



**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 2: Fast Basic Service Set (BSS)
Transition**

IEEE Computer Society

Sponsored by the
LAN/MAN Standards Committee

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

15 July 2008

IEEE Std 802.11r™-2008
(Amendment to
IEEE Std 802.11™-2007
as amended by
IEEE Std 802.11k™-2008)

802.11r™

Authorized licensed use limited to: Johns Hopkins University. Downloaded on June 23, 2025 at 20:52:22 UTC from IEEE Xplore. Restrictions apply.

**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 2: Fast Basic Service Set (BSS)
Transition**

Sponsored by

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

Approved 9 May 2008

IEEE-SA Standards Board

Abstract: This amendment specifies the extensions to IEEE Std 802.11-2007 for wireless local area networks (WLANs) providing mechanisms for fast basic service set (BSS) transition.

Keywords: LAN, local area network, wireless LAN, WLAN

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

Copyright © 2008 by the Institute of Electrical and Electronics Engineers, Inc.
All rights reserved. Published 15 July 2008. Printed in the United States of America.

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

PDF: ISBN 973-07381-5442-0 STD95794
Print: ISBN 973-07381-5423-7 STDPD95794

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. When a document is more than five years old and has not been reaffirmed, it is reasonable to conclude that its contents, although still of some value, do not wholly reflect the present state of the art. Users are cautioned to check to determine that they have the latest edition of any IEEE Standard.

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

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

Comments for revision of IEEE Standards are welcome from any interested party, regardless of membership affiliation with IEEE. Suggestions for changes in documents should be in the form of a proposed change of text, together with appropriate supporting comments. Comments on standards and requests for interpretations should be submitted to the following address:

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 802.11-2007, IEEE Standard for information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements—Part 11: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications—Amendment 2: Fast Basic Service Set (BSS) Transition.

This amendment describes mechanisms that minimize the amount of time data connectivity is lost between the station (STA) and the distribution system (DS) during a basic service set (BSS) transition. The STA determines when to transition and to which access point (AP) to transition based on a number of factors, some of which may be out of the scope of this standard.

The following summarizes the typical behavior of the non-AP STA and AP when a transition occurs without fast BSS transition (FT) services:

- The STA uses scanning or neighbor reports to discover APs available for transition.
- The STA chooses a target AP and performs an IEEE 802.11 authentication exchange with that AP; typically this exchange will be an “open auth” exchange. During this time, the STA may still exchange data with the DS through its current AP.
- The STA sends a (Re)Association frame to establish a connection at the target AP.
- In a robust security network (RSN), the STA and the AP then generate and confirm matching temporal keys based on a preshared key (PSK) or an IEEE 802.1X authentication (which could be through an earlier preauthentication or key caching).
- In an RSN, the STA and AP install the keys and start to exchange data with the DS.
- For a quality of service (QoS) STA connected to a QoS AP, the STA may then request QoS resources by issuing one or more ADDTS (add traffic stream) requests.

The FT mechanism allows a STA to establish security and/or QoS state at the target AP prior to or during reassociation, avoiding delays in connecting to the DS after transition. The overall changes to the protocol do not introduce any new security vulnerabilities beyond the current IEEE 802.11 standard and its amendments. The FT mechanism preserves the behavior of legacy STAs and APs.

The FT time is the total transition time that starts after the receipt of the last acknowledged data frame sent within an originating BSS and ends after the receipt of the first acknowledged data frame sent within the destination BSS, while the non-AP STA transitions from one BSS to another using the FT mechanisms.

This amendment addresses solutions to two classes of network infrastructures from a QoS perspective: one where the transition-enabled AP is willing to provision QoS resources at reassociation time; and another where the AP needs to reserve the network infrastructure resources before transitioning.

This amendment does not specifically address the solution of when or where a STA will roam. Other tools give the STA information that could be used in making this decision.

IEEE 802.11 enables the AP to convey a BSS Load information element in Probe Response and Beacon frames. The BSS Load information element has three fields that indicate the number of associated STAs, the channel utilization for the BSS, and the available admission capacity. These QoS BSS metrics give information on the AP's ability to accept new QoS streams.

IEEE 802.11 defines the neighbor reports, which can assist in optimizing scanning.

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. The IEEE shall not be responsible for identifying patents or patent applications for which a license may be required to implement an IEEE standard or for conducting inquiries into the legal validity or scope of those patents that are brought to its attention. 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 and nondiscriminatory, reasonable terms and conditions to

applicants desiring to obtain such licenses. The IEEE makes no representation as to the reasonableness of rates, terms, and conditions of the license agreements offered by patent holders or patent applicants. Further information may be obtained from the IEEE Standards Department.

Participants

At the time this amendment was sent to sponsor ballot, the IEEE 802.11 Working Group had the following officers:

Stuart J. Kerry, *Chair*
Al Petrick, *Vice Chair, Treasurer and Chair, Task Group mb*
Harry R. Worstell, *Vice Chair*
Stephen McCann, *Secretary and Chair, Publicity Standing Committee*
Teik-Kheong Tan, *Chair, Wireless Next Generation Standing Committee*
Terry L. Cole, *Technical Editor and Assigned Number Authority*

Richard H. Paine, *Chair, Task Group k*
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 Sherma, *Chair, Task Group T*
Stephen McCann, *Chair, Task Group u*
Dorothy V. Stanley, *Chair, Task Group v & IETF Ad hoc Committee*
Jesse Walker, *Chair, Task Group w & JCT1 Ad hoc Committee*
Peter Ecclesine, *Chair, Task Group y*
Menzo Wentink, *Direct Link Setup Study Group*
Bob O'Hara, *QoS Extensions Study Group*
Ganesh Venkatesan, *Video Transport Stream Study Group*
Eldad Perahia, *Very High Throughput Study Group*
Darwin Engwer, *Co-Chair, IMT-Advanced Ad hoc Committee*

At the time this amendment was submitted to sponsor ballot, the Task Group r had the following officers:

Clint Chaplin, *Chair*
Michael Montemurro, *Secretary*
Bill Marshall, *Technical Editor*

When the IEEE 802.11 Working Group approved this amendment, the Working Group had the following membership:

| | | |
|-----------------------------|---------------------|-------------------|
| Osama Aboul-Magd | Michael Bahr | Broady Cash |
| Tomoko Adachi | Dennis Baker | Dave Cavalcanti |
| Carlos Aldana | Amit Bansal | Douglas Chan |
| Thomas Alexander | John Barr | Yi-Ming Chen |
| Keith Amann | Gal Basson | Hong Cheng |
| David Andrus | Anuj Batra | Paul Cheng |
| Takashi Aramaki | Moussa Bavafa | Aik Chindapol |
| Sirikiat Lek Ariyavisitakul | Mathilde Benveniste | Abhijit Choudhury |
| Larry Arnett | Bjorn Bjerke | Liwen Chu |
| Alex Ashley | Tony Braskich | Frank Ciotti |
| Arthur Astrin | George Bumiller | W. Steven Conner |
| Malik Audeh | Alistair Buttar | Charles Cook |
| Geert Awater | Pat Calhoun | Steven Crowley |
| Floyd Backes | Nancy Cam-Winget | David Cypher |
| David Bagby | James Carlo | Marc de Courville |
| | Pat Carson | |

Sabine Demel
Dee Denteneer
Susan Dickey
Yoshiharu Doi
John Dorsey
Roger Durand
Donald E. Eastlake, III
Hesham Elbakoury
Michael Ellis
Stephen Emeott
Marc Emmelmann
Darwin Engwer
Joseph Epstein
Leonid Epstein
Vinko Erceg
Lars Falk
Stefan Fechtel
Paul Feinberg
Matthew Fischer
Wayne Fisher
Michael Foegelle
Edoardo Gallizio
Matthew Gast
Sudhanshu Gaur
James Gilb
Tim Godfrey
Michelle Gong
Hrishikesh Gossain
Jeremy Gosteau
Sudheer Grandhi
Gordon Gray
Larry Green
Pratibha Gupta
Robert J. Hall
Mark Hamilton
Christopher Hansen
Daniel Harkins
Brian Hart
Amer Hassan
Myron Hattig
James Hauser
Shigenori Hayase
Kevin Hayes
Robert Heile
Eleanor Hepworth
Karl Heubaum
Guido Hiertz
Garth Hillman
Christopher Hinsz
Robert Hsieh
Wendong Hu
Jiyoung Huh
David Hunter
Yasuhiko Inoue
Marc Jalfon
Jorjeta Jetcheva
Lusheng Ji
Daniel Jiang
Jari Jokela
V. K. Jones
Padam Kafle
Carl Kain
Naveen Kakani
Srinivas Kandala

Assaf Kasher
Masato Kato
Douglas Kavner
Richard Kennedy
Stuart J. Kerry
John Ketchum
JinKyeong (Joseph) Kim
Joonsuk Kim
Kyeongsoo Kim
Tae-eun Kim
Guenter Kleindl
Jarkko Knecht
Mark Kobayashi
Benjamin Koh
Thomas Kolze
Gopal Krishnan
Jan Kruys
Thomas Kuehnel
Christian Kuhtz
Rajendra Kumar
Rajneesh Kumar
Thomas Kurihara
Joe Kwak
Jeremy Landt
Joseph Lauer
Jehun Lee
Jin Lee
Martin Lefkowitz
Uriel Lemberger
Joseph Levy
Azman-Osman Lim
Huashih Lin
Hang Liu
Michael Livshitz
Peter Loc
Peter Lojko
Dan Lubar
Krishna Sankar Madhavan Pillai
Alastair Malarky
Majid Malek
Jouni Malinen
Mahalingam Mani
William Marshall
Sudheer Matta
Matthieu Maupetit
William McFarland
Darren McNamara
Justin McNew
Irina Medvedev
Pratik Mehta
Sven Mesecke
Klaus Meyer
Robert Miller
Hidekazu Miyoshi
Fanny Mlinarsky
Patrick Mo
Andreas Molisch
Michael Montemurro
Gabriel Montenegro
Rajendra Moorti
Hitoshi Morioka
Yuichi Morioka
James Murphy
Peter Murray

Andrew Myles
Rohit Nabar
Yukimasa Nagai
Tetsuya Nakamura
Seigo Nakao
Ravi Nalamati
Sanjiv Nanda
Partha Narasimhan
Chiu Ngo
Eero Nikula
Gunnar Nitsche
Erwin Noble
Richard Noens
Hideaki Odagiri
Bob O'Hara
Eric Ojard
Chandra Olson
Satoshi Oyama
Richard Paine
Subra Parameswaran
Xavier Perez Costa
James Petranovich
Fahd Pirzada
Masood Pirzada
Victoria Poncini
Subbu Ponnuswamy
James Portaro
Henry Ptasinski
Emily Qi
Luke Qian
Jim Raab
Vinuth Rai
Ali Raissinia
Stephen Raymond
Ivan Reede
Joe Repice
Edward Reuss
Carlos Rios
Jon Rosdahl
Kazuyuki Sakoda
Atul Salhotra
Anil Sanwalka
Nicholas J Sargologos
Ambatipudi Sastry
Vincenzo Scarpa
Donald Schultz
Erik Schylander
Huai-Rong Shao
Neeraj Sharma
Suman Sharma
Stephen Shellhammer
Ian Sherlock
Kai Shi
Donghee Shim
D. J. Shyy
Massimiliano Siti
Matt Smith
Kapil Sood
Amjad Soomro
Srinivas Sreemanthula
Robert Stafford
Dorothy Stanley
Adrian Stephens
David Stephenson

Fabrice Stevens
Carl Stevenson
Guenael Strutt
Winston Sun
Shravan Surineni
Hideyuki Suzuki
Eiji Takagi
Mineo Takai
Daisuke Takeda
Tsuyoshi Tamaki
Allan Thomson
Jerry Thrasher
Alexander Tolpin
Jason Trachewsky
Solomon Trainin
Richard Van Nee

Allert van Zelst
Prabodh Varshney
Ganesh Venkatesan
Dalton Victor
George Vlantis
Tim Wakeley
Brad Wallace
Huihui Wang
Qi Wang
Xudong Wang
Dennis Ward
Deric Waters
Filip Weytjens
Stephen Whitesell
James Worsham

Charles Wright
Akiyoshi Yagi
Katsuhiko Yamada
Masaya Yamada
Takeshi Yamamoto
Tomoya Yamaura
Yuli Yang
Chi-Hsiang Yeh
Kanji Yokohira
Seiji Yoshida
Chris Young
Artur Zaks
Jinyun Zhang
Junping Zhang
Juan-Carlos Zuniga
Johnny Zweig

Major contributions were received from the following individuals:

Bernard Aboba
Peyush Agarwal
Areg Alimian
Keith Amann
Bob Beach
Stefan Berg
Florent Bersani
Tony Braskich
Bill Burr
Pat Calhoun
Alan Carlton
Nancy Cam-Winget
Clint Chaplin
James Chen
Lily Chen
Randy Chou
Frank Ciotti
Charles Clancy
Steve Connor
Anupam Datta
Chris Durand
Jon Edney
Steve Emeott
Darwin Engwer
Stefano Faccin
Paul Funk
Wolfgang Groting
Du Hanmei
Dan Harkins

Kevin Hayes
Haixiang He
Xiaoning He
Eleanor Hepworth
Katrin Hoepfer
Russ Housley
Srinivas Inguva
Marc Jalfon
Moo Ryong Jeong
Theodore Karoubalis
Toshiro Kawahara
Scott Kelly
Joe Kubler
Dirk Kuijsten
Rajneesh Kumar
Martin Lefkowitz
Jie Liang
Zhibin Lin
Peter Loc
Robert Love
Mani Mahalingam
Jouni Malinen
Bill Marshall
John C. Mitchell
Michael Montemurro
Tim Moore
Mike Moreton
Patrick Mourot
Paul Newton
Bob O'Hara

SooHong Daniel Park
Chris Polanec
Henry Ptasinski
Emily Qi
Arnab Roy
Marian Rudolf
Suresh Satapati
Ioanna Samprakou
Dan Simon
Floyd Simpson
Vishal Sinha
Matt Smith
Kapil Sood
Jeremy Spilman
Dorothy Stanley
Hui Tang
Chris Trecker
Sandy Turner
Jesse Walker
Stephen Wang
Fujio Watanabe
Jim Wendt
Michael Williams
Charles Wright
Gang Wu
Artur Zaks
Meiyuan Zhao
Juan-Carlos Zuniga
Johnny Zweig

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

Thomas Alexander
Keith Amann
Danilo Antonelli
Roger Berg
Gennaro Boggia
William Byrd
Peter J. Calderon
James Carlo

Juan Carreon
Jay Catelli
Clint Chaplin
Lidong Chen
Yi-Ming Chen
Hong Cheng
Aik Chindapol
Keith Chow

Charles Cook
Russell Dietz
Petar Djukic
Vern A. Dubendorf
Guy R. Duryee
Sourav Dutta
Donald E. Eastlake, III
Paul Eastman

Richard Eckard
Jonathan Edney
Joseph Epstein
Matthew Fischer
Wayne K. Fisher
C. Fitzgerald
Andre Fournier
Prince Francis
Avraham Freedman
Devon Gayle
Randall Groves
C. Guy
C. Hansen
Karl Heubaum
Russell Housley
David Hunter
Yasuhiko Inoue
Atsushi Ito
Raj Jain
Jari Jokela
Bobby Jose
Junghong Kao
Stuart J. Kerry
Brian Kiernan
Eunkyung Kim
Yongbum Kim

Yongho Kim
Joseph Kubler
Thomas Kurihara
Jeremy Landt
Daniel Levesque
Joseph Levy
Jan-Ray Liao
Jouni Malinen
Sudheer Matta
W. Kyle Maus
Stephen McCann
Gary Michel
R. Miller
Apurva Mody
Michael Montemurro
Jose Morales
Joseph Moran
Andrew Myles
Michael S. Newman
Richard Noens
Satoshi Obara
Bob O'Hara
Satoshi Oyama
Stephen Palm
Michael Probasco
Henry S. Ptasinski
Maximilian Riegel

Robert Robinson
Randall Safier
Osman Sakr
John Sargent
Peter Saunderson
Suman Sharma
Kapil Sood
Amjad Soomro
Srinivas Sreemanthula
Dorothy Stanley
Thomas Starai
Adrian P. Stephens
Rene Struik
Walter Struppler
Alourdes Sully
Masahiro Takagi
Solomon Trainin
Ganesh Venkatesan
John Vergis
Stanley Wang
Stephen Webb
Stephen Whitesell
Harry Worstell
Oren Yuen
Paolo Zangheri
Surong Zeng

When the IEEE-SA Standards Board approved this amendment on 9 May 2008, it had the following membership:

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

Victor Berman
Richard DeBlasio
Andy Drozd
Mark Epstein
Alexander Gelman
William R. Goldbach
Arnold M. Greenspan
Kenneth S. Hanus

Jim Hughes
Richard H. Hulett
Young Kyun Kim
Joseph L. Koepfinger*
John Kulick
David J. Law
Glenn Parsons
Ronald C. Petersen

Chuck Powers
Narayanan Ramachandran
Jon Walter Rosdahl
Robby Robson
Anne-Marie Sahazizia
Malcolm V. Thaden
Howard L. Wolfman
Don Wright

*Member Emeritus

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

Satish K. Aggarwal, *NRC Representative*
Michael H. Kelly, *NIST Representative*

Michelle Turner
IEEE Standards Program Manager, Document Development

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

CONTENTS

| | | |
|----------|-----------------------------------------------------------------------------------------|----|
| 2. | Normative references | 1 |
| 3. | Definitions | 2 |
| 4. | Abbreviations and acronyms | 3 |
| 5. | General description | 4 |
| 5.2 | Components of the IEEE 802.11 architecture | 4 |
| 5.2.3 | Distribution system (DS) concepts | 4 |
| 5.2.3.2 | Robust security network association (RSNA) | 4 |
| 5.4 | Overview of the services..... | 5 |
| 5.4.2 | Services that support the distribution services..... | 5 |
| 5.4.2.1 | Mobility types | 5 |
| 5.4.3 | Access control and data confidentiality services | 5 |
| 5.4.3.1 | Authentication..... | 5 |
| 5.4.3.4 | Key management | 5 |
| 5.4.3.7 | Fast BSS transition..... | 6 |
| 5.8 | IEEE Std 802.11 and IEEE Std 802.1X-2004 | 6 |
| 5.8.1 | IEEE 802.11 usage of IEEE Std 802.1X-2004 | 6 |
| 5.8.2 | Infrastructure functional model overview..... | 6 |
| 5.8.2.1 | Authentication and key management (AKM) operations with Authentication Server (AS)..... | 6 |
| 6. | Medium access control (MAC) service definition..... | 6 |
| 6.1 | Overview of MAC services | 6 |
| 6.1.2 | Security services | 6 |
| 7. | Frame formats | 7 |
| 7.2 | Format of individual frame types..... | 7 |
| 7.2.3 | Management frames..... | 7 |
| 7.2.3.1 | Beacon frame format | 7 |
| 7.2.3.4 | Association Request frame format..... | 7 |
| 7.2.3.5 | Association Response frame format | 7 |
| 7.2.3.6 | Reassociation Request frame format | 8 |
| 7.2.3.7 | Reassociation Response frame format..... | 8 |
| 7.2.3.9 | Probe Response frame format..... | 9 |
| 7.2.3.10 | Authentication frame format..... | 9 |
| 7.3 | Management frame body components..... | 10 |
| 7.3.1 | Fields that are not information elements..... | 10 |
| 7.3.1.1 | Authentication Algorithm Number field..... | 10 |
| 7.3.1.9 | Status Code field..... | 11 |
| 7.3.1.11 | Action field | 11 |
| 7.3.2 | Information elements | 11 |
| 7.3.2.25 | RSN information element (RSNIE)..... | 12 |
| 7.3.2.37 | Neighbor Report element..... | 13 |
| 7.3.2.47 | Mobility domain information element (MDIE)..... | 13 |
| 7.3.2.48 | Fast BSS transition information element (FTIE)..... | 14 |
| 7.3.2.49 | Timeout Interval information element (TIE)..... | 16 |
| 7.3.2.50 | RIC Data information element (RDIE)..... | 17 |

| | | |
|-----------|------------------------------------------------|----|
| 7.3.2.51 | RIC Descriptor information element | 17 |
| 7.4 | Action frame format details | 18 |
| 7.4.8 | FT Action frame details | 18 |
| 7.4.8.1 | FT Request frame..... | 18 |
| 7.4.8.2 | FT Response frame | 19 |
| 7.4.8.3 | FT Confirm frame | 20 |
| 7.4.8.4 | FT Ack frame | 20 |
| 8. | Security | 21 |
| 8.4 | RSNA Security association management | 21 |
| 8.4.1 | Security associations | 21 |
| 8.4.1.1 | Security association definitions | 21 |
| 8.4.6 | RSNA authentication in an ESS | 23 |
| 8.4.6.1 | Preauthentication and RSNA key management..... | 23 |
| 8.4.10 | RSNA security association termination | 23 |
| 8.5 | Keys and key distribution | 24 |
| 8.5.1 | Key hierarchy | 24 |
| 8.5.1.5 | FT key hierarchy | 24 |
| 8.5.2 | EAPOL-Key frames..... | 28 |
| 8.5.2.1 | EAPOL-Key frame notation | 29 |
| 8.5.3 | 4-Way Handshake | 30 |
| 8.5.3.1 | 4-Way Handshake Message 1 | 30 |
| 8.5.3.2 | 4-Way Handshake Message 2 | 30 |
| 8.5.3.3 | 4-Way Handshake Message 3 | 30 |
| 8.5.3.4 | 4-Way Handshake Message 4 | 30 |
| 8.5.4 | Group Key Handshake | 31 |
| 8.5.4.1 | Group Key Handshake Message 1 | 31 |
| 8.5.4.2 | Group Key Handshake Message 2 | 31 |
| 8.5.8 | PeerKey Handshake | 31 |
| 8.5.8.1 | SMK Handshake | 31 |
| 8.5.8.3 | STKSA rekeying..... | 32 |
| 8.5.8.4 | Error reporting | 32 |
| 10. | Layer management..... | 33 |
| 10.3 | MLME SAP interface | 33 |
| 10.3.4 | Authenticate | 33 |
| 10.3.4.1 | MLME-AUTHENTICATE.request | 33 |
| 10.3.4.2 | MLME-AUTHENTICATE.confirm | 33 |
| 10.3.4.3 | MLME-AUTHENTICATE.indication | 34 |
| 10.3.4.4 | MLME-AUTHENTICATE.response | 35 |
| 10.3.6 | Associate | 35 |
| 10.3.6.1 | MLME-ASSOCIATE.request..... | 35 |
| 10.3.6.2 | MLME-ASSOCIATE.confirm | 36 |
| 10.3.6.3 | MLME-ASSOCIATE.indication | 37 |
| 10.3.6.4 | MLME-ASSOCIATE.response | 37 |
| 10.3.7 | Reassociate..... | 38 |
| 10.3.7.1 | MLME-REASSOCIATE.request | 38 |
| 10.3.7.2 | MLME-REASSOCIATE.confirm | 38 |
| 10.3.7.3 | MLME-REASSOCIATE.indication | 39 |
| 10.3.7.4 | MLME-REASSOCIATE.response | 40 |
| 10.3.33 | MLME SAP interface for resource request | 40 |
| 10.3.33.1 | MLME-RESOURCE_REQUEST.request..... | 40 |

| | | |
|-----------|-----------------------------------------------------------|----|
| 10.3.33.2 | MLME-RESOURCE_REQUEST.indication | 41 |
| 10.3.33.3 | MLME-RESOURCE_REQUEST.response | 42 |
| 10.3.33.4 | MLME-RESOURCE_REQUEST.confirm | 42 |
| 10.3.33.5 | MLME-RESOURCE_REQUEST_LOCAL.request | 43 |
| 10.3.33.6 | MLME-RESOURCE_REQUEST_LOCAL.confirm | 44 |
| 10.3.34 | MLME SAP interface for remote requests | 45 |
| 10.3.34.1 | MLME-REMOTE_REQUEST.request | 45 |
| 10.3.34.2 | MLME-REMOTE_REQUEST.indication | 45 |
| 10.3.34.3 | MLME-REMOTE_REQUEST.confirm | 46 |
| 11. | MLME | 47 |
| 11.3 | STA authentication and association | 47 |
| 11.3.1 | Authentication and deauthentication | 47 |
| 11.3.1.1 | Authentication—originating STA | 47 |
| 11.3.1.2 | Authentication—destination STA | 47 |
| 11.3.2 | Association, reassociation, and disassociation | 48 |
| 11.3.2.3 | STA reassociation procedures | 48 |
| 11.3.2.4 | AP reassociation procedures | 48 |
| 11.4 | Traffic stream (TS) operation | 48 |
| 11.4.1 | Introduction | 48 |
| 11.4.3 | TS lifecycle | 48 |
| 11.4.4a | TS setup by resource request during a fast BSS transition | 49 |
| 11A. | Fast BSS transition | 50 |
| 11A.1 | Overview | 50 |
| 11A.2 | Key holders | 51 |
| 11A.2.1 | Introduction | 51 |
| 11A.2.2 | Authenticator key holders | 51 |
| 11A.2.3 | Supplicant key holders | 52 |
| 11A.3 | Capability and policy advertisement | 53 |
| 11A.4 | FT initial mobility domain association | 53 |
| 11A.4.1 | Overview | 53 |
| 11A.4.2 | FT initial mobility domain association in an RSN | 53 |
| 11A.4.3 | FT initial mobility domain association in a non-RSN | 56 |
| 11A.5 | FT Protocol | 57 |
| 11A.5.1 | Overview | 57 |
| 11A.5.2 | Over-the-air FT Protocol authentication in an RSN | 57 |
| 11A.5.3 | Over-the-DS FT Protocol authentication in an RSN | 59 |
| 11A.5.4 | Over-the-air FT Protocol authentication in a non-RSN | 61 |
| 11A.5.5 | Over-the-DS FT Protocol authentication in a non-RSN | 62 |
| 11A.6 | FT Resource Request Protocol | 63 |
| 11A.6.1 | Overview | 63 |
| 11A.6.2 | Over-the-air fast BSS transition with resource request | 63 |
| 11A.6.3 | Over-the-DS fast BSS transition with resource request | 66 |
| 11A.7 | FT reassociation | 68 |
| 11A.7.1 | FT reassociation in an RSN | 68 |
| 11A.7.2 | FT reassociation in a non-RSN | 69 |
| 11A.8 | FT authentication sequence | 70 |
| 11A.8.1 | Overview | 70 |
| 11A.8.2 | FT authentication sequence: contents of first message | 72 |
| 11A.8.3 | FT authentication sequence: contents of second message | 72 |
| 11A.8.4 | FT authentication sequence: contents of third message | 73 |

| | |
|----------------------------------------------------------------------------------------------|---------|
| 11A.8.5 FT authentication sequence: contents of fourth message | 73 |
| 11A.9 FT security architecture state machines | 75 |
| 11A.9.1 Introduction | 75 |
| 11A.9.2 R0KH state machine | 75 |
| 11A.9.2.1 R0KH state machine states | 76 |
| 11A.9.2.2 R0KH state machine variables | 77 |
| 11A.9.2.3 R0KH state machine procedures | 77 |
| 11A.9.3 R1KH state machine | 77 |
| 11A.9.3.1 R1KH state machine states | 79 |
| 11A.9.3.2 R1KH state machine variables | 80 |
| 11A.9.3.3 R1KH state machine procedures | 81 |
| 11A.9.4 S0KH state machine | 81 |
| 11A.9.4.1 S0KH state machine states | 81 |
| 11A.9.4.2 S0KH state machine variables | 82 |
| 11A.9.4.3 S0KH state machine procedures | 82 |
| 11A.9.5 S1KH state machine | 82 |
| 11A.9.5.1 S1KH state machine states | 82 |
| 11A.9.5.2 S1KH state machine variables | 85 |
| 11A.9.5.3 S1KH state machine procedures | 86 |
| 11A.10 Remote request broker (RRB) communication | 86 |
| 11A.10.1 Overview | 86 |
| 11A.10.2 Remote request broker (RRB) | 86 |
| 11A.10.3 Remote Request/Response frame definition | 87 |
| 11A.11 Resource request procedures | 88 |
| 11A.11.1 General | 88 |
| 11A.11.2 Resource information container (RIC) | 89 |
| 11A.11.3 Creation and handling of a resource request | 91 |
| 11A.11.3.1 STA procedures | 91 |
| 11A.11.3.2 AP procedures | 92 |
| Annex A (normative) Protocol Implementation Conformance Statements (PICS) proforma | 95 |
| Annex D (normative) ASN.1 encoding of the MAC and PHY MIB | 97 |
| Annex Q (normative) ANS.1 encoding of the RRM MIB | 108 |

List of figures

| | |
|-------------------------------------------------------------------------------|----|
| Figure 7-95c—BSSID Information field | 13 |
| Figure 7-95o1—MDIE format..... | 13 |
| Figure 7-95o3—FTIE format..... | 14 |
| Figure 7-95o4—MIC Control field..... | 14 |
| Figure 7-95o2—FT Capability and Policy field..... | 14 |
| Figure 7-95o5—Optional Parameter(s) field..... | 15 |
| Figure 7-95o6—GTK subelement format..... | 15 |
| Figure 7-95o7—GTK subelement’s Key Info subfield | 15 |
| Figure 7-95o8—TIE format..... | 16 |
| Figure 7-95o9—RDIE format..... | 17 |
| Figure 7-95o10—RIC Descriptor information element format..... | 17 |
| Figure 7-101i—FT Request frame format | 18 |
| Figure 7-101j—FT Response frame format..... | 19 |
| Figure 7-101k—FT Confirm frame format | 20 |
| Figure 7-101l—FT Ack frame format | 21 |
| Figure 8-22a—FT key hierarchy at an Authenticator..... | 24 |
| Figure 11-7—TS lifecycle | 49 |
| Figure 11A-1—FT key holder architecture | 51 |
| Figure 11A-2—FT initial mobility domain association in an RSN..... | 54 |
| Figure 11A-3—FT initial mobility domain association in a non-RSN | 56 |
| Figure 11A-4—Over-the-air FT Protocol in an RSN | 58 |
| Figure 11A-5—Over-the-DS FT Protocol in an RSN | 59 |
| Figure 11A-6—MLME interfaces for over-the-DS FT Protocol messages..... | 60 |
| Figure 11A-7—Over-the-air FT Protocol in a non-RSN..... | 62 |
| Figure 11A-8—Over-the-DS FT Protocol in a non-RSN..... | 62 |
| Figure 11A-9—Over-the-air FT Resource Request Protocol in an RSN | 64 |
| Figure 11A-10—Over-the-air FT Resource Request Protocol in a non-RSN | 65 |
| Figure 11A-11—Over-the-DS FT Resource Request Protocol in an RSN | 66 |
| Figure 11A-12—Over-the-DS FT Resource Request Protocol in a non-RSN | 67 |
| Figure 11A-13—R0KH state machine | 76 |
| Figure 11A-14—R1KH state machine, including portions of the SME (part 1)..... | 78 |
| Figure 11A-15—R1KH state machine, including portions of the SME (part 2)..... | 79 |
| Figure 11A-16—S0KH state machine | 81 |
| Figure 11A-17—S1KH state machine, including portions of the SME (part 1)..... | 83 |
| Figure 11A-18—S1KH state machine, including portions of the SME (part 2)..... | 84 |
| Figure 11A-19—Sample message flow for over-the-DS resource request | 87 |
| Figure 11A-20—Remote Request/Response frame format..... | 88 |
| Figure 11A-21—RIC-Request format | 89 |
| Figure 11A-22—Resource Request format | 89 |
| Figure 11A-23—Resource Request example #1 | 90 |
| Figure 11A-24—Resource Request example #2 | 90 |
| Figure 11A-25—RIC-Request example #1 | 90 |
| Figure 11A-26—RIC-Request example #2 | 90 |
| Figure 11A-27—RIC-Request example #3 | 90 |
| Figure 11A-28—RIC-Response format..... | 91 |
| Figure 11A-29—Example QoS RIC-Response | 91 |
| Figure 11A-30—Overview of RIC processing at an AP | 93 |

List of tables

| | |
|------------------------------------------------------------------------------------------|----|
| Table 7-8—Beacon frame body..... | 7 |
| Table 7-10—Association Request frame body..... | 7 |
| Table 7-11—Association Response frame body..... | 7 |
| Table 7-12—Reassociation Request frame body..... | 8 |
| Table 7-13—Reassociation Response frame body..... | 8 |
| Table 7-15—Probe Response frame body..... | 9 |
| Table 7-16—Authentication frame body..... | 9 |
| Table 7-17—Presence of challenge text information elements in Authentication frames..... | 10 |
| Table 7-23—Status codes..... | 11 |
| Table 7-24—Category values..... | 11 |
| Table 7-26—Element IDs..... | 11 |
| Table 7-34—AKM suite selectors..... | 12 |
| Table 7-43g—Subelement IDs..... | 15 |
| Table 7-43h—Timeout Interval Type field value..... | 16 |
| Table 7-57g—Action field values in FT Action frames..... | 18 |
| Table 7-43i—Resource type code in RIC Descriptor information element..... | 18 |
| Table 7-57h—FT Request frame body..... | 19 |
| Table 7-57j—FT Confirm frame body..... | 20 |
| Table 7-57i—FT Response frame body..... | 20 |
| Table 7-57k—FT Ack frame body..... | 21 |
| Table 11A-1—FT authentication information elements..... | 71 |
| Table 11A-2—Resource types and resource descriptor definitions..... | 89 |

Authorized licensed use limited to: Johns Hopkins University. Downloaded on June 23, 2025 at 20:52:22 UTC from IEEE Xplore. Restrictions apply.

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 2: Fast Basic Service Set (BSS) Transition

IMPORTANT NOTICE: *This standard is not intended to assure 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>.

(This amendment is based on IEEE Std 802.11™-2007, as amended by IEEE Std 802.11k™-2008.)

NOTE—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.

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

2. Normative references

Insert the following references in alpha numeric order into Clause 2:

FIPS PUB 180-2-2002, Secure Hash Standard.

FIPS SP800-38B, Dworkin, M., “Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication.”

3. Definitions

Change the following definitions in Clause 3 as indicated:

3.97 pairwise master key (PMK): ~~The highest order key used within this standard. The PMK may be derived from a key generated by an Extensible Authentication Protocol (EAP) method or may be obtained directly from a preshared key (PSK).~~

3.99 pairwise transient key (PTK): ~~A value that is derived from the pairwise master key (PMK), Authenticator address (AA), Supplicant address (SPA), Authenticator nonce (ANonce), and Supplicant nonce (SNonce) using the pseudo-random function (PRF) and that is split up into as many as five keys, i.e. temporal encryption key, two temporal message integrity code (MIC) keys, EAPOL-Key encryption key (KEK), EAPOL-Key confirmation key (KCK). A concatenation of session keys derived from the pairwise master key (PMK) or from the PMK-R1. Its components include a key confirmation key (KCK), a key encryption key (KEK), and one or more temporal keys that are used to protect information exchanged over the link.~~

3.130 robust security network association (RSNA) key management: Key management that includes the 4-Way Handshake, the 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.

Insert the following new definitions in alphabetical order into Clause 3, renumbering as necessary:

3.193 fast basic service set (BSS) transition: A station (STA) movement that is from one BSS in one extended service set (ESS) to another BSS within the same ESS and that minimizes the amount of time that data connectivity is lost between the STA and the distribution system (DS).

3.194 fast basic service set (BSS) transition (FT) 4-Way Handshake: A pairwise key management protocol used during FT initial mobility domain association. This handshake confirms mutual possession of a pairwise master key, the PMK-R1, by two parties and distributes a group temporal key (GTK).

3.195 fast basic service set (BSS) transition (FT) initial mobility domain association: The first association or first reassociation procedure within a mobility domain, during which a station (STA) indicates its intention to use the FT procedures.

3.196 mobility domain: A set of basic service sets (BSSs), within the same extended service set (ESS), that support fast BSS transitions between themselves and that are identified by the set's mobility domain identifier (MDID).

3.197 mobility domain identifier (MDID): An identifier that names a mobility domain.

3.198 network access server (NAS) client: The client component of a NAS that communicates with the Authentication Server (AS).

3.199 over-the-air fast basic service set (BSS) transition (FT): An FT method in which the station (STA) communicates over a direct IEEE 802.11 link to the target access point (AP).

3.200 over-the-DS (distribution system) fast basic service set (BSS) transition (FT): An FT method in which the station (STA) communicates with the target access point (AP) via the current AP.

3.201 pairwise master key R0 (PMK-R0): The key at the first level of the fast basic service set (BSS) transition (FT) key hierarchy.

3.202 pairwise master key (PMK) R0 key holder (R0KH): The component of robust security network association (RSNA) key management of the Authenticator that is authorized to derive and hold the PMK-R0, derive the PMK-R1s, and distribute the PMK-R1s to the R1KHs.

3.203 pairwise master key (PMK) R0 key holder identifier (R0KH-ID): An identifier that names the holder of the PMK-R0 in the Authenticator.

3.204 pairwise master key R1 (PMK-R1): A key at the second level of the fast basic service set (BSS) transition (FT) key hierarchy.

3.205 pairwise master key (PMK) R1 key holder (R1KH): The component of robust security network association (RSNA) key management of the Authenticator that receives a PMK-R1 from the R0KH, holds the PMK-R1, and derives the PTKs.

3.206 pairwise master key (PMK) R1 key holder identifier (R1KH-ID): An identifier that names the holder of a PMK-R1 in the Authenticator.

3.207 pairwise master key (PMK) S0 key holder (S0KH): The component of robust security network association (RSNA) key management of the Supplicant that derives and holds the PMK-R0, derives the PMK-R1s, and provides the PMK-R1s to the S1KH.

3.208 pairwise master key (PMK) S0 key holder identifier (S0KH-ID): An identifier that names the holder of the PMK-R0 in the Supplicant.

3.209 pairwise master key (PMK) S1 key holder (S1KH): The component of robust security network association (RSNA) key management in the Supplicant that receives a PMK-R1 from the S0KH, holds the PMK-R1, and derives the PTKs.

3.210 pairwise master key (PMK) S1 key holder identifier (S1KH-ID): An identifier that names the holder of the PMK-R1 in the Supplicant.

3.211 pairwise transient key (PTK) name (PTKName): An identifier that names the PTK.

3.212 pairwise master key (PMK) R0 name (PMKR0Name): An identifier that names the PMK-R0.

3.213 pairwise master key (PMK) R1 name (PMKR1Name): An identifier that names a PMK-R1.

3.214 remote request broker (RRB): The component of the station management entity (SME) of an access point (AP) that supports fast basic service set (BSS) transitions over the distribution system (DS).

3.215 resource information container (RIC): A sequence of information elements that include resource request and response parameters.

4. Abbreviations and acronyms

Insert the following abbreviations in alphabetical order into Clause 4:

| | |
|--------------|------------------------------------------------------------------------------------------|
| AES-128-CMAC | advanced encryption standard (with 128-bit key) cipher-based message authentication code |
| FT | fast BSS transition |
| FTAA | fast BSS transition authentication algorithm |

| | |
|---------|---------------------------------------------------|
| FTIE | fast BSS transition information element |
| KDF | key derivation function |
| MDID | mobility domain identifier |
| MDIE | Mobility Domain information element |
| NAS | network access server |
| PMK-R0 | pairwise master key, first level |
| PMK-R1 | pairwise master key, second level |
| RDIE | RIC Data information element |
| RIC | resource information container |
| RRB | remote request broker |
| RSNIE | Robust Security Network information element |
| R0KH | PMK-R0 key holder in the Authenticator |
| R0KH-ID | PMK-R0 key holder identifier in the Authenticator |
| R1KH | PMK-R1 key holder in the Authenticator |
| R1KH-ID | PMK-R1 key holder identifier in the Authenticator |
| S0KH | PMK-R0 key holder in the Supplicant |
| S0KH-ID | PMK-R0 key holder identifier in the Supplicant |
| S1KH | PMK-R1 key holder in the Supplicant |
| S1KH-ID | PMK-R1 key holder identifier in the Supplicant |
| TIE | Timeout Interval information element |

5. General description

5.2 Components of the IEEE 802.11 architecture

5.2.3 Distribution system (DS) concepts

5.2.3.2 Robust security network association (RSNA)

Change the first paragraph of 5.2.3.2 as follows:

An RSNA defines a number of security features in addition to wired equivalent privacy (WEP) and IEEE 802.11 authentication. These features include the following:

- Enhanced authentication mechanisms for STAs
- Key management algorithms
- Cryptographic key establishment
- An enhanced data cryptographic encapsulation mechanism, called Counter mode with Cipher-block chaining Message authentication code Protocol (CCMP), and, optionally, Temporal Key Integrity Protocol (TKIP)
- Fast basic service set (BSS) transition (FT) mechanism

Each TS established by this resource request is placed in the accepted state. This state is an intermediate state between inactive and active. In the accepted state, the inactivity and suspension timers shall not be started for the TS. For a TS based on hybrid coordination function (HCF) controlled channel access (HCCA), the HC shall not generate CF-Poll for the TS.

The SME may take the resource/timing requirements of the TS in the accepted state into consideration before assigning any further resources to any other admitted or accepted TS, and in calculating the available admission capacity for the BSS Load information element.

The TS is moved to the active state once the STA performs a reassociation to the AP (see 11A.11.3). Once the TS becomes active, the inactivity and suspension timers are started.

If the reassociation timer times out and the TS is not yet in the active state, the TS goes back to the inactive state.

Insert the following clause (Clause 11A) after Clause 11:

11A. Fast BSS transition

11A.1 Overview

Fast BSS transition seeks to reduce the length of time that connectivity is lost between the STA and the DS during a BSS transition. The FT protocols are part of the reassociation service and only apply to STA transitions between APs within the same mobility domain within the same ESS.

The FT protocols require information to be exchanged during the initial association (or a later reassociation) between the non-AP STA and AP. The initial exchange is referred to as the *FT initial mobility domain association*. Subsequent reassociations to APs within the same mobility domain may make use of the FT protocols.

Two FT protocols are defined:

- *FT Protocol*. This protocol is executed when a STA makes a transition to a target AP and does not require a resource request prior to its transition.
- *FT Resource Request Protocol*. This protocol is executed when a STA requires a resource request prior to its transition.

For a STA to move from its current AP to a target AP utilizing the FT protocols, the message exchanges are performed using one of two methods:

- *Over-the-Air*. The STA communicates directly with the target AP using IEEE 802.11 authentication with the FT authentication algorithm.
- *Over-the-DS*. The STA communicates with the target AP via the current AP. The communication between the STA and the target AP is carried in FT Action frames between the STA and the current AP. Between the current AP and target AP, communication is via an encapsulation method described in 11A.10.3. The current AP converts between the two encapsulations.

APs advertise both capabilities and policies for supporting the FT protocols and methods.

NOTE—Throughout this clause, the notation *Authentication-Request* refers to an Authentication frame with the Authentication Transaction Sequence Number field set to 1; *Authentication-Response* refers to an Authentication frame with the Authentication Transaction Sequence Number field set to 2; *Authentication-Confirm* refers to an Authentication frame with the Authentication Transaction Sequence Number field set to 3; *Authentication-Ack* refers to an Authentication frame with the Authentication Transaction Sequence Number field set to 4. The first parameter to the above four messages is the authentication algorithm, such as Open System authentication algorithm (i.e., *Open* in figures in this clause) or FT authentication algorithm (i.e., *FTAA* in figures in this clause).

11A.2 Key holders

11A.2.1 Introduction

The FT key holder architecture, shown in Figure 11A-1, describes the FT key management entities and is defined in the context of the IEEE 802.11 basic reference model (see Figure 5-10 in 5.7).

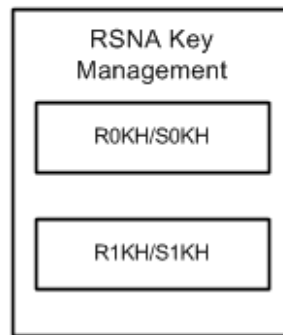


Figure 11A-1—FT key holder architecture

The R0KH and R1KH are part of AP SME RSNA key management. The computation of PMK-R0 and PMK-R1, and all the intermediate results in the computations, shall be restricted to the R0KH. The computation of PTK, and all intermediate results in its computation, shall be restricted to the R1KH.

The S0KH and S1KH are part of the non-AP STA SME RSNA key management. The computation of PMK-R0 and PMK-R1, and all the intermediate results in the computations, shall be restricted to the S0KH. The computation of PTK, and all intermediate results in its computation, shall be restricted to the S1KH.

11A.2.2 Authenticator key holders

The R0KH and R1KH are responsible for the derivation of keys in the FT key hierarchy. For fast BSS transition, the functions of the IEEE 802.1X Authenticator are distributed among the R0KH and R1KHs.

The R0KH interacts with the IEEE 802.1X Authenticator to receive the MSK resulting from an EAP authentication. The R1KH interacts with the IEEE 802.1X Authenticator to open the Controlled Port. Both the R0KH and R1KH interactions with the IEEE 802.1X Authenticator occur within the SME.

The R0KH derives the PMK-R0 for use in the mobility domain utilizing either the MSK (when the AKM negotiated is 00-0F-AC:3) or the PSK (when the AKM negotiated is 00-0F-AC:4). The R0KH shall be responsible for deriving a PMK-R1 for each R1KH within the mobility domain.

The R1KH and S1KH each derive the PTK.

Each R0KH-ID and R1KH-ID is assumed to be expressed as a unique identifier within the mobility domain. This identifier is communicated to the non-AP STA and other key holders. The R0KH-ID is bound into the PMK-R0 derivation and the R1KH-ID is bound into the PMK-R1 derivation.

The R0KH shall meet the following requirements:

- The R0KH shall be co-located with the network access server (NAS) Client functionality of the IEEE 802.1X Authenticator.

- The R0KH-ID shall be set to the identity of the co-resident NAS Client (e.g., NAS-Identifier as defined in RFC 2865 if RADIUS is used as the backend protocol). R0KH-ID shall not be longer than 48 octets to fit in the length limitation of the FTIE.
- When the PMK-R0 lifetime expires, the R0KH shall delete the PMK-R0 security association and shall revoke within the R0KH all PMK-R1s derived from the PMK-R0.
- The R0KH shall not expose the PMK-R0 to other parties.
- The R0KH shall not expose the PMK-R1 to parties other than the authorized R1KH.

The R1KH shall meet the following requirements:

- The R1KH-ID shall be set to a MAC address of the physical entity that stores the PMK-R1 and uses it to generate the PTK. That same MAC address shall be used to advertise the PMK-R1 identity to the STA and the R0KH.
- The R1KH shall derive and distribute the GTK to all connected STAs.
- When the PMK-R1 lifetime expires, the R1KH shall delete the PMK-R1 PMKSA and shall revoke all PTKSAs derived from the PMK-R1 using the MLME-DELETEKEYS primitive.
- The R1KH shall not expose the PMK-R1 to other parties.

The management information base (MIB) variables dot11FTR0KeyHolderID and dot11FTR1KeyHolderID shall contain the values of R0KH-ID and R1KH-ID as defined in this clause, respectively.

The R0KH and the R1KH are assumed to have a secure channel between them that can be used to exchange cryptographic keys without exposure to any intermediate parties. The cryptographic strength of the secure channel between the R0KH and R1KH is assumed to be greater than or equal to the cryptographic strength of the channels for which the keys will be used. This standard assumes that the key transfer includes the PMK-R1, the PMK-R1 PMKSA, the PMK-R1 context, and the associated key authorizations. The protocol for distribution of keying material from the R0KH to the R1KH is outside the scope of this standard.

The PMK-R1 distribution from the R0KH to the R1KHs within the same mobility domain shall satisfy the following assumptions:

- The R0KH authenticates a potential R1KH with the same identity as is included in the PMK-R1 derivation. The cryptographic strength of the authentication is assumed to be greater than or equal to the cryptographic strength of the authentication between the Supplicant and AS.
- The authorization of holding a PMK-R1 is based on the authentication of the R1KH.
- The protected channel provides confidentiality and integrity protection.

11A.2.3 Supplicant key holders

The S0KH and S1KH are responsible for the derivation of keys in the FT key hierarchy. The S0KH and S1KH are entities that are assumed to physically reside in the Supplicant.

The S0KH interacts with the IEEE 802.1X functional block (see Figure 5-10 in 5.7) to receive the MSK resulting from an EAP authentication. The S1KH interacts with 802.1X to open the Controlled Port. Both the S0KH and S1KH interactions with 802.1X occur within the SME of a STA.

The S0KH derives the PMK-R0 for use in the mobility domain utilizing either the MSK (when the AKM negotiated is 00-0F-AC:3) or the PSK (when the AKM negotiated is 00-0F-AC:4).

The S1KH shall derive the PTK mutually with the R1KH.

The S0KH and S1KH shall be identified by the SPA. The S0KH shall not expose the PMK-R0 to other parties and shall not expose the PMK-R1 to parties other than the authorized S1KH. The S1KH shall not expose the PMK-R1 to other parties.

11A.3 Capability and policy advertisement

The FT capability is advertised in the Beacon and Probe Response frames by including the MDIE. The MDIE is advertised in the Beacon and Probe Response frames to indicate the MDID, FT capability, and the FT policy.

The MDID field shall be the value of dot11FTMobilityDomainID. The Fast BSS Transition Policy bits in the MDIE, i.e., Fast BSS Transition over DS subfield and Resource Request Protocol Capability subfield, shall be set according to the values of the MIB variables dot11FTOver-DSEnabled, and dot11FTResourceRequestSupported, respectively.

NOTE—It is assumed by this standard that the Fast BSS Transition Policy bits in the MDIE are administered consistently across the mobility domain.

The capability is advertised in the Neighbor Report information element. See 11.11 and 7.3.2.37.

If an FTIE is included in a Request information element in a Probe Request frame, the FTIE in the Probe Response frame shall contain the R0KH-ID and R1KH-ID (set according to the values of the MIB variables dot11FTR0KeyHolderID and dot11FTR1KeyHolderID), and all other fields shall be set to 0.

11A.4 FT initial mobility domain association

11A.4.1 Overview

The FT initial mobility domain association is the first (re)association in the mobility domain, where the SME of the non-AP STA enables its future use of the FT procedures.

FT initial mobility domain association will typically be the first association within the ESS. In addition to association frames, reassociation frames are supported in the initial mobility domain association to enable both FT and non-FT APs to be present in a single ESS.

11A.4.2 FT initial mobility domain association in an RSN

The STA indicates its support for the FT procedures by including the MDIE in the (Re)Association Request frame and indicates its support of security by including the RSNIE. The AP responds by including the FTIE, MDIE, and RSNIE in the (Re)Association Response frame. After a successful IEEE 802.1X authentication (if needed), the STA and AP perform an FT 4-Way Handshake. At the end of the sequence, the IEEE 802.1X Controlled Port is opened, and the FT key hierarchy has been established. The message flow is shown in Figure 11A-2.

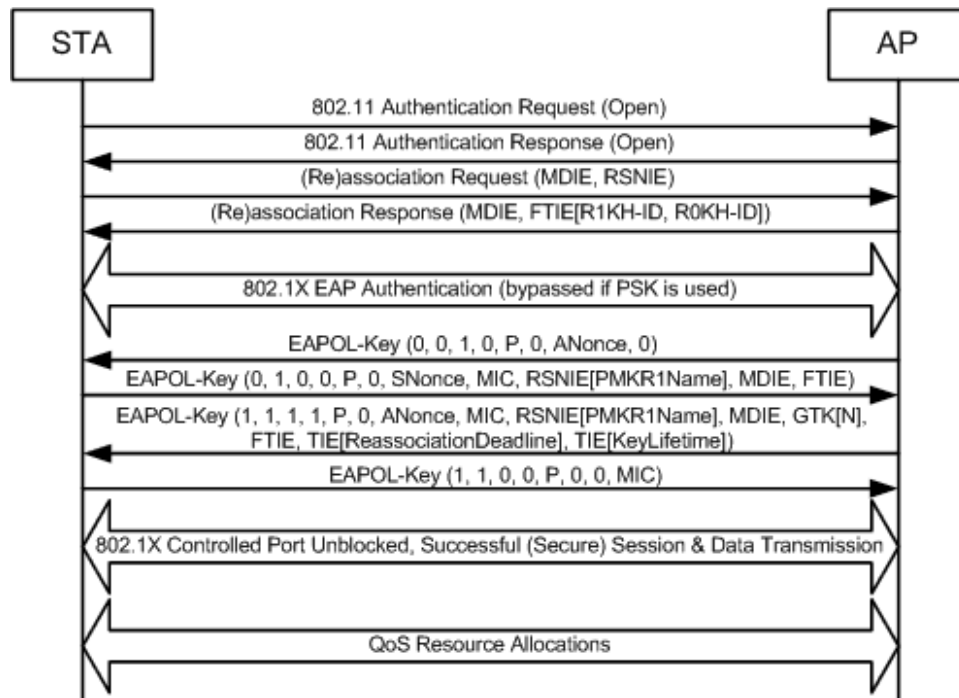


Figure 11A-2—FT initial mobility domain association in an RSN

The STA initiates the FT initial mobility domain association procedures by performing an IEEE 802.11 authentication using the Open System authentication algorithm.

STA→AP: Authentication-Request (Open System authentication algorithm)
 AP→STA: Authentication-Response (Open System authentication algorithm, Status)

The SME of the STA initiates the authentication exchange, through the use of the primitive MLME-AUTHENTICATE.request, and the SME of the AP responds with MLME-AUTHENTICATE.response primitive. See 11.3.1.

Upon successful IEEE 802.11 Open System authentication, the STA shall send a (Re)Association Request frame to the AP that includes the MDIE. The contents of the MDIE shall be the values advertised by the AP in its Beacon or Probe Response frames. Additionally, the STA includes its security capabilities in the RSNIE.

STA→AP: (Re)Association Request (MDIE, RSNIE)
 AP→STA: (Re)Association Response (MDIE, FTIE[R1KH-ID, R0KH-ID])

The SME of the STA initiates the (re)association through the use of the MLME-ASSOCIATE.request or MLME-REASSOCIATE.request primitive. The SME of the AP responds to the indication with MLME-ASSOCIATE.response or MLME-REASSOCIATE.response primitive. See 11.3.2.

If the contents of the MDIE received by the AP do not match the contents advertised in the Beacon and Probe Response frames, the AP shall reject the (Re)Association Request frame with status code 54 (i.e., Invalid MDIE). If an MDIE is present in the (Re)Association Request frame and the contents of the RSNIE do not indicate a negotiated AKM of Fast BSS Transition (suite type 00-0F-AC:3 or 00-0F-AC:4), the AP shall reject the (Re)Association Request frame with status code 43 (i.e., Invalid AKMP).

The (Re)Association Response frame from the AP shall contain an MDIE, with contents as presented in Beacon and Probe Response frames. The FTIE shall include the key holder identities of the AP, the R0KH-ID and R1KH-ID, set to the values of dot11FTR0KeyHolderID and dot11FTR1KeyHolderID, respectively. The FTIE shall have a MIC information element count of zero (i.e., no MIC present) and have ANonce, SNonce, and MIC fields set to 0.

On successful (re)association, the S0KH on the STA and the R0KH on the AP then proceed with an IEEE 802.1X authentication using EAPOL messages carried in IEEE 802.11 data frames. The S0KH shall use the value of R0KH-ID as the endpoint identifier of the NAS Client (NAS-Identifier if RADIUS is used) in the exchange as defined in IETF RFC 3748-2004 [B26].

Upon successful completion of the IEEE 802.1X authentication, the R0KH receives the MSK and authorization attributes. If a key hierarchy already exists for this non-AP STA belonging to the same mobility domain (i.e., having the same MDID), the R0KH shall delete the existing PMK-R0 security association and PMK-R1 security associations. It then calculates the PMK-R0, PMKR0Name, and PMK-R1 and makes the PMK-R1 available to the R1KH of the AP with which the STA is associated.

If the SME of the STA cannot authenticate the AS, then it shall disassociate with an MLME-DISASSOCIATE.request primitive. If the AS signals the Authenticator that the STA cannot be authenticated, then the SME of the AP shall disassociate with an MLME-DISASSOCIATE.request primitive.

If the MSK lifetime attribute is provided by the AS, the lifetime of the PMK-R0 shall not be more than the lifetime of the MSK. If the MSK lifetime attribute is not provided, the PMK-R0 lifetime shall be the value of the MIB variable dot11FTR0KeyLifetime. For PSK, the PMK-R0 lifetime shall be the value of the MIB variable dot11FTR0KeyLifetime. The lifetime of the PMK-R1s and PTK shall be the same as the lifetime of PMK-R0. When the key lifetime expires, each key holder shall delete its respective PMK-R0, PMK-R1, and PTK SAs.

The R1KH and S1KH then perform an FT 4-Way Handshake. The EAPOL-Key frame notation is defined in 8.5.2.1.

| | |
|------------|---------------------------------------------------------------------------------------------------------------------------------------|
| R1KH→S1KH: | Data(EAPOL-Key(0, 0, 1, 0, P, 0, 0, ANonce, 0)) |
| S1KH→R1KH: | Data(EAPOL-Key(0, 1, 0, 0, P, 0, 0, SNonce, MIC, RSNIE[PMKR1Name], MDIE, FTIE)) |
| R1KH→S1KH: | Data(EAPOL-Key(1, 1, 1, 1, P, 0, 0, ANonce, MIC, RSNIE[PMKR1Name], MDIE, GTK[N], FTIE, TIE[ReassociationDeadline], TIE[KeyLifetime])) |
| S1KH→R1KH: | Data(EAPOL-Key(1, 1, 0, 0, P, 0, 0, 0, MIC)) |

The message sequence is similar to that of 8.5.3. The contents of each message shall be as described in 8.5.3 except as follows:

- Message 2: the S1KH shall include the PMKR1Name in the PMKID field of the RSNIE. The PMKR1Name shall be as calculated by the S1KH according to the procedures of 8.5.1.5.4; all other fields of the RSNIE shall be identical to the RSNIE present in the (Re)Association Request frame. The S1KH shall include the FTIE and MDIE; the FTIE and MDIE shall be the same as those provided in the AP's (Re)Association Response frame.
- Message 3: the R1KH shall include the PMKR1Name in the PMKID field of the RSNIE. The PMKR1Name shall be as calculated by the R1KH according to the procedures of 8.5.1.5.4 and shall be the same as the PMKR1Name in Message #2; all other fields of the RSNIE shall be identical to the RSNIE present in the Beacon or Probe Response frames. The R1KH shall also include the FTIE, the MDIE, the reassociation deadline timeout in the TIE[ReassociationDeadline], and the PTK key lifetime in the TIE[KeyLifetime]. The FTIE and MDIE shall be the same as in the (Re)Association

Response frame. The reassociation deadline shall be set to the minimum of $\text{dot11FTReassociationDeadline}$ and the key lifetime.

NOTE—“Data()” indicates the message is an IEEE 802.11 data frame.

It is assumed by this standard that the reassociation deadline is administered consistently across the mobility domain. The mechanism for such consistent administration is outside the scope of this standard.

The PTK shall be calculated by the R1KH and S1KH according to the procedures given in 8.5.1.5.5.

Upon completion of a successful FT 4-Way Handshake, the IEEE 802.1X Controlled Port shall be opened on both the non-AP STA and the AP. Subsequent EAPOL-Key frames shall use the key replay counter to detect replayed messages.

Upon completion of a successful FT 4-Way Handshake, the PTK key lifetime timer is initiated to ensure that the lifetime of the PTKSA is no longer than the value provided in the TIE[KeyLifetime] sent in Message 3.

Once the PTKSA key lifetime expires, as indicated by the TIE[KeyLifetime] , to continue its association in the mobility domain the non-AP STA shall perform the FT initial mobility domain association procedures. If the AP sends a Deauthentication or Disassociation frame to the non-AP STA with reason code 2 (i.e., Previous authentication no longer valid), then to continue its association in the mobility domain, the non-AP STA shall perform the FT initial mobility domain association procedures with any AP in the mobility domain. If the Supplicant EAPOL state machines are triggered to send an EAPOL-Start packet after a successful initial mobility domain association, the non-AP STA shall perform the FT initial mobility domain association procedures.

11A.4.3 FT initial mobility domain association in a non-RSN

In this sequence, the STA utilizes the FT procedures by including the MDIE in the (Re)Association Request frame. The AP responds by including the MDIE in the (Re)Association Response frame. The message flow is shown in Figure 11A-3.

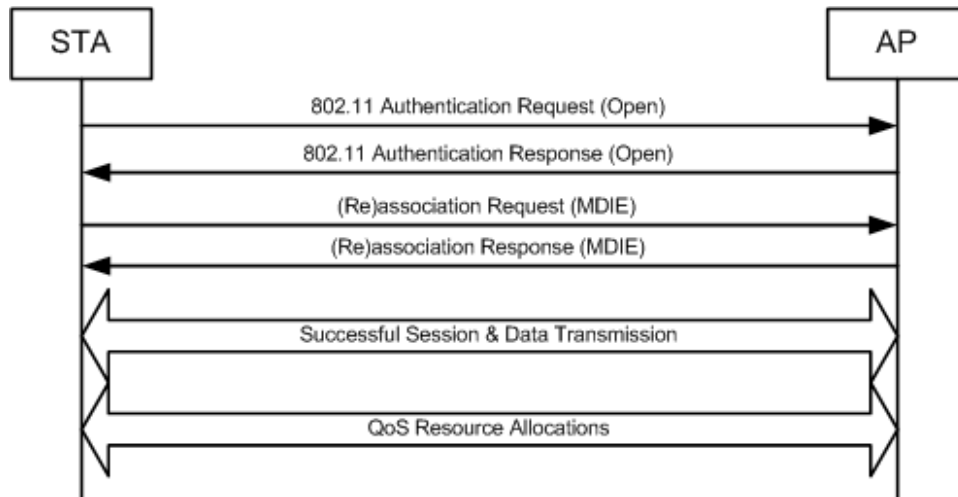


Figure 11A-3—FT initial mobility domain association in a non-RSN

The STA initiates the FT initial mobility domain association procedures by performing an IEEE 802.11 authentication using the Open System authentication algorithm.

STA→AP: Authentication-Request (Open System authentication algorithm)
 AP→STA: Authentication-Response (Open System authentication algorithm, Status)

The SME of the STA initiates the authentication exchange through the use of the primitive MLME-AUTHENTICATE.request primitive, and the SME of the AP responds with MLME-AUTHENTICATE.response primitive. See 11.3.1.

Upon successful IEEE 802.11 Open System authentication, the STA shall send a (Re)Association Request frame to the AP and shall include the MDIE. The contents of the MDIE shall be the values advertised by the AP in its Beacon or Probe Response frames.

STA→AP: (Re)Association Request (MDIE)
 AP→STA: (Re)Association Response (MDIE)

The SME of the STA initiates the (Re)association through the use of the MLME-ASSOCIATE.request or MLME-REASSOCIATE.request primitive. The SME of the AP responds to the indication with MLME-ASSOCIATE.response or MLME-REASSOCIATE.response primitive. See 11.3.2.

If the contents of the MDIE received by the AP do not match the contents advertised in the Beacon and Probe Response frames, the AP shall reject the (Re)Association Request frame with status code 54 (i.e., Invalid MDIE).

The (Re)Association Response frame from the AP shall contain an MDIE, with contents as presented in Beacon and Probe Response frames.

On successful (re)association, the AP and the non-AP STA shall transition to State 3 (as defined in 11.3) to enable data frame transmission.

11A.5 FT Protocol

11A.5.1 Overview

STAs with dot11FastBSSTransitionEnabled set to TRUE shall support the FT Protocol.

The FT Protocol supports resource requests as part of the reassociation. The optional FT Resource Request Protocol (see 11A.6) supports resource requests prior to reassociation.

A STA shall not use any authentication algorithm except the FT authentication algorithm when using the FT Protocol.

11A.5.2 Over-the-air FT Protocol authentication in an RSN

The over-the-air FT Protocol in an RSN is shown in Figure 11A-4.

The STA and AP use the FT authentication sequence to specify the PMK-R1 security association and to provide values of SNonce and ANonce that enable a liveness proof, replay protection, and PTK key separation. This exchange enables a fresh PTK to be computed in advance of reassociation. The PTKSA is used to protect the subsequent reassociation transaction, including the optional RIC-Request.

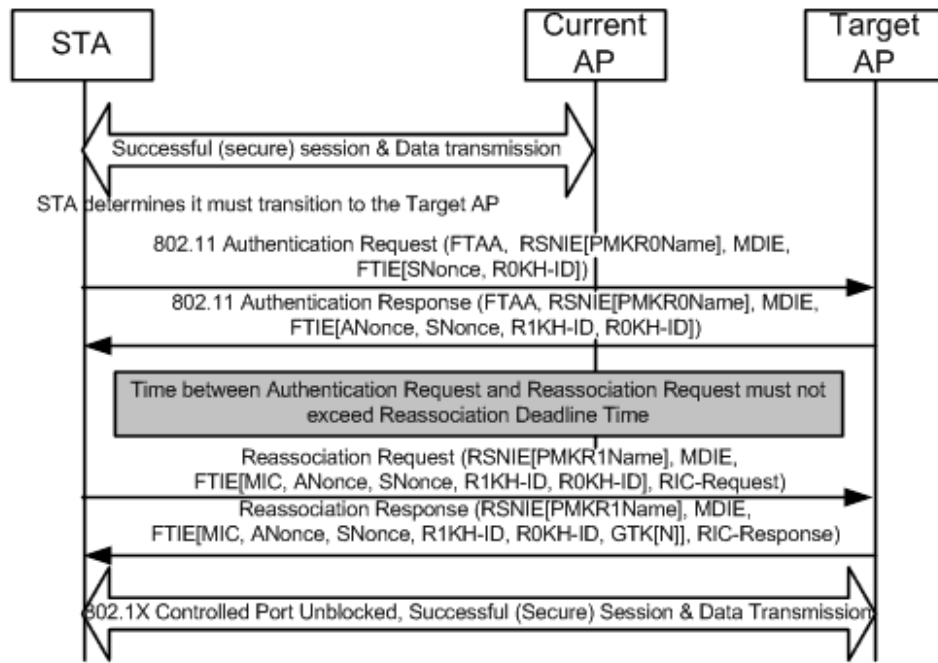


Figure 11A-4—Over-the-air FT Protocol in an RSN

To perform an over-the-air fast BSS transition to a target AP, the STA and target AP shall perform the following exchange:

- STA→Target AP: Authentication-Request (FTAA, 0, RSNIE[PMKR0Name], MDIE, FTIE[SNonce, R0KH-ID])
- Target AP→STA: Authentication-Response (FTAA, Status, RSNIE[PMKR0Name], MDIE, FTIE[ANonce, SNonce, R1KH-ID, R0KH-ID])

The SME of the STA initiates the authentication exchange, through the use of the MLME-AUTHENTICATE.request primitive, and the SME of the AP responds with an MLME-AUTHENTICATE.response primitive. See 11.3.1. The MLME primitives for Authentication when the FT authentication algorithm is selected use only Authentication transaction sequence number values 1 and 2.

In the Authentication Request frame, the SA field of the message header shall be set to the MAC address of the STA, and the DA field of the message header shall be set to the BSSID of the target AP. The information elements in the frame, and their required contents, shall be as given in 11A.8.2.

If the contents of the MDIE received by the AP do not match the contents advertised in the Beacon and Probe Response frames, the AP shall reject the Authentication Request with status code 54 (i.e., Invalid MDIE). If the Authentication Request frame contains an authentication algorithm set to FT authentication and the contents of the RSNIE do not indicate a negotiated AKM of Fast BSS Transition (suite type 00-0F-AC:3 or 00-0F-AC:4), the AP shall reject the Authentication Request with status code 43 (i.e., Invalid AKMP). If the FTIE in the FT Request frame contains an invalid R0KH-ID, the AP shall reject the FT Request frame with status code 55 (i.e., Invalid FTIE). If the RSNIE in the Authentication Request frame contains an invalid PMKR0Name and the AP has determined that it is an invalid PMKR0Name, the AP shall reject the Authentication Request with status code 53 (i.e., Invalid PMKID). If the requested R0KH is not reachable, the AP shall respond to the Authentication Request with status code 28 (i.e., R0KH unreachable). If the non-AP STA selects a pairwise cipher suite in the RSNIE that is different from the ones used in the Initial mobility domain association, then the AP shall reject the Authentication Request with status code 19

(i.e., Invalid Pairwise Cipher). Subsequent to a rejection of an Authentication Request, the STA may retry the Authentication Request.

In the Authentication Response frame, the SA field of the message header shall be set to the BSSID of the target AP, and the DA field of the message header shall be set to the MAC address of the STA. The Status Code field shall be a value from the options listed in 7.3.1.9. The information elements in the frame, and their required contents, shall be as given in 11A.8.3.

The R1KH of the target AP uses the value of PMKR0Name and other information in the frame to calculate PMKR1Name. If the target AP does not have the key identified by PMKR1Name, it may retrieve that key from the R0KH identified by the STA. See 11A.2. Upon receiving a new PMK-R1 for a STA, the target AP shall delete the prior PMK-R1 security association and PTKSAs derived from the prior PMK-R1.

The STA and the target AP compute the PTK and PTKName using the PMK-R1, PMKR1Name, ANonce, and SNonce, as specified in 8.5.1.5.5. The PTKSA shall be deleted by the target AP if it does not receive a Reassociation Request frame from the STA within the reassociation deadline timeout value.

If the STA does not receive a response to the Authentication Request frame, it may reissue the request following the restrictions given for Authentication frames in 11.3. If the Status Code field value returned by the target AP is 0, indicating success, the STA and target AP transition to State 2 (as defined in 11.3); the STA may continue with reassociation (11A.7.1). Handling of errors returned in the Status Code field shall be as specified in 11.3.

11A.5.3 Over-the-DS FT Protocol authentication in an RSN

A STA shall not initiate an over-the-DS FT authentication to a target AP whose MDIE contains the Fast BSS Transition over DS bit set to 0.

The over-the-DS FT Protocol in an RSN is shown in Figure 11A-5.

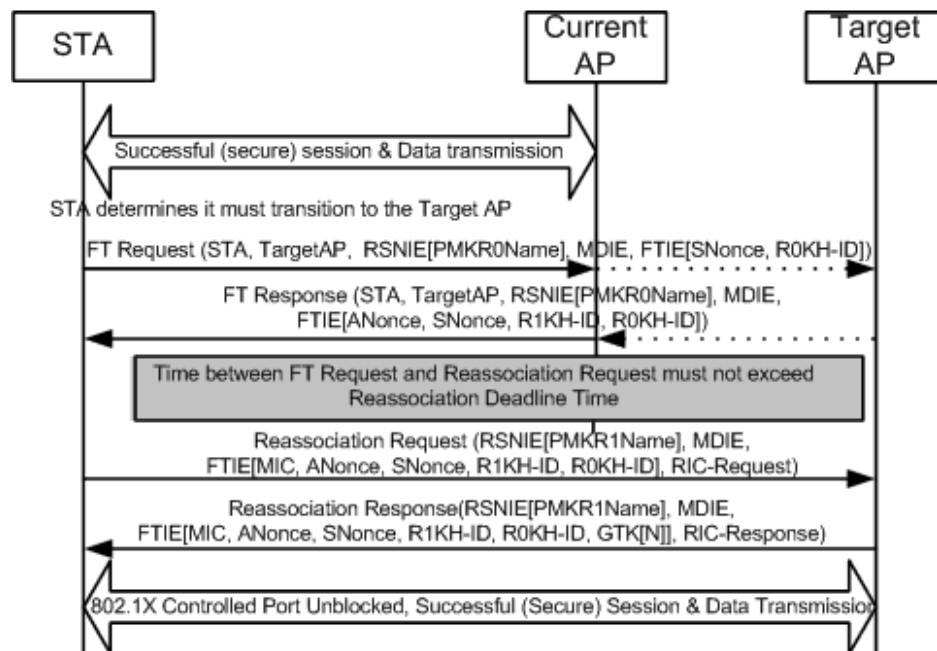


Figure 11A-5—Over-the-DS FT Protocol in an RSN

To perform an over-the-DS fast BSS transition to a target AP, the STA and the target AP (through the current AP) shall perform the following exchange:

STA→Target AP: FT Request (STA address, TargetAP address, RSNIE[PMKR0Name], MDIE, FTIE[SNonce, R0KH-ID])

Target AP→STA: FT Response (STA address, TargetAP address, Status, RSNIE[PMKR0Name], MDIE, FTIE[ANonce, SNonce, R1KH-ID, R0KH-ID])

The SME of the non-AP STA initiates the FT Request frame to the target AP by issuing a MLME-REMOTE_REQUEST.request primitive with parameters including the contents of the FT Request frame (FT Action frame with an Action field value indicating FT Request) to be sent. The MAC of the non-AP STA transmits this Action frame and issues a MLME-REMOTE_REQUEST.confirm primitive to signal that it has been sent. For processing at the current AP and target AP see 11A.10. When the MAC of the non-AP STA receives the FT Response frame (FT Action frame with an Action field value indicating FT Response), it passes it to the SME by use of MLME-REMOTE_REQUEST.indication primitive, with parameters including the contents of the received Action frame. The MLME interfaces on the non-AP STA, current AP, and the target AP for executing the over-the-DS fast BSS transition are shown in Figure 11A-6.

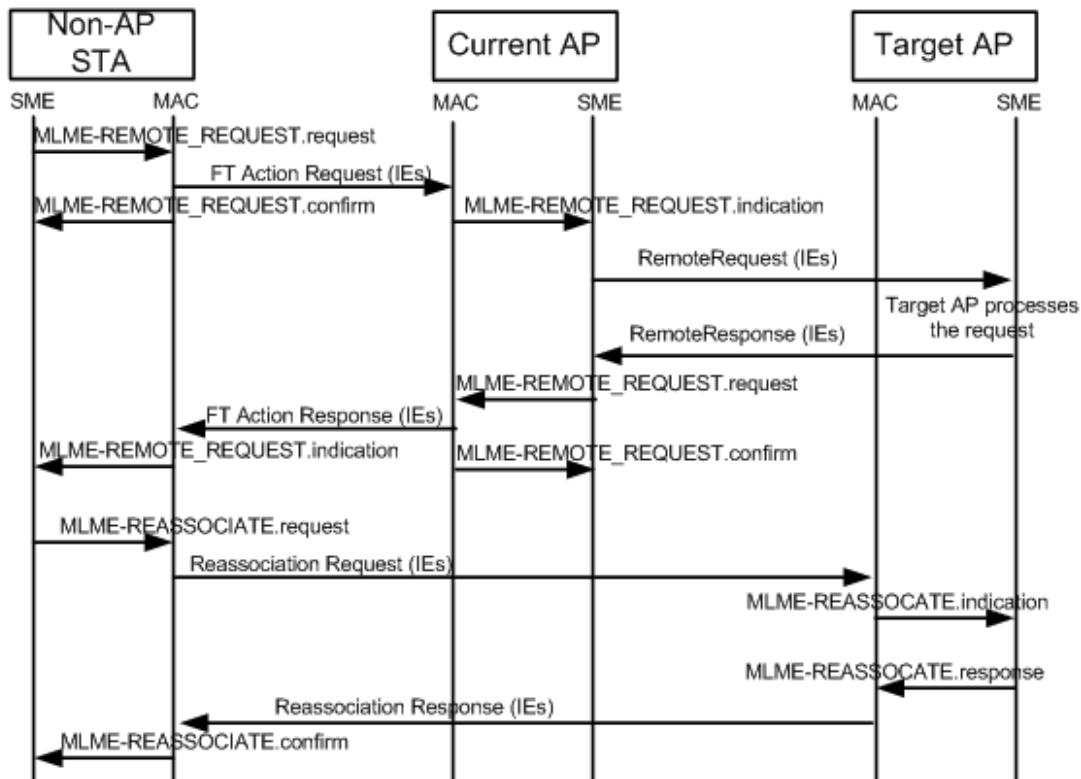


Figure 11A-6—MLME interfaces for over-the-DS FT Protocol messages

The STA Address field of the FT Request frame shall be set to the MAC address of the STA, and the Target AP Address field of the FT Request frame shall be set to the BSSID of the target AP. The information elements in the FT Request frame, and their required contents, shall be as given in 11A.8.2.

If the contents of the MDIE received by the target AP do not match the contents advertised in the Beacon and Probe Response frames, the target AP shall reject the FT Request frame with status code 54 (i.e., Invalid MDIE). If the contents of the RSNIE do not indicate a negotiated AKM of Fast BSS Transition (suite type

00-0F-AC:3 or 00-0F-AC:4), the AP shall reject the FT Request frame with status code 43 (i.e., Invalid AKMP). If the FTIE in the FT Request frame contains an invalid R0KH-ID, the AP shall reject the FT Request frame with status code 55 (i.e., Invalid FTIE). If the RSNIE in the FT Request frame contains an invalid PMKR0Name, and the AP has determined that it is an invalid PMKR0Name, the AP shall reject the Authentication Request with status code 53 (i.e., Invalid PMKID). If the requested R0KH is not reachable, the AP shall respond to the FT Request frame with status code 28 (i.e., R0KH unreachable). The AP may reject the FT Request frame for limiting the non-AP STA's reassociation to this AP by using the status code 37 ("This request has been declined"). If the non-AP STA selects a pairwise cipher suite in the RSNIE that is different from the ones used in the initial mobility domain association, then the AP shall reject the FT Request frame with status code 19 (i.e., Invalid Pairwise Cipher).

The STA Address field of the FT Response frame shall be set to the MAC address of the non-AP STA, and the Target AP Address field of the FT Response frame shall be set to the BSSID of the target AP. The information elements in the FT Response frame, and their required contents, shall be as given in 11A.8.3. The Status Code field shall be a value from the options listed in 7.3.1.9.

The R1KH of the target AP uses the value of PMKR0Name and other information from the frame to calculate PMKR1Name. If the target AP does not have the key identified by PMKR1Name, it may retrieve that key from the R0KH identified by the non-AP STA. See 11A.2. Upon receiving a new PMK-R1 for a non-AP STA, the target AP shall delete the prior PMK-R1 security association and PTKSAs derived from the prior PMK-R1.

The non-AP STA and the target AP compute the PTK and PTKName using the PMK-R1, PMKR1Name, ANonce, and SNonce, as specified in 8.5.1.5.5. The PTKSA shall be deleted by the target AP if it does not receive a Reassociation Request frame from the STA within the reassociation deadline timeout value.

If the non-AP STA does not receive a response to the FT Request frame, it may reissue the request following the restrictions given for Authentication frames in 11.3. If the Status Code field value returned by the target AP is 0, indicating success, the STA and target AP transition to State 2 (as defined in 11.3); the STA may continue with reassociation (11A.7.1). Handling of errors returned in the Status Code field shall be as specified for Authentication frames in 11.3.

11A.5.4 Over-the-air FT Protocol authentication in a non-RSN

The over-the-air FT Protocol in a non-RSN is shown in Figure 11A-7.

To perform an over-the-air fast BSS transition to a target AP in a non-RSN, the STA and target AP shall perform the following exchange:

STA→Target AP: Authentication-Request (FTAA, 0, MDIE)

Target AP→STA: Authentication-Response (FTAA, Status, MDIE)

In the Authentication Request frame, the SA field of the message header shall be set to the MAC address of the STA, and the DA field of the message header shall be set to the BSSID of the target AP. The information elements in the frame, and their required contents, shall be as given in 11A.8.2.

If the contents of the MDIE received by the target AP do not match the contents advertised in the Beacon and Probe Response frames, the target AP shall reject the Authentication Request with status code 54 (i.e., Invalid MDIE).

In the Authentication Response frame, the SA field of the message header shall be set to the BSSID of the target AP, and the DA field of the message header shall be set to the MAC address of the STA. The Status Code field shall be a value from the options listed in 7.3.1.9. The information elements in the frame, and their required contents, shall be as given in 11A.8.3.

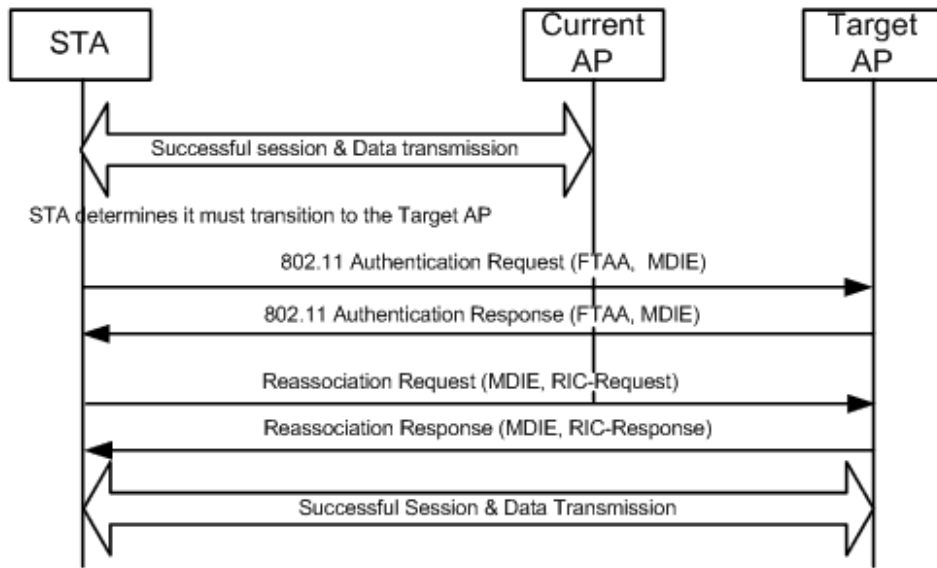


Figure 11A-7—Over-the-air FT Protocol in a non-RSN

If the STA does not receive a response to the Authentication Request frame, it may reissue the request following the restrictions given for Authentication frames in 11.3. If the Status Code field value returned by the target AP is 0, indicating success, the STA and target AP transition to State 2 (as defined in 11.3); the STA may continue with reassociation (11A.7.2). Handling of errors returned in the Status Code field shall be as specified in 11.3.

11A.5.5 Over-the-DS FT Protocol authentication in a non-RSN

The over-the-DS FT Protocol in a non-RSN is shown in Figure 11A-8.

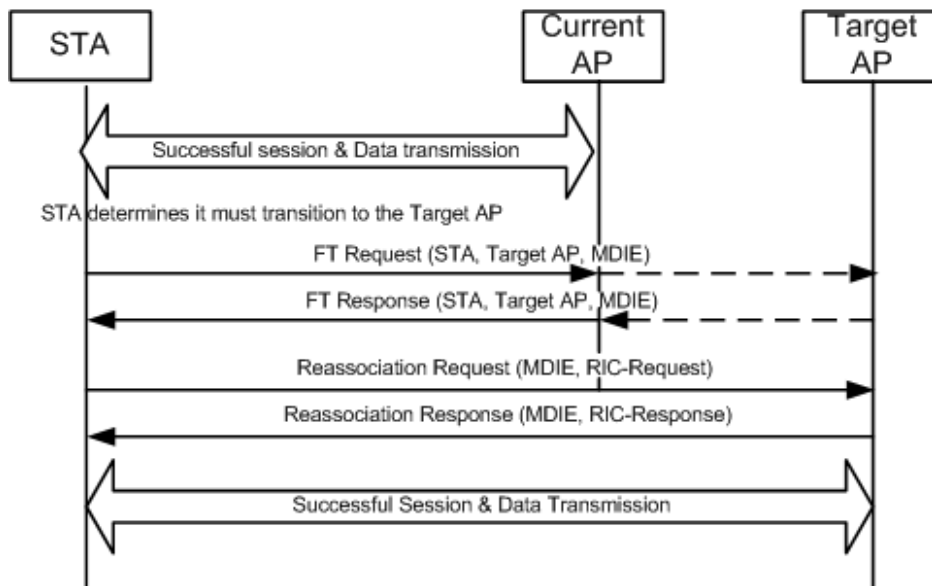


Figure 11A-8—Over-the-DS FT Protocol in a non-RSN

To perform an over-the-DS fast BSS transition to a target AP in a non-RSN, the STA and the target AP (through the current AP) shall perform the following exchange:

STA→Target AP: FT Request(STA, TargetAP, MDIE)

Target AP→STA: FT Response(STA, TargetAP, Status, MDIE)

The STA Address field of the FT Request frame shall be set to the MAC address of the STA, and the Target AP Address field of the FT Request frame shall be set to the BSSID of the target AP. The information elements in the FT Request frame, and their required contents, shall be as given in 11A.8.2.

If the contents of the MDIE received by the target AP do not match the contents advertised in the Beacon and Probe Response frames, the target AP shall reject the FT Request frame with status code 54 (i.e., Invalid MDIE).

The STA Address field of the FT Response frame shall be set to the MAC address of the STA, and the Target AP Address field of the FT Response frame shall be set to the BSSID of the target AP. The information elements in the FT Response frame, and their required contents, shall be as given in 11A.8.3. The Status Code field shall be a value from the options listed in 7.3.1.9.

If the STA does not receive a response to the FT Request frame, it may reissue the request following the restrictions given for Authentication frames in 11.3. If the Status Code field value returned by the target AP is 0, indicating success, the STA and target AP transition to State 2 (as defined in 11.3); the STA may continue with reassociation (11A.7.2). Handling of errors returned in the Status Code field shall be as specified for Authentication frames in 11.3.

11A.6 FT Resource Request Protocol

11A.6.1 Overview

The FT Resource Request Protocol involves an additional message exchange after the Authentication Request/Response frame, or FT Request/Response frame, and prior to reassociation.

APs capable of fast BSS transition may allow STAs to request resources prior to reassociation. Availability of the FT Resource Request Protocol is advertised by the target AP in the MDIE. If the Resource Request Protocol Capability subfield is set to 0, then the STA shall not send an Authentication Confirm nor FT Confirm frame to the AP. An AP that receives an Authentication Confirm or FT Confirm frame from a STA and does not support the FT Resource Request Protocol shall respond with status code 38 (i.e., the request has not been successful as one or more parameters have invalid values).

The additional message exchange for the FT Resource Request Protocol shall be performed using the same method (over-the-air or over-the-DS) as was used for the Authentication Request/Response frame or FT Request/Response frame. An AP that receives an FT Confirm frame that did not previously receive an FT Request frame from the same STA shall reject the request with status code 52 (i.e., Invalid FT Action Frame Count). An AP that receives an Authentication Confirm frame that did not previously receive an Authentication Request frame from the same STA shall reject the request with status code 14 (i.e., Received an Authentication frame with authentication transaction sequence number out of expected sequence).

11A.6.2 Over-the-air fast BSS transition with resource request

The over-the-air FT Resource Request Protocol in an RSN is shown in Figure 11A-9.

The over-the-air FT Resource Request Protocol in a non-RSN is shown in Figure 11A-10.

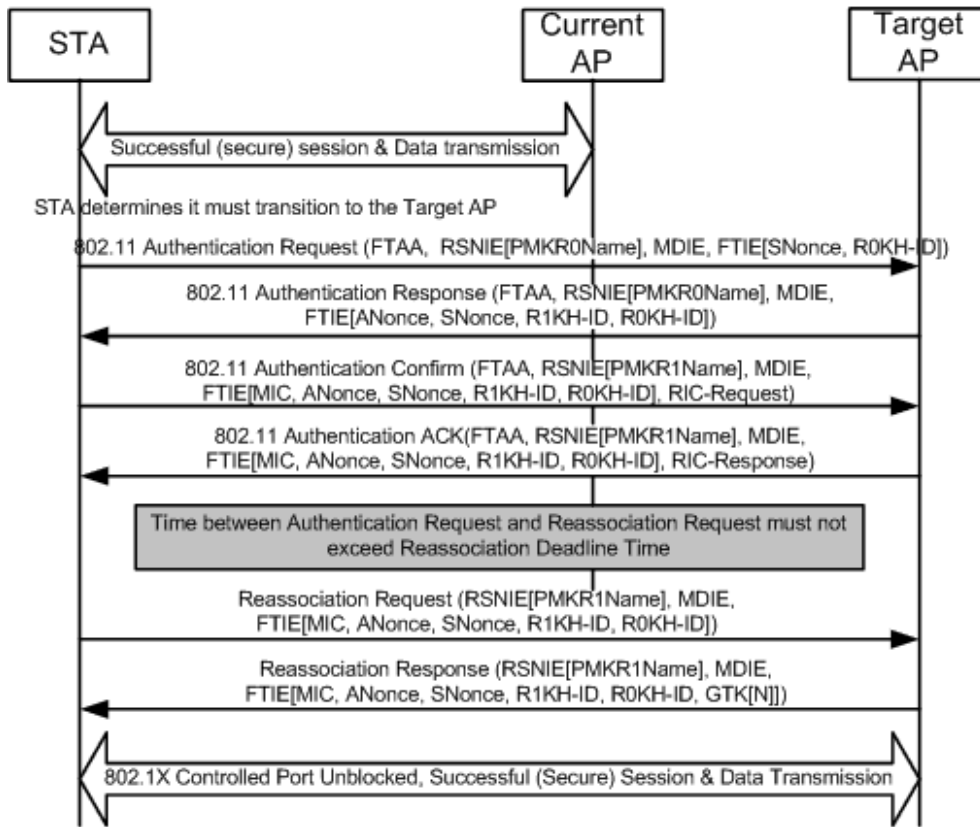


Figure 11A-9—Over-the-air FT Resource Request Protocol in an RSN

To perform an over-the-air FT Resource Request Protocol to a target AP, after completing the Authentication Request/Response exchange given in 11A.5.2 or 11A.5.4, the STA and target AP shall perform the following exchange:

STA→Target AP: Authentication-Confirm (FTAA, 0, RSNIE[PMKR1Name], MDIE, FTIE[MIC, ANonce, SNonce, R1KH-ID, R0KH-ID], RIC-Request)

Target AP→STA: Authentication-Ack (FTAA, Status, RSNIE[PMKR1Name], MDIE, FTIE[MIC, ANonce, SNonce, R1KH-ID, R0KH-ID], RIC-Response)

The SME of the STA initiates the resource request exchange through the use of the primitive MLME-RESOURCE_REQUEST.request primitive, and the SME of the AP responds with MLME-RESOURCE_REQUEST.response primitive.

In the Authentication Confirm frame, the SA field of the message header shall be set to the MAC address of the STA, and the DA field of the message header shall be set to the BSSID of the target AP. In a non-RSN, the FTIE and RSNIE shall not be present. The information elements in the frame, the information element contents, and MIC calculation shall be as given in 11A.8.4.

If the contents of the MDIE received by the target AP do not match the contents advertised in the Beacon and Probe Response frames, the target AP shall reject the Authentication Confirm frame with status code 54 (i.e., Invalid MDIE).

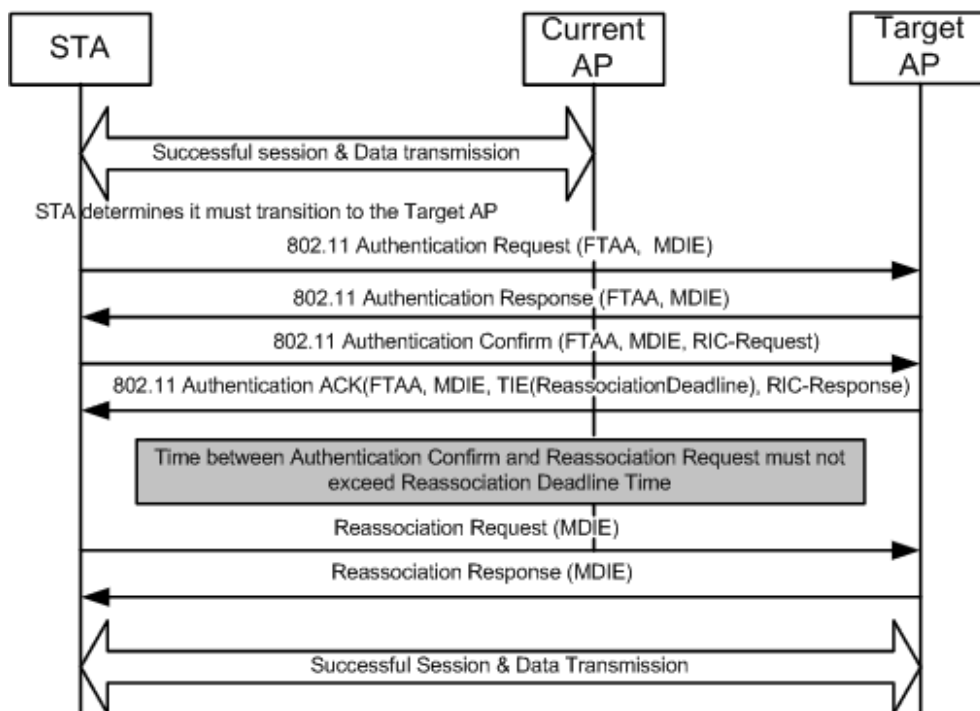


Figure 11A-10—Over-the-air FT Resource Request Protocol in a non-RSN

In an RSN, the R1KH of the target AP verifies the MIC in the FTIE in the Authentication Confirm frame and shall discard the request if it is incorrect. If the FTIE in the Authentication Confirm frame contains a different ROKH-ID, R1KH-ID, ANonce, or SNonce, the AP shall reject the Authentication Confirm frame with status code 55 (i.e., Invalid FTIE). If the RSNIE in the Authentication Confirm frame contains an invalid PMKR1Name, the AP shall reject the Authentication Confirm frame with status code 53 (i.e., Invalid PMKID).

In the Authentication Ack frame, the SA field of the message header shall be set to the BSSID of the target AP, and the DA field of the message header shall be set to the MAC address of the STA. In a non-RSN, the FTIE and RSNIE shall not be present. The Status Code field shall be a value from the options listed in 7.3.1.9. The information elements in the frame, the information element contents, and MIC calculation shall be as given in 11A.8.5.

In an RSN, the S1KH of the STA verifies the MIC in the FTIE in the Authentication Ack frame and shall discard the response if the MIC is incorrect.

The STA may make a request for resources by including a RIC-Request (see 11A.11) in the Authentication Confirm frame. The RIC-Request is generated by the procedures of 11A.11.3.1, and the RIC-Response is generated by the procedures of 11A.11.3.2.

If the value of the Status Code field returned by the target AP in the Authentication Ack frame is nonzero, then the STA shall abandon this transition attempt.

In an RSN, on successful completion of the FT authentication exchange of the FT Resource Request Protocol, the PTKSA has been established and proven live. The key replay counter shall be initialized to zero, and the subsequent EAPOL-Key frames (e.g., GTK updates) shall use the key replay counter to ensure

they are not replayed. The PTKSA shall be deleted by the target AP if it does not receive a Reassociation Request frame from the STA within the reassociation deadline timeout value.

In a non-RSN, the Authentication Ack frame contains a TIE with a reassociation deadline. If the STA does not send a Reassociation Request frame to the target AP within that interval, the STA shall abandon this transition attempt.

The exchange between the STA and the target AP may continue with reassociation (11A.7.1 or 11A.7.2).

11A.6.3 Over-the-DS fast BSS transition with resource request

The over-the-DS FT Resource Request Protocol in an RSN is shown in Figure 11A-11.

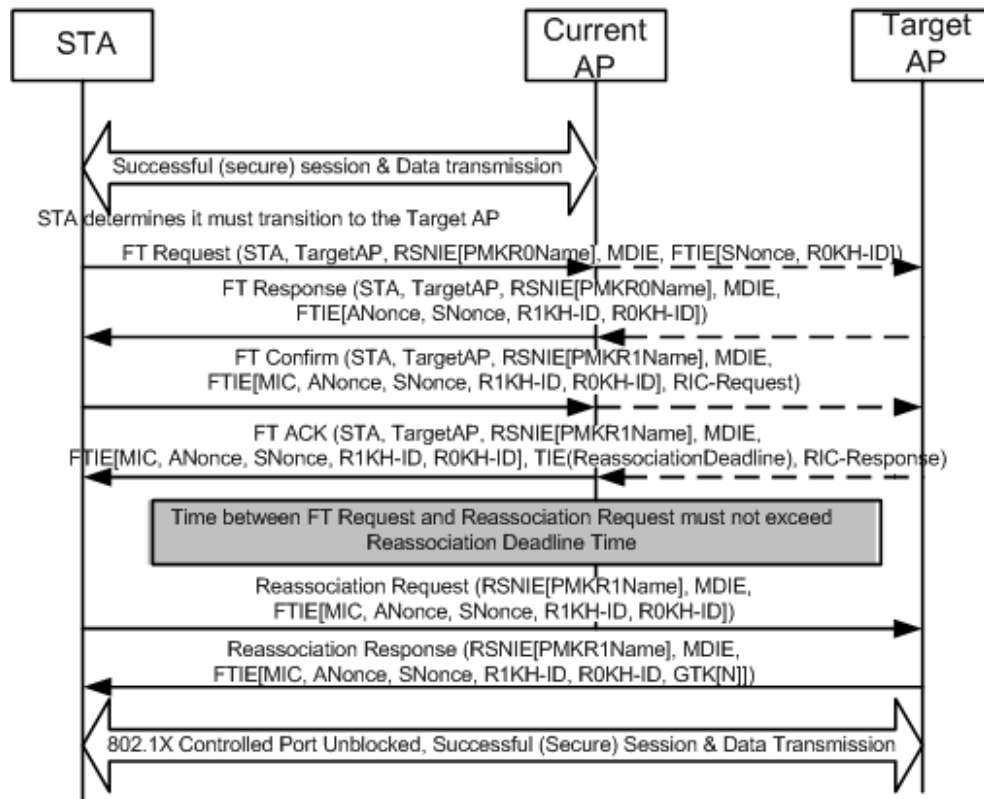


Figure 11A-11—Over-the-DS FT Resource Request Protocol in an RSN

The over-the-DS FT Resource Request Protocol in a non-RSN is shown in Figure 11A-12.

To perform an Over-the-DS FT Resource Request Protocol to a target AP, after completing the FT Request/Response frame exchange given in 11A.5.3 or 11A.5.5, the STA and target AP (through the current AP) shall perform the following exchange, using the mechanism described in 11A.10:

- STA→Target AP: FT Confirm (STA, TargetAP, RSNIE[PMKR1Name], MDIE, FTIE[MIC, ANonce, SNonce, R1KH-ID, R0KH-ID], RIC-Request)
- Target AP→STA: FT Ack (STA, TargetAP, Status, RSNIE[PMKR1Name], MDIE, FTIE[MIC, ANonce, SNonce, R1KH-ID, R0KH-ID], TIE[ReassociationDeadline], RIC-Response)

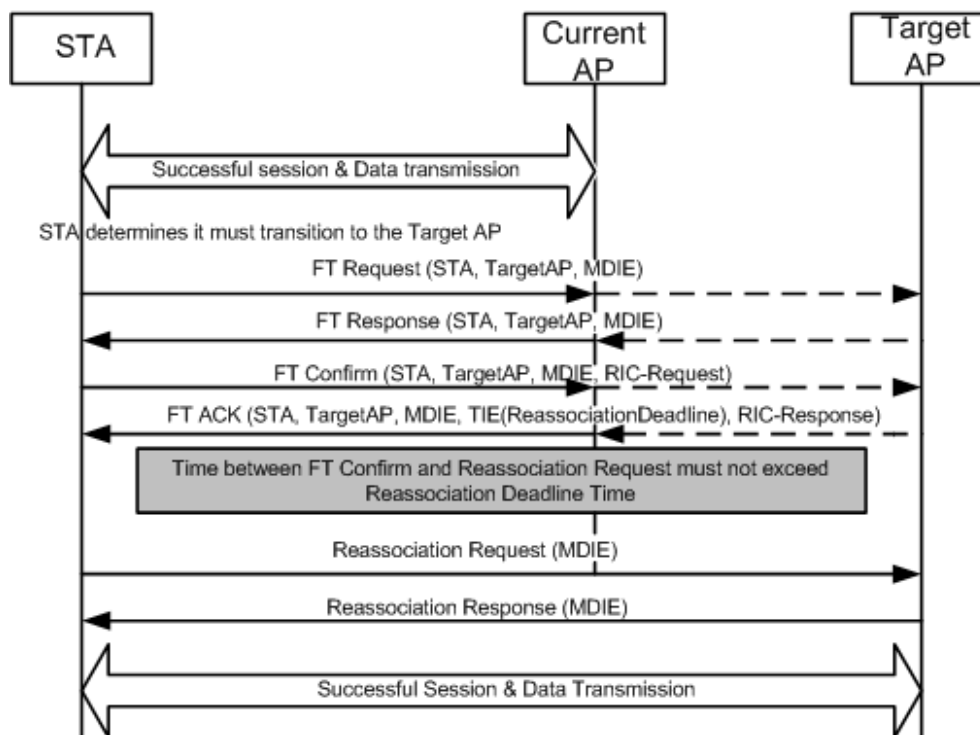


Figure 11A-12—Over-the-DS FT Resource Request Protocol in a non-RSN

The SME of the STA initiates the FT Confirm frame to the target AP by issuing a MLME-REMOTE_REQUEST.request primitive with parameters including the contents of the FT Confirm frame (FT Action frame with an Action field value indicating FT Confirm) to be sent. The MAC of the STA transmits this Action frame and issues a MLME-REMOTE_REQUEST.confirm primitive to signal that it has been sent. For processing at the current AP and target AP, see 11A.10. When the MAC of the STA receives the FT Ack frame (FT Action frame with an Action field value indicating FT Ack), it passes it to the SME by use of an MLME-REMOTE_REQUEST.indication primitive, with parameters including the contents of the received Action frame.

The STA Address field of the FT Confirm frame shall be set to the MAC address of the STA, and the Target AP Address field of the FT Confirm frame shall be set to the BSSID of the target AP. The information elements in the FT Confirm frame, the information element contents, and the MIC calculation shall be as given in 11A.8.4. In a non-RSN, the FTIE and RSNIE shall not be present.

If the contents of the MDIE received by the target AP do not match the contents advertised in the Beacon and Probe Response frames, the target AP shall reject the FT Confirm frame with status code 54 (i.e., Invalid MDIE).

In an RSN, the R1KH of the target AP verifies the MIC in the FTIE and shall discard the request if it is incorrect. If the FTIE in the FT Confirm frame contains a different R0KH-ID, R1KH-ID, ANonce, or SNonce from the values sent in the FT Response frame, the AP shall reject the FT Confirm frame with status code 55 (i.e., Invalid FTIE). If the RSNIE in the FT Confirm frame contains an invalid PMKR1Name, the AP shall reject the FT Confirm frame with status code 53 (i.e., Invalid PMKID).

The STA Address field of the FT Ack frame shall be set to the MAC address of the STA, and the Target AP Address field of the FT Ack frame shall be set to the BSSID of the target AP. The information elements in

the FT Ack frame, the information element contents, and the MIC calculation shall be as given in 11A.8.5. In a non-RSN, the FTIE and RSNIE shall not be present. The Status Code field value shall be a value from the options listed in 7.3.1.9, and a TIE may appear.

In an RSN, the S1KH of the STA verifies the MIC in the FTIE in the FT Ack frame and shall discard the response if the MIC is incorrect.

The STA may make a request for resources by including a RIC-Request (see 11A.11) in the FT Confirm frame. The RIC-Request is generated by the procedures of 11A.11.3.1, and the RIC-Response is generated by the procedures of 11A.11.3.2.

In order to recover from over-the-DS packet losses, the STA may retransmit the FT Confirm frame until the reassociation deadline time is reached. If the STA does not receive a response to the FT Confirm frame or if the value of the Status Code field returned by the target AP in the FT Ack frame is nonzero, then the STA shall abandon this transition attempt.

In an RSN, on successful completion of the FT Confirm/Acknowledgment frame exchange, the PTKSA has been established and proven live. The key replay counter shall be initialized to zero, and the subsequent EAPOL-Key frames (e.g., GTK updates) shall use the key replay counter to ensure they are not replayed. The PTKSA shall be deleted by the target AP if it does not receive a Reassociation Request frame from the STA within the reassociation deadline timeout value. Resource request procedures are specified in 11A.11.

In a non-RSN, the FT Ack frame contains a TIE with a reassociation deadline. If the STA does not send a Reassociation Request frame to the target AP within that interval, the STA shall abandon this transition attempt.

The exchange between the STA and the target AP may continue with reassociation (11A.7.1 or 11A.7.2).

11A.7 FT reassociation

11A.7.1 FT reassociation in an RSN

If the non-AP STA does not send a Reassociation Request frame to the target AP within the reassociation deadline interval received during the FT initial mobility domain association, the target AP may delete the PTKSA, and the non-AP STA shall abandon this transition attempt.

The non-AP STA shall perform a reassociation directly with the target AP via the following exchange:

STA→Target AP: Reassociation Request(RSNIE[PMKR1Name], MDIE, FTIE[MIC, ANonce, SNonce, R1KH-ID, R0KH-ID], RIC-Request)

Target AP→STA: Reassociation Response(RSNIE[PMKR1Name], MDIE, FTIE[MIC, ANonce, SNonce, R1KH-ID, R0KH-ID, GTK[N]], RIC-Response)

The SME of the STA initiates the reassociation through the use of the MLME-REASSOCIATE.request primitive. The SME of the AP responds to the indication with MLME-REASSOCIATE.response primitive. See 11.3.2.

In the Reassociation Request frame, the SA field of the message header shall be set to the MAC address of the STA, and the DA field of the message header shall be set to the BSSID of the target AP. The information elements in the frame, the information element contents, and the MIC calculation shall be as given in 11A.8.4.

The R1KH of the target AP verifies the MIC in the FTIE in the Reassociation Request frame and shall discard the request if the MIC is incorrect. If the contents of the MDIE received by the target AP do not

match the contents advertised in the Beacon and Probe Response frames, the target AP shall reject the Reassociation Request frame with status code 54 (i.e., Invalid MDIE). If the FTIE in the Reassociation Request frame contains a different R0KH-ID, R1KH-ID, ANonce, or SNonce, the AP shall reject the Reassociation Request frame with status code 55 (i.e., Invalid FTIE). If the RSNIE in the Reassociation Request frame contains an invalid PMKR1Name, the AP shall reject the Reassociation Request frame with status code 53 (i.e., Invalid PMKID).

In the Reassociation Response frame, the SA field of the message header shall be set to the BSSID of the target AP, and the DA field of the message header shall be set to the MAC address of the non-AP STA. The Status Code field shall be a value from the options listed in 7.3.1.9. The information elements in the frame, the information element contents, and the MIC calculation shall be as given in 11A.8.5.

The S1KH of the non-AP STA verifies the MIC in the FTIE in the Reassociation Response frame and shall discard the response if the MIC is incorrect.

If the non-AP STA is performing a reassociation exchange as part of the FT Resource Request Protocol, then the non-AP STA shall not include the RIC-Request in the Reassociation Request frame, and the AP shall not include the RIC-Response in the Reassociation Response frame. If the reassociation exchange is part of the FT Resource Request Protocol and the AP is unable to honor the resources that have been placed in the accepted state for that non-AP STA, then the AP shall reject the Reassociation Request frame and may use status code 33 (i.e., Association denied because QoS AP has insufficient bandwidth to handle another QoS STA).

If the non-AP STA did not utilize the FT Resource Request Protocol, the STA may make a request for resources by including a RIC-Request (see 11A.11) in the Reassociation Request frame. The RIC-Request is generated by the procedures of 11A.11.3.1, and the RIC-Response is generated by the procedures of 11A.11.3.2.

If the Status Code field value returned by the target AP in the response is 1 (i.e., Unspecified failure), 14 (i.e., Authentication transaction sequence number out of sequence), or 16 (i.e., Authentication rejected due to timeout waiting for next frame in sequence), then the non-AP STA shall abandon this transition attempt. Handling of other errors returned in the Status Code field shall be as specified in 11.3.

Upon a successful reassociation, the PTKSA has been established and proven live. The SME of the AP shall open the IEEE 802.1X Controlled Port. The non-AP STA shall transition to State 3 (as defined in 11.3). If the target AP is distinct from the previous AP, the non-AP STA shall enter State 1 with respect to the previous AP.

Upon a successful reassociation, the non-AP STA shall delete any corresponding PTKSA with its previous AP. The SME of the STA shall issue an MLME-DELETEKEYS.request primitive to delete the pairwise keys with the previous AP, and the STA and the AP shall issue a MLME-SETKEYS.request primitive and MLME-SETPROTECTION.request primitive to install the pairwise keys. The PTK key lifetime timer shall be initialized with the value calculated as the difference between the TIE[KeyLifetime] sent in Message 3 of the FT initial mobility domain association and the time since the completion of the FT 4-Way Handshake during the FT initial mobility domain association.

When the IEEE 802.1X Controlled Port is opened, the EAPOL-Key frame replay counter shall be initialized to zero. The R1KH shall increment the key replay counter on each successive EAPOL-Key frame that it transmits.

11A.7.2 FT reassociation in a non-RSN

The STA shall perform a reassociation with the target AP via the following exchange:

STA→Target AP: Reassociation Request(MDIE, RIC-Request)

Target AP→STA: Reassociation Response(MDIE, RIC-Response)

The non-AP SME of the STA initiates the reassociation through the use of the MLME-REASSOCIATE.request primitive. The SME of the AP responds to the indication with MLME-REASSOCIATE.response primitive. See 11.3.2.

In the Reassociation Request frame, the SA field of the message header shall be set to the MAC address of the non-AP STA, and the DA field of the message header shall be set to the BSSID of the target AP. The information elements in Reassociation Request frame, and their required contents, shall be as given in 11A.8.4.

If the contents of the MDIE received by the target AP do not match the contents advertised in the Beacon and Probe Response frames, the target AP shall reject the Reassociation Request frame with status code 54 (i.e., Invalid MDIE).

In the Reassociation Response frame, the SA field of the message header shall be set to the BSSID of the target AP, and the DA field of the message header shall be set to the MAC address of the non-AP STA. The information elements in Reassociation Response frame, and their required contents, shall be as given in 11A.8.5. The Status Code field shall be a value from the options listed in 7.3.1.9.

If the STA is performing a reassociation exchange as part of the FT Resource Request Protocol, then the STA shall not include the RIC-Request in the Reassociation Request frame, and the AP shall not include the RIC-Response in the Reassociation Response frame.

If the non-AP STA did not utilize the FT Resource Request Protocol, the STA may make a request for resources by including a RIC-Request (see 11A.11) in the Reassociation Request frame. The RIC-Request is generated by the procedures of 11A.11.3.1, and the RIC-Response is generated by the procedures of 11A.11.3.2.

If the Status Code field value returned by the target AP in the response is 1 (i.e., Unspecified failure), 14 (i.e., Authentication transaction sequence number out of sequence), or 16 (i.e., Authentication rejected due to timeout waiting for next frame in sequence), then the non-AP STA shall abandon this transition attempt. Handling of other errors returned in the Status Code field shall be as specified in 11.3.

If the AP has dot11RSNAEnabled set to TRUE, upon a successful reassociation, the SME shall open the IEEE 802.1X Controlled Port.

Upon a successful reassociation, the target AP and the non-AP STA shall transition to State 3 (as defined in 11.3). If the target AP is distinct from the previous AP, then the non-AP STA shall enter State 1 with respect to the previous AP.

11A.8 FT authentication sequence

11A.8.1 Overview

The FT authentication sequence comprises four sets of FT information elements. Each set of FT information elements is referred to in 11A.8 as a *message*. These messages are included in the FT Protocol frames or FT Resource Request Protocol frames to initiate a fast BSS transition. The FT authentication sequence is always initiated by the non-AP STA and responded to by the target AP.

In an RSN, the first two messages in the sequence allow the non-AP STA and target AP to provide association instance identifiers, SNonce and ANonce, respectively. SNonce and ANonce are chosen

randomly or pseudo-randomly and are used to generate a fresh PTK. The first two messages also enable the target AP to provision the PMK-R1 and the non-AP STA and target AP to compute the PTK. The third and fourth messages demonstrate liveness of the peer, authenticate the information elements, and enable an authenticated resource request.

When a non-AP STA invokes the FT Protocol, then the first two messages of the sequence are both carried in Authentication frames or both carried in Action frames, and these messages are described in 11A.8.2 and 11A.8.3. The third and fourth messages in the sequence are carried in the Reassociation Request and Reassociation Response frames and are described in 11A.8.4 and 11A.8.5.

When the non-AP STA invokes the FT Resource Request Protocol, then the first four messages of the sequence are all carried in Authentication frames or all carried in Action frames, and these messages are described in 11A.8.2 through 11A.8.5. The fifth and sixth frames of the FT Resource Request Protocol are carried in the Reassociation Request frame and Reassociation Response frame and are described in 11A.8.4 and 11A.8.5.

Regardless of the transport mechanism, the information contained in the FT authentication sequence consists of the set of information elements shown in Table 11A-1:

Table 11A-1—FT authentication information elements

| Information | Presence in Authentication Sequence messages | Description |
|-------------------------------------------|-----------------------------------------------------------------------------------------------------|-------------|
| RSN | Present in all messages of the sequence if dot11RSNAEnabled is set to TRUE. | 7.3.2.25 |
| Mobility domain | Present in all messages of the sequence. | 7.3.2.47 |
| Fast BSS transition | Present in all messages of the sequence if dot11RSNAEnabled is set to TRUE. | 7.3.2.48 |
| Timeout interval (reassociation deadline) | May optionally appear in the fourth message of the sequence if dot11RSNAEnabled is not set to TRUE. | 7.3.2.49 |
| RIC | May appear in the third and fourth messages. | 7.3.2.50 |

The first message is used by the non-AP STA to initiate a fast BSS transition. When RSNA is enabled, the STA shall include the ROKH-ID and the SNonce in the FTIE and the PMKR0Name in the RSNIE. The target AP can use the PMKR0Name to derive the PMKR1Name, and if the target AP does not have the PMK-R1 identified by PMKR1Name, it may attempt to retrieve that key from the ROKH identified by ROKH-ID. See 11A.2. The non-AP STA includes a fresh SNonce as its contribution to the association instance identifier and to provide key separation of the derived PTK; it is selected randomly to serve as a challenge that will demonstrate the liveness of the peer in the fourth message.

The second message is used by the target AP to respond to the requesting non-AP STA. The target AP provides the key holder identifiers and key names used to generate the PTK. The target AP also includes a fresh ANonce as its contribution to the association instance identifier and to provide key separation of the derived PTK. The response includes a status code.

In an RSN, the third message is used by the non-AP STA to assert to the target AP that it has a valid PTK. If no resources are required, then the STA omits inclusion of the RIC.

The fourth message is used by the target AP to respond to the requesting non-AP STA. This message serves as final confirmation of the transition, establishes that the AP possesses the PMK-R1 and is participating in this association instance, and protects against downgrade attacks. Note, however, that the RIC will be absent if no resources were requested in the third message. This also includes a status code and may include a reassociation deadline.

11A.8.2 FT authentication sequence: contents of first message

The RSNIE shall be present only if dot11RSNAEnabled is set to TRUE. If present, the RSNIE shall be set as follows:

- Version field shall be set to 1.
- PMKID Count field shall be set to 1.
- PMKID List field shall contain the PMKR0Name.
- All other fields shall be as specified in 7.3.2.25 and 8.4.3.

The MDIE shall contain the MDID field and the FT Capability and Policy field settings obtained from the target AP, as advertised by the target AP in Beacon and Probe Response frames. The MDID shall be identical to that obtained during the FT initial mobility domain association exchange.

The FTIE shall be present only if dot11RSNAEnabled is set to TRUE. If present, the FTIE shall be set as follows:

- R0KH-ID shall be the value of R0KH-ID obtained by the non-AP STA during its FT initial mobility domain association exchange.
- SNonce shall be set to a value chosen randomly by the non-AP STA, following the recommendations of 8.5.7.
- All other fields shall be set to 0.

11A.8.3 FT authentication sequence: contents of second message

If the status code is zero, then the following rules apply.

The RSNIE shall be present only if dot11RSNAEnabled is set to TRUE. If present, the RSNIE shall be set as follows:

- Version field shall be set to 1.
- PMKID Count field shall be set to 1.
- PMKID List field shall be set to the value contained in the first message of this sequence.
- All other fields shall be identical to the contents of the RSNIE advertised by the AP in Beacon and Probe Response frames.

The MDIE shall contain the MDID and FT Capability and Policy fields. This information element shall be the same as the MDIE advertised by the target AP in Beacon and Probe Response frames.

The FTIE shall be present only if dot11RSNAEnabled is set to TRUE. If present, the FTIE shall be set as follows:

- R0KH-ID shall be identical to the R0KH-ID provided by the non-AP STA in the first message.
- R1KH-ID shall be set to the R1KH-ID of the target AP, from the MIB variable dot11FTR1KeyHolderID.

- ANonce shall be set to a value chosen randomly by the target AP, following the recommendations of 8.5.7.
- SNonce shall be set to the value contained in the first message of this sequence.
- All other fields shall be set to 0.

11A.8.4 FT authentication sequence: contents of third message

The RSNIE shall be present only if dot11RSNAEnabled is set to TRUE. If present, the RSNIE shall be set as follows:

- Version field shall be set to 1.
- PMKID Count field shall be set to 1.
- PMKID field shall contain the PMKR1Name.
- All other fields shall be as specified in 7.3.2.25 and 8.4.3.

The MDIE shall contain the MDID and FT Capability and Policy fields. This information element shall be identical to the MDIE contained in the first message of this sequence.

The FTIE shall be present only if dot11RSNAEnabled is set to TRUE. If present, the FTIE shall be set as follows:

- ANonce, SNonce, R0KH-ID, and R1KH-ID shall be set to the values contained in the second message of this sequence.
- The Information Element Count field of the MIC Control field shall be set to the number of information elements protected in this frame (variable).
- When the negotiated AKM is 00-0F-AC:3 or 00-0F-AC:4, the MIC shall be calculated using the KCK and the AES-128-CMAC algorithm. The output of the AES-128-CMAC shall be 128 bits.
- The MIC shall be calculated on the concatenation of the following data, in the order given here:
 - non-AP STA MAC address (6 octets)
 - Target AP MAC address (6 octets)
 - Transaction sequence number (1 octet), which shall be set to the value 5 if this is a Reassociation Request frame and, otherwise, set to the value 3.
 - Contents of the RSNIE.
 - Contents of the MDIE.
 - Contents of the FTIE, with the MIC field of the FTIE set to 0.
 - Contents of the RIC-Request (if present)
- All other fields shall be set to 0.

If resources are being requested by the STA, then a sequence of information elements forming the RIC-Request shall be included.

11A.8.5 FT authentication sequence: contents of fourth message

If the status code is zero, then the following rules apply.

The RSNIE shall be present only if dot11RSNAEnabled is set to TRUE. If present, the RSNIE shall be set as follows:

- Version field shall be set to 1.

- PMKID Count field shall be set to 1.
- PMKID field shall contain the PMKR1Name
- All other fields shall be identical to the contents of the RSNIE advertised by the target AP in Beacon and Probe Response frames.

The MDIE shall contain the MDID and FT Capability and Policy fields. This information element shall be identical to the MDIE contained in the second message of this sequence.

The FTIE shall be present only if dot11RSNAEnabled is set to TRUE. If present, the FTIE shall be set as follows:

- ANonce, SNonce, R0KH-ID, and R1KH-ID shall be set to the values contained in the second message of this sequence.
- The Information Element Count field of the MIC Control field shall be set to the number of information elements protected in this frame (variable).
- When this message of the authentication sequence appears in a Reassociation Response frame, the Optional Parameter(s) field in the FTIE may include a GTK subelement. If a GTK is included, the Key field of the subelement shall be encrypted using KEK and the NIST AES key wrap algorithm. The Key field shall be padded before encrypting if the key length is less than 16 octets or if it is not a multiple of 8. The padding consists of appending a single octet 0xdd followed by zero or more 0x00 octets. When processing a received message, the receiver shall ignore this trailing padding. Addition of padding does not change the value of the Key Length field. Note: The length of the encrypted Key field can be determined from the length of the GTK subelement.
- When the negotiated AKM is 00-0F-AC:3 or 00-0F-AC:4, the MIC shall be calculated using the KCK and the AES-128-CMAC algorithm. The output of the AES-128-CMAC algorithm shall be 128 bits.
- The MIC shall be calculated on the concatenation of the following data, in the order given here:
 - Non-AP STA MAC address (6 octets)
 - Target AP MAC address (6 octets)
 - Transaction sequence number (1 octet), which shall be set to the value 6 if this is a Reassociation Response frame or, otherwise, set to the value 4.
 - Contents of the RSNIE.
 - Contents of the MDIE.
 - Contents of the FTIE, with the MIC field of the FTIE set to 0.
 - Contents of the RIC-Response (if present)
- All other fields shall be set to 0.

If this message is other than a Reassociation Response frame and dot11RSNAEnabled is set to FALSE, a TIE may appear. If this message is other than a Reassociation Response frame, includes a RIC-Response, and dot11RSNAEnabled is set to FALSE, then a timeout interval shall appear. If it appears, it shall be set as follows:

- Timeout Interval Type field shall be set to 1 (reassociation deadline)
- Timeout Interval Value field shall be set to the reassociation deadline time.

If resources were requested by the non-AP STA, then a RIC-Response shall be included.