Antenna Information (see 7.3.2.40)	64	3	Yes
RSNI (see 7.3.2.41)	65	3	Yes
Measurement Pilot Transmission Information (see 7.3.2.42)	66	3 to 257	Subelements
BSS Available Admission Capacity (see 7.3.2.43)	67	4 to 28	Yes
BSS AC Access Delay (see 7.3.2.44)	68	6	Yes
Reserved	69		
RRM Enabled Capabilities (see 7.3.2.45)	70	7	Yes
Multiple BSSID (see 7.3.2.46)	71	3 to 257	Subelements
Reserved	72–74		
RIC Descriptor (see 7.3.2.51)	75	3 to 257	
<u>Management MIC [see 7.3.2.55 (MMIE)]</u>	<u>76</u>	<u>18</u>	
Reserved	~~77~~ –126		

7.3.2.25 RSN information element

Change the first paragraph of 7.3.2.25 as follows:

The RSN information element contains authentication and pairwise cipher suite selectors, a single group data cipher suite selector, an RSN Capabilities field, the PMK identifier (PMKID) count, ~~and~~ PMKID list, ~~and a single group management cipher suite selector.~~ See Figure 7-72. All STAs implementing RSNA ~~shall~~ support this element. The size of the RSN information element is limited by the size of an information element, which is 255 octets. Therefore, the number of pairwise cipher suites, AKM suites, and PMKIDs is limited.

Replace Figure 7-72 with the following figure:

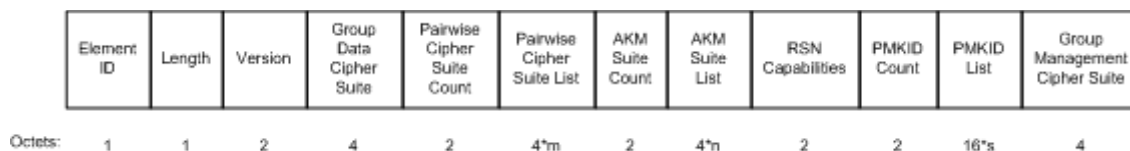


Figure 7-72—RSN Information Element format

Change the third paragraph in 7.3.2.25 as follows:

All fields use the bit convention from 7.1.1. The RSN information element shall contain up to and including the Version field. All fields after the Version field are optional. If any ~~optional~~ non-zero length field is absent, then none of the subsequent fields ~~are~~ shall be included.

Change the NOTE at the end of 7.3.2.25 as follows:

NOTE—The following represent sample information elements:

802.1X authentication, CCMP pairwise and group data cipher suites (WEP-40, WEP-104, and TKIP not allowed):

```
30, // information element id, 48 expressed as Hex value
14, // length in octets, 20 expressed as Hex value
01 00, // Version 1
00 0F AC 04, // CCMP as group data key cipher suite
01 00, // pairwise cipher suite count
00 0F AC 04, // CCMP as pairwise cipher suite
01 00, // authentication count
00 0F AC 01 // IEEE 802.1X authentication
00 00 // No capabilities
```

802.1X authentication, CCMP pairwise and group data cipher suites (WEP-40, WEP-104, and TKIP not allowed), preauthentication supported:

```
30, // information element id, 48 expressed as Hex value
14, // length in octets, 20 expressed as Hex value
01 00, // Version 1
00 0F AC 04, // CCMP as group data key cipher suite
01 00, // pairwise cipher suite count
00 0F AC 04, // CCMP as pairwise cipher suite
```