INTERNATIONAL STANDARD

ISO/IEC 8802-11

Second edition
2005-08-01

AMENDMENT 6
2006-12-15

**IEEE STD 802.11i-2004
(Amendment to
IEEE Std 802.11-1999)**

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 6: Medium Access Control (MAC) Security Enhancements

Technologies de l'information — Télécommunications et échange d'information entre systèmes — Réseaux locaux et métropolitains — Exigences spécifiques

Partie 11: Spécifications pour le contrôle d'accès au support et la couche physique

AMENDEMENT 6: Perfectionnements de la sécurité de moyens de contrôle d'accès (MAC)

Reference number
ISO/IEC 8802-11:2005/Amd.6:2006(E)
IEEE Std 802.11i-2004
(Amendment to IEEE Std 802.11-1999)

Documents
Document Sharing Hub

Full document details: ISO_IEC 8802-11_2005_AMD6_2006

PDF disclaimer

This PDF file may contain embedded typefaces. In accordance with Adobe's licensing policy, this file may be printed or viewed but shall not be edited unless the typefaces which are embedded are licensed to and installed on the computer performing the editing. In downloading this file, parties accept therein the responsibility of not infringing Adobe's licensing policy. The ISO Central Secretariat accepts no liability in this area.

Adobe is a trademark of Adobe Systems Incorporated.

Details of the software products used to create this PDF file can be found in the General Info relative to the file; the PDF-creation parameters were optimized for printing. Every care has been taken to ensure that the file is suitable for use by ISO member bodies. In the unlikely event that a problem relating to it is found, please inform the Central Secretariat at the address given below.

ISO
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org

Documents
Document Sharing Hub
Full document details: ISO_IEC 8802-11_2005_AMD6_2006

IEEE Std 802.11i™-2004
[Amendment to IEEE Std 802.11™, 1999 Edition (Reaff 2003)
as amended by
IEEE Stds 802.11a™-1999, 802.11b™-1999,
802.11b™-1999/Cor 1-2001, 802.11d™-2001,
802.11g™-2003, and 802.11h™-2003]

IEEE Standards

802.11i™

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 6: Medium Access Control (MAC) Security Enhancements

IEEE Computer Society

Sponsored by the
LAN/MAN Standards Committee

This amendment is an approved IEEE Standard. It will be incorporated into the base standard in a future edition.

IEEE

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

23 July 2004

Print: SH95248
PDF: SS95248

AVA Documents
Document Sharing Hub

Full document details: ISO_IEC 8802-11_2005_AMD6_2006

IEEE Std 802.11i™-2004
[Amendment to IEEE Std 802.11™, 1999 Edition (Reaff 2003)
as amended by IEEE Stds 802.11a™-1999, 802.11b™-1999,
802.11b™-1999/Cor 1-2001, 802.11d™-2001,
802.11g™-2003, and 802.11h™-2003]

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 6: Medium Access Control (MAC) Security Enhancements

Sponsor
LAN/MAN Committee
of the
IEEE Computer Society

Approved 24 June 2004

IEEE-SA Standards Board

Documents
Document Sharing Hub

Full document details: ISO_IEC 8802-11_2005_AMD6_2006

Abstract: Security mechanisms for IEEE 802.11 are defined in this amendment, which includes a definition of WEP for backward compatibility with the original standard, IEEE Std 802.11, 1999 Edition. This amendment defines TKIP and CCMP, which provide more robust data protection mechanisms than WEP affords. It introduces the concept of a security association into IEEE 802.11 and defines security association management protocols called the 4-Way Handshake and the Group Key Handshake. Also, it specifies how IEEE 802.1X may be utilized by IEEE 802.11 LANs to effect authentication.
Keywords: AES, authentication, CCM, CCMP, confidentiality, countermeasures, data authenticity, EAPOL-Key, 4-Way Handshake, Group Key Handshake, IEEE 802.1X, key management, key mixing, Michael, RC4, replay protection, robust security network, RSN, security, security association, TKIP, WEP

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

Copyright © 2004 by the Institute of Electrical and Electronics Engineers, Inc.
All rights reserved. Published 23 July 2004. Printed in the United States of America.

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

Print: ISBN 0-7381-4073-2 SH95248
PDF: ISBN 0-7381-4074-0 SS95248

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.

Documents
Document Sharing Hub

Full document details: ISO_IEC 8802-11_2005_AMD6_2006

International Standard ISO/IEC 8802-11:2005/Amd.6:2006(E)

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

Amendment 6 to ISO/IEC 8802-11:2005 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 6, *Telecommunications and information exchange between systems*.

International Organization for Standardization / International Electrotechnical Commission
Case postale 56 • CH-1211 Genève 20 • Switzerland

Documents
Document Sharing Hub

Full document details: ISO_IEC 8802-11_2005_AMD6_2006

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 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. 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 addressed to:

Secretary, IEEE-SA Standards Board

445 Hoes Lane

P.O. Box 1331

Piscataway, NJ 08855-1331USA

NOTE—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 for which a license may be required by an IEEE standard or for conducting inquiries into the legal validity or scope of those patents that are brought to its attention.

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.

Documents
Document Sharing Hub

Full document details: ISO_IEC 8802-11_2005_AMD6_2006

Introduction

[This introduction is not part of IEEE Std 802.11i™-2004, 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 6: Medium Access Control (MAC) Security Enhancements.)]

Enhanced security services and mechanisms for the IEEE 802.11 medium access control (MAC) beyond those features and capabilities provided by the wired equivalent privacy (WEP) mechanism of the base standard, IEEE Std 802.11, 1999 Edition, are defined in this amendment. This amendment retains the WEP feature for purposes of backwards compatibility with existing IEEE 802.11 devices, but WEP is deprecated in favor of the new security features provided in this amendment.

Notice to users

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

Stuart J. Kerry, *Chair*
Al Petrick and **Harry Worstell,** *Vice-Chairs*
Tim Godfrey, *Secretary*
Brian Mathews, *Publicity Standing Committee*

Copyright © 2004 IEEE. All rights reserved.
Documents
Document Sharing Hub
Full document details: ISO_IEC 8802-11_2005_AMD6_2006

Tan Teik-Kheong, *Wireless Next Generation Standing Committee*
Terry L. Cole, *Editor*

John Fakatselis, *Chair Task Group e*
Duncan Kitchen, *Vice-Chair Task Group e*
Sheung Li, *Chair Task Group j*
Richard Paine, *Chair Task Group k*
Bob O'Hara, *Chair Task Group m*
Bruce Kramer, *Chair Task Group n*

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

David Halasz, *Chair*
Jesse Walker, *Editor*
Frank Ciotti, *Secretary*

Osama Aboul-Magd
Tomoko Adachi
Jaemin Ahn
Thomas Alexander
Areg Alimian
Richard Allen
Keith Amann
Dov Andelman
Merwyn Andrade
Carl Andren
David Andrus
Butch Anton
Hidenori Aoki
Tsuguhide Aoki
Michimasa Aramaki
Takashi Aramaki
William Arbaugh
Lee Armstrong
Larry Arnett
Hiroshi Asai
Yusuke Asai
Arthur Astrin
Malik Audeh
Geert Awater
Shahrnaz Azizi
Floyd Backes
Jin-Seok Bae
David Bagby
Dennis Baker
Ramanathan Balachander
Jaiganesh Balakrishnan
Boyd Bangerter
John Barr
Simon Barber
Farooq Bari
Michael Barkway
Kevin Barry
Anuj Batra
Burak Baysal
Tomer Bentzion
Mathilde Benveniste
Don Berry
Jan Biermann
Arnold Bilstad
Harry Bims
Bjorn Bjerke
Simon Black
Jan Boer
William Brasier
Jennifer Bray
Phillip Brownlee
Alex Bugeja
Alistair Buttar
Peter Cain
Richard Cam
Nancy Cam-Winget
Bill Carney
Pat Carson
Broady Cash
Jayant Chande
Kisoo Chang
Clint Chaplin
Ye Chen
Hong Cheng
Greg Chesson
Aik Chindapol
Sunghyun Choi
Won-Joon Choi
Woo-Yong Choi
Yang-Seok Choi
Per Christoffersson
Simon Chung
Ken Clements
Sean Coffey
Terry L. Cole
Paul Congdon
W. Steven Conner
Charles Cook
Kenneth Cook
Mary Cramer
Steven Crowley
Nora Dabbous
Rolf De Vegt
Javier del Prado Pavon
Georg Dickmann
Yoshiharu Doi
Brett Douglas
Simon Duggins
Baris Dundar
Bryan Dunn
Roger Durand
Eryk Dutkiewicz
Mary DuVal
Yaron Dycian
Dennis Eaton
Peter Ecclesine
Jonathan Edney
Bruce Edwards
Natarajan Ekambaram
Jason Ellis
Darwin Engwer
Jeff Erwin
Andrew Estrada
Christoph Euscher
Knut Evensen
John Fakatselis
Lars Falk
Steve Fantaske
Paul Feinberg
Alex Feldman
Weishi Feng
Nestor Fesas
Matthew Fischer
Wayne Fisher
Helena Flygare
Brian Ford
Ruben Formoso
Sheila Frankel
John Fuller
James Gardner
Atul Garg
Albert Garrett
Ramez Gerges
Noam Geri

Copyright © 2004 IEEE. All rights reserved.

Documents
Document Sharing Hub
Full document details: ISO_IEC 8802-11_2005_AMD6_2006

Vafa Ghazi
Monisha Ghosh
James Gilb
Jeffrey Gilbert
Rabinder Gill
Tim Godfrey
Wataru Gohda
Yuri Goldstein
Jim Goodman
Aviv Goren
Andrew Gowans
Rik Graulus
Gordon Gray
Evan Green
Patrick Green
Kerry Greer
Daqing Gu
Rajugopal Gubbi
Sam Guirguis
Srikanth Gummadi
Qiang Guo
Vivek Gupta
Herman Haisch
Steven Halford
Robert Hall
Neil Hamady
Mounir Hamdi
Christopher Hansen
Yasuo Harada
Daniel Harkins
Thomas Haslestad
Amer Hassan
Vann Hasty
James Hauser
Yutaka Hayakawa
Morihiko Hayashi
Haixiang He
Xiaoning He
Robert Heile
Frans Hermodsson
Dave Hetherington
Guido Hiertz
Garth Hillman
Christopher Hinsz
Jun Hirano
Mikael Hjelm
Jin-Meng Ho
Michael Hoghooghi
Allen Hollister
Keith Holt
Satoru Hori
William Horne
Srinath Hosur
Frank Howley
Yungping Hsu
Robert Huang
Dave Hudak
David Hunter
Syang-Myau Hwang
David Hytha
Muhammad Ikram
Daichi Imamura
Kimihiko Imamura
Yasuhiko Inoue
Katsumi Ishii
Stephen Jackson
Eric Jacobsen
Marc Jalfon
KyungHun Jang
Bruno Jechoux
Taehyun Jeon
Moo Ryong Jeong
Daniel Jiang
Kuniko Jimi
Walter Johnson
David Johnston
Jari Jokela
VK Jones
Bobby Jose
Tyan-Shu Jou
Carl Kain
Srinivas Kandala
You Sung Kang
Jeyhan Karaoguz
Kevin Karcz
Pankaj Karnik
Mika Kasslin
Dean Kawaguchi
Patrick Kelly
Richard Kennedy
Stuart Kerry
John Ketchum
Vytas Kezys
Andrew Khieu
Ryoji Kido
Tomohiro Kikuma
Byoung-Jo Kim
Dooseok Kim
Joonsuk Kim
Yongbum Kim
Yongsuk Kim
Young Kim
Youngsoo Kim
Wayne King
John Klein
Guenter Kleindl
Toshiya Kobashi
Keiichiro Koga
Lalit Kotecha
John Kowalski
Bruce Kraemer
Gopal Krishnan
Shuji Kubota
Thomas Kuehnel
Tomoaki Kumagai
Takushi Kunihiro
Thomas M. Kurihara
Denis Kuwahara
Joe Kwak
Paul Lambert
David Landeta
Jim Lansford
Colin Lanzl
Choi Law
Dongjun Lee
Insun Lee
Jae Hwa Lee
Marty Lefkowitz
Onno Letanche
Joseph Levy
Mike Lewis
Pen Li
Quinn Li
Sheung Li
Jie Liang
Wei Lih Lim
Yong Je Lim
Huashih Lin
Sheng Lin
Victor Lin
Stanley Ling
Der-Zheng Liu
I-Ru Liu
Yonghe Liu
Titus Lo
Peter Loc
Patrick Lopez
Hui-Ling Lou
Xiaolin Lu
Luke Ludeman
Yi-Jen Lung
Akira Maeki
Ravishankar Mahadevappa
Doug Makishima
Majid Malek
Rahul Malik
Jouni Malinen
Krishna Malladi
Stefan Mangold
Mahalingam Mani
Jonn Martell
Naotaka Maruyama
Paul Marzec
Brian Mathews
Yoichi Matsumoto
Sudheer Matta
Thomas Maufer
Conrad Maxwell
Stephen McCann
Kelly McClellan
Gary McCoy
William McFarland
Timothy McGovern
Bill McIntosh
Justin McNew
Irina Medvedev
Pratik Mehta
Robert Meier
Graham Melvile
Klaus Meyer
Robert Miller
Partho Mishra
David Mitton
Kenichi Miyoshi
Rishi Mohindra
Peter Molnar
Leo Monteban
Michael Montemurro
Rondal Moore
Tim Moore
Anthony Morelli
Mike Moreton

Copyright © 2004 IEEE. All rights reserved.
Documents
Document Sharing Hub
Full document details: ISO_IEC 8802-11_2005_AMD6_2006

Yuichi Morioka
Steven Morley
Robert Moskowitz
Joseph Mueller
Syed Mujtaba
Willem Mulder
Peter Murphy
Peter Murray
Andrew Myers
Andrew Myles
Yukimasa Nagai
Katsuyoshi Naka
Makoto Nakahara
Michiharu Nakamura
Seigo Nakao
Hiroyuki Nakase
Sanjiv Nanda
Ravi Narasimhan
Slobodan Nedic
Robert Neilsen
David Nelson
Dan Nemits
Chiu Ngo
Tuan Nguyen
Qiang Ni
Gunnar Nitsche
Erwin Noble
Tzvetan Novkov
Ivan Oakes
Kei Obara
Karen O'Donoghue
Hiroshi Oguma
Jongtaek Oh
Bob O'Hara
Sean O'Hara
Yoshihiro Ohtani
Chandra Olson
Timothy Olson
Hiroshi Ono
Peter Oomen
Lior Ophir
Satoshi Oyama
Richard Paine
Michael Paljug
Stephen Palm
Jong Ae Park
Jonghun Park
Joon Goo Park
Taegon Park
Steve Parker
Glenn Parsons
Vijay Patel
Eldad Perahia
Sebastien Perrot
Al Petrick
Joe Pitarresi
Leo Pluswick
Stephen Pope
James Portaro
Al Potter
Henry Ptasinski
Anuj Puri
Aleksandar Purkovic
Jim Raab
Ali Raissinia
Ajay Rajkumar
Noman Rangwala
Ivan Reede
Stanley Reible
Anthony Reid
Joe Repice
Edward Reuss
Valentine Rhodes
Maximilian Riegel
Edmund Ring
Carlos Rios
Stefan Rommer
Jon Rosdahl
John Sadowsky
Ali Sadri
Kazuyuki Sakoda
Shoji Sakurai
Kenichi Sakusabe
Hemanth Sampath
Sumeet Sandhu
Anil Sanwalka
Ryo Sawai
Tom Schaffnit
Brian Schreder
Sid Schrum
Erik Schylander
Michael Seals
Joe Sensendorf
N. Shankaranarayanan
Donald Shaver
Stephen Shellhammer
Tamara Shelton
Ian Sherlock
Matthew Sherman
Ming Sheu
Shusaku Shimada
Matthew Shoemake
William Shvodian
D. J. Shyy
Thomas Siep
Floyd Simpson
Manoneet Singh
Hasse Sinivaara
Efstratios (Stan) Skafidas
David Skellern
Roger Skidmore
Donald Sloan
Kevin Smart
David Smith
Yoram Solomon
V. Somayazulu
Amjad Soomro
Robert Soranno
Gary Spiess
William Spurgeon
Dorothy Stanley
William Steck
Greg Steele
Adrian Stephens
William Stevens
Carl Stevenson
Fred Stivers
Warren Strand
Paul Struhsaker
Michael Su
Hiroki Sugimoto
Abhaya Sumanasena
Qinfang Sun
SK Sung
Shravan Surineni
Hirokazu Tagiri
Masahiro Takagi
Mineo Takai
Katsumi Takaoka
Daisuke Takeda
Nir Tal
Tsuyoshi Tamaki
Pek-Yew Tan
Teik-Kheong Tan
Wai-Cheung Tang
Takuma Tanimoto
Henry Taylor
James Taylor
Carl Temme
Stephan ten Brink
John Terry
Timothy Thornton
Jerry Thrasher
James Tomcik
Allen Tsai
Jean Tsao
Chih Tsien
Tom Tsoulogiannis
Kwei Tu
David Tung
Sandra Turner
Mike Tzamaloukas
Marcos Tzannes
Yusuke Uchida
Takashi Ueda
Naoki Urano
Hidemi Usuba
Chandra Vaidyanathan
Hans Van Leeuwen
Richard van Leeuwen
Richard Van Nee
Nico van Waes
Allert van Zelst
Madan Venugopal
George Vlantis
Dennis Volpano
Tim Wakeley
Brad Wallace
Thierry Walrant
Vivek Wandile
Huaiyuan Wang
Stanley Wang
Christopher Ware
Fujio Watanabe
Mark Webster
Matthew Welborn
Bryan Wells
Filip Weytjens
Stephen Whitesell
Michael Wilhoyte
Michael Glenn Williams
Peter Williams

Copyright © 2004 IEEE. All rights reserved.

Documents
Document Sharing Hub
Full document details: ISO_IEC 8802-11_2005_AMD6_2006

Richard Williams
James Wilson
Steven Wilson
Jack Winters
Jin Kue Wong
Timothy Wong
Patrick Worfolk
Harry Worstell
Charles Wright
Gang Wu
Yang Xiao
James Yee
Jung Yee
Kazim Yildiz
Jijun Yin
Kit Yong
Heejung Yu
Hon Yung
Erol Yurtkuran
Zhun Zhong
Glen Zorn
James Zyren

Major contributions were received from the following individuals:

Bernard Aboba
Areg Alimian
Keith Amann
Merwyn Andrade
Arun Ayyagari
Butch Anton
Bob Beach
Simon Black
Simon Blake-Wilson
Nancy Cam-Winget
Clint Chaplin
Greg Chesson
Alan Chickinsky
Frank Ciotti
Donald Eastlake III
Jonathan Edney
Niels Ferguson
Aaron Friedman
Craig Goston
Larry Green
Daniel Harkins
Dan Hassett
Kevin Hayes
Russ Housley
Jin-Meng Ho
Dick Hubbard
Tony Jeffree
Hong Jiang
David Johnston
Asa Kalvade
Kevin Karcz
Paul Lambert
Marty Lefkowitz
Onno Letanche
Jie Liang
Jouni Malinen
Thomas Maufer
Kelly McClellan
Bill McIntosh
Graham Melville
Tim Moore
Leo Monteban
Mike Moreton
Robert Moskowitz
David Nelson
Bob O'Hara
Richard Paine
Henry Ptasinski
Ivan Reede
Carlos Rios
Phil Rogaway
Mike Sabin
Dan Simon
Doug Smith
Mike Sordi
Dorothy Stanley
Fred Stivers
Sandra Turner
Dennis Volpano
Doug Whiting
Albert Young
Glen Zorn
Arnoud Zwemmer

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

Tomoko Adachi
John Adams
Toru Aihara
James Allen
Keith Amann
Butch Anton
Eladio Arvelo
Colin Ayer
David Bagby
Daniel Bailey
John Barr
Les Baxter
Anader Benyamin-Seeyar
Barbara Bickham
Jan Boer
Gennaro Boggia
Gary Bourque
Ed Callaway
Lon Canaday
Edward Carley
Bill Carney
Clint Chaplin
Amalavoyal Chari
Brendon Chetwynd
Alan Chickinsky
Aik Chindapol
Keith Chow
Terry L. Cole
Christopher Cooke
Todor Cooklev
Todd Cooper
Javier del Prado Pavon
Guru Dutt Dhingra
Thomas Dineen
Lakshminath Dondeti
Vern Dubendorf
Sourav Dutta
Clint Early
Jonathan Edney
Carl Eklund
Michael Fischer
Michele Gammel
Corey Gates
Theodore Georgantas
Andrew Germano
Tim Godfrey
Jose Gutierrez
Chris Guy
David Halasz
Karen Halford
Steven Halford
Christopher Hansen
Robert Heile
Stuart Holoman
Russell Housley
Atsushi Ito
Peeya Iwagoshi
Tony Jeffree
David Johnston
Bobby Jose
Joe Juisai
Thomas M. Kurihara
Srinivas Kandala
Kevin Karcz
Pankaj Karnik
Michael Kelsen
Stuart Kerry
Brian Kiernan
Thomas Kolze
John Kowalski
Joe Kubler
Denis Kuwahara
William Lane
Colin Lanzl
John Lemon
Jie Liang

Copyright © 2004 IEEE. All rights reserved.
Documents
Document Sharing Hub
Full document details: ISO_IEC 8802-11_2005_AMD6_2006

Jan-Ray Liao
Randolph Little
Gregory Luri
Ryan Madron
Peter Martini
Kelly McClellan
Michael McInnis
Ingolf Meier
George Miao
Yinghua Min
Apurva Mody
Leo Monteban
Mike Moreton
Robert Moskowitz
Oliver Muelhens
Andrew Myles
Paul Nikolich
Erwin Noble
Bob O'Hara
Satoshi Oyama
Leo Pluswick
Richard Paine
Stephen Palm
Roger Pandanda
Subbu Ponnuswamy
Albert Potter
Vikram Punj
Bijan Raahemi
Moshe Ran
Terry Richards
Maximilian Riegel
Calvin Roberts
David Rockwell
Mike Rudnick
Tom Siep
Thomas Sapiano
John Sarallo
Durga Satapathy
George She
Hiroyasu Shimizu
Akihiro Shimura
Matthew Shoemake
Gil Shultz
Yoram Solomon
Amjad Soomro
Kenneth Stanwood
Thomas Starai
Adrian Stephens
Carl Stevenson
Masahiro Takagi
Pek Yew Tan
Joseph Tardo
Jerry Thrasher
Jim Tomcik
Scott Valcourt
Richard van Leeuwen
Hung-yu Wei
Stephen Whitesell
Dave Willow
Harry Worstell
Shugong Xu
Jung Yee
Patrick Yu
Oren Yuen
Arnoud Zwemmer

When the IEEE-SA Standards Board approved this standard on 24 June 2004, it had the following membership:

Don Wright, *Chair*
Steve M. Mills, *Vice Chair*
Judith Gorman, *Secretary*

Chuck Adams
H. Stephen Berger
Mark D. Bowman
Joseph A. Bruder
Bob Davis
Roberto de Boisson
Julian Forster*
Arnold M. Greenspan
Mark S. Halpin
Raymond Hapeman
Richard J. Holleman
Richard H. Hulett
Lowell G. Johnson
Joseph L. Koepfinger*
Hermann Koch
Thomas J. McGean
Daleep C. Mohla
Paul Nikolich
T. W. Olsen
Ronald C. Petersen
Gary S. Robinson
Frank Stone
Malcolm V. Thaden
Doug Topping
Joe D. Watson

*Member Emeritus

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

Satish K. Aggarwal, *NRC Representative*
Richard DeBlasio, *DOE Representative*
Alan Cookson, *NIST Representative*

Savoula Amanatidis
IEEE Standards Managing Editor

Copyright © 2004 IEEE. All rights reserved.

Documents
Document Sharing Hub
Full document details: ISO_IEC 8802-11_2005_AMD6_2006

Contents

1. Overview ... 1

1.2 Purpose ... 1

2. Normative references ... 2

3. Definitions ... 2

4. Abbreviations and acronyms ... 6

5. General description ... 8

5.1 General description of the architecture ... 8
5.1.1 How wireless LAN systems are different ... 8
5.1.1.4 Interaction with other IEEE 802® layers ... 8
5.1.1.5 Interaction with non-IEEE 802 protocols ... 8
5.2 Components of the IEEE 802.11 architecture ... 8
5.2.2 Distribution system (DS) concepts ... 8
5.2.2.2 RSNA ... 8
5.3 Logical service interfaces ... 9
5.3.1 Station service (SS) ... 9
5.4 Overview of the services ... 9
5.4.2 Services that support the distribution service ... 9
5.4.2.2 Association ... 9
5.4.2.3 Reassociation ... 9
5.4.3 Access control and confidentiality ~~control~~services ... 9
5.4.3.1 Authentication ... 10
5.4.3.2 Deauthentication ... 11
5.4.3.3 ~~Privacy~~Confidentiality ... 11
5.4.3.4 Key management ... 12
5.4.3.5 Data origin authenticity ... 12
5.4.3.6 Replay detection ... 12
5.6 Differences between ESS and IBSS LANs ... 12
5.7 Message information contents that support the services ... 13
5.7.5 ~~Privacy~~Confidentiality ... 13
5.7.6 Authentication ... 13
5.7.7 Deauthentication ... 13
5.8 Reference model ... 13
5.9 IEEE 802.11 and IEEE 802.1X ... 14
5.9.1 IEEE 802.11 usage of IEEE 802.1X ... 14
5.9.2 Infrastructure functional model overview ... 14
5.9.2.1 AKM operations with AS ... 14
5.9.2.2 Operations with PSK ... 17
5.9.3 IBSS functional model description ... 17
5.9.3.1 Key usage ... 17
5.9.3.2 Sample IBSS 4-Way Handshakes ... 17
5.9.3.3 IBSS IEEE 802.1X Example ... 19
5.9.4 Authenticator-to-AS protocol ... 19
5.9.5 PMKSA caching ... 20

6. MAC service definition ... 20

Copyright © 2004 IEEE. All rights reserved.
Documents Document Sharing Hub
Full document details: ISO_IEC 8802-11_2005_AMD6_2006

6.1 Overview of MAC services ... 20
6.1.2 Security services ... 20
6.1.4 MAC data service architecture ... 21

7. Frame formats ... 22

7.1 MAC frame formats ... 22
7.1.3 Frame fields ... 22
7.1.3.1 Frame Control field ... 22
7.2 Format of individual frame types ... 23
7.2.2 Data frames ... 23
7.2.3 Management frames ... 23
7.2.3.1 Beacon frame format ... 23
7.2.3.4 Association Request frame format ... 24
7.2.3.6 Reassociation Request frame format ... 24
7.2.3.9 Probe Response frame format ... 24
7.2.3.10 Authentication frame format ... 24
7.3 Management frame body components ... 25
7.3.1 Fixed fields ... 25
7.3.1.4 Capability Information field ... 25
7.3.1.7 Reason Code field ... 25
7.3.1.9 Status Code field ... 26
7.3.2 Information elements ... 26
7.3.2.25 RSN information element ... 27

8. Security ... 32

8.1 Framework ... 32
8.1.1 Security methods ... 32
8.1.2 RSNA equipment and RSNA capabilities ... 32
8.1.3 RSNA establishment ... 32
8.1.4 RSNA assumptions and constraints (informative) ... 34
8.2 Pre-RSNA security methods ... 34
8.2.1 Wired equivalent privacy (WEP) ... 35
8.2.1.1 WEP overview ... 35
8.2.1.2 WEP MPDU format ... 35
8.2.1.3 WEP state ... 36
8.2.1.4 WEP procedures ... 36
8.2.2 Pre-RSNA authentication ... 38
8.2.2.1 Overview ... 38
8.2.2.2 Open System authentication ... 38
8.2.2.3 Shared Key authentication ... 39
8.3 RSNA data confidentiality protocols ... 43
8.3.1 Overview ... 43
8.3.2 Temporal Key Integrity Protocol (TKIP) ... 43
8.3.2.1 TKIP overview ... 43
8.3.2.2 TKIP MPDU formats ... 45
8.3.2.3 TKIP MIC ... 46
8.3.2.4 TKIP countermeasures procedures ... 49
8.3.2.5 TKIP mixing function ... 52
8.3.2.6 TKIP replay protection procedures ... 56
8.3.3 CTR with CBC-MAC Protocol (CCMP) ... 57
8.3.3.1 CCMP overview ... 57
8.3.3.2 CCMP MPDU format ... 57

Copyright © 2004 IEEE. All rights reserved.

Documents
Document Sharing Hub
Full document details: ISO_IEC 8802-11_2005_AMD6_2006

8.3.3.3 CCMP encapsulation ... 58
8.3.3.4 CCMP decapsulation ... 60
8.4 RSNA security association management ... 62
8.4.1 Security associations ... 62
8.4.1.1 Security association definitions ... 62
8.4.1.2 Security association life cycle ... 64
8.4.2 RSNA selection ... 66
8.4.3 RSNA policy selection in an ESS ... 66
8.4.3.1 TSN policy selection in an ESS ... 67
8.4.4 RSNA policy selection in an IBSS ... 67
8.4.4.1 TSN policy selection in an IBSS ... 68
8.4.5 RSN management of the IEEE 802.1X Controlled Port ... 68
8.4.6 RSNA authentication in an ESS ... 68
8.4.6.1 Preauthentication and RSNA key management ... 69
8.4.6.2 Cached PMKSAs and RSNA key management ... 70
8.4.7 RSNA authentication in an IBSS ... 70
8.4.8 RSNA key management in an ESS ... 71
8.4.9 RSNA key management in an IBSS ... 72
8.4.10 RSNA security association termination ... 72
8.5 Keys and key distribution ... 73
8.5.1 Key hierarchy ... 73
8.5.1.1 PRF ... 74
8.5.1.2 Pairwise key hierarchy ... 75
8.5.1.3 Group key hierarchy ... 76
8.5.2 EAPOL-Key frames ... 77
8.5.2.1 STAKey Handshake for STA-to-STA link security ... 84
8.5.2.2 EAPOL-Key frame notation ... 84
8.5.3 4-Way Handshake ... 85
8.5.3.1 4-Way Handshake Message 1 ... 86
8.5.3.2 4-Way Handshake Message 2 ... 87
8.5.3.3 4-Way Handshake Message 3 ... 87
8.5.3.4 4-Way Handshake Message 4 ... 89
8.5.3.5 4-Way Handshake implementation considerations ... 89
8.5.3.6 Sample 4-Way Handshake (informative) ... 90
8.5.3.7 4-Way Handshake analysis (informative) ... 91
8.5.4 Group Key Handshake ... 92
8.5.4.1 Group Key Handshake Message 1 ... 93
8.5.4.2 Group Key Handshake Message 2 ... 94
8.5.4.3 Group Key Handshake implementation considerations ... 94
8.5.4.4 Sample Group Key Handshake (informative) ... 94
8.5.5 STAKey Handshake ... 95
8.5.5.1 STAKey Request message ... 96
8.5.5.2 STAKey Message 1 ... 96
8.5.5.3 STAKey Message 2 ... 97
8.5.5.4 STAKey Message 1 and Message 2 to the initiating STA ... 97
8.5.6 RSNA Supplicant key management state machine ... 98
8.5.6.1 Supplicant state machine states ... 98
8.5.6.2 Supplicant state machine variables ... 99
8.5.6.3 Supplicant state machine procedures ... 99
8.5.7 RSNA Authenticator key management state machine ... 102
8.5.7.1 Authenticator state machine states ... 105
8.5.7.2 Authenticator state machine variables ... 106
8.5.7.3 Authenticator state machine procedures ... 108
8.5.8 Nonce generation (informative) ... 108

Copyright © 2004 IEEE. All rights reserved.
Documents
Document Sharing Hub
Full document details: ISO_IEC 8802-11_2005_AMD6_2006

8.6 Mapping EAPOL keys to IEEE 802.11 keys ... 108
8.6.1 Mapping PTK to TKIP keys ... 108
8.6.2 Mapping GTK to TKIP keys ... 108
8.6.3 Mapping PTK to CCMP keys ... 109
8.6.4 Mapping GTK to CCMP keys ... 109
8.6.5 Mapping GTK to WEP-40 keys ... 109
8.6.6 Mapping GTK to WEP-104 keys ... 109
8.7 Per-frame pseudo-code ... 109
8.7.1 WEP frame pseudo-code ... 109
8.7.2 RSNA frame pseudo-code ... 111
8.7.2.1 Per-MSDU Tx pseudo-code ... 111
8.7.2.2 Per-MPDU Tx pseudo-code ... 112
8.7.2.3 Per-MPDU Rx pseudo-code ... 112
8.7.2.4 Per-MSDU Rx pseudo-code ... 113

10. Layer management ... 114

10.3 MLME SAP interface ... 114
10.3.2 Scan ... 114
10.3.2.2 MLME-SCAN.confirm ... 114
10.3.6 Associate ... 114
10.3.6.1 MLME-ASSOCIATE.request ... 114
10.3.6.3 MLME-ASSOCIATE.indication ... 114
10.3.7 Reassociate ... 115
10.3.7.1 MLME-REASSOCIATE.request ... 115
10.3.7.3 MLME-REASSOCIATE.indication ... 115
10.3.17 SetKeys ... 116
10.3.17.1 MLME-SETKEYS.request ... 116
10.3.17.2 MLME-SETKEYS.confirm ... 117
10.3.18 DeleteKeys ... 117
10.3.18.1 MLME-DELETEKEYS.request ... 117
10.3.18.2 MLME-DELETEKEYS.confirm ... 118
10.3.19 MIC (Michael) failure event ... 118
10.3.19.1 MLME-MICHAELMICFAILURE.indication ... 118
10.3.20 EAPOL ... 119
10.3.20.1 MLME-EAPOL.request ... 119
10.3.20.2 MLME-EAPOL.confirm ... 120
10.3.21 MLME-STAKEYESTABLISHED ... 121
10.3.21.1 MLME-STAKEYESTABLISHED.indication ... 121
10.3.22 SetProtection ... 121
10.3.22.1 MLME-SETPROTECTION.request ... 121
10.3.22.2 MLME-SETPROTECTION.confirm ... 122
10.3.23 MLME-PROTECTEDFRAMEDROPPED ... 123
10.3.23.1 MLME- PROTECTEDFRAMEDROPPED.indication ... 123

11. MAC sublayer management entity ... 123

11.3 Association and reassociation ... 123
11.3.1 Authentication—originating STA ... 124
11.3.2 Authentication—destination STA ... 124
11.3.3 Deauthentication—originating STA ... 124
11.3.4 Deauthentication—destination STA ... 124
11.4 Association, reassociation, and disassociation ... 125
11.4.1 STA association procedures ... 125

Copyright © 2004 IEEE. All rights reserved.

Documents
Document Sharing Hub
Full document details: ISO_IEC 8802-11_2005_AMD6_2006

11.4.2 AP association procedures ... 125
11.4.3 STA reassociation procedures ... 126
11.4.4 AP reassociation procedures ... 126
11.4.5 STA disassociation procedures ... 127
11.4.6 AP disassociation procedures ... 127

Annex A (normative) Protocol Implementation Conformance Statements (PICS) ... 128

A.4 PICS proforma—IEEE Std 802.11, 1999 Edition ... 128
A.4.4 MAC protocol ... 128

Annex C (normative) Formal description of MAC operation ... 130

C.3 State machines for MAC stations ... 130
C.4 State machines for MAC AP ... 130

Annex D (normative) ASN.1 encoding of the MAC and PHY MIB ... 131

Annex E (informative) Bibliography ... 147

E.1 General ... 147

Annex H (informative) RSNA reference implementations and test vectors ... 148

H.1 TKIP temporal key mixing function reference implementation and test vector ... 148
H.1.1 Test vectors ... 156
H.2 Michael reference implementation and test vectors ... 157
H.2.1 Michael test vectors ... 157
H.2.2 Sample code for Michael ... 158
H.3 PRF reference implementation and test vectors ... 164
H.3.1 PRF reference code ... 164
H.3.2 PRF test vectors ... 165
H.4 Suggested pass-phrase-to-PSK mapping ... 165
H.4.1 Introduction ... 165
H.4.2 Reference implementation ... 166
H.4.3 Test vectors ... 167
H.5 Suggestions for random number generation ... 167
H.5.1 Software sampling ... 168
H.5.2 Hardware-assisted solution ... 169
H.6 Additional test vectors ... 170
H.6.1 Notation ... 170
H.6.2 WEP encapsulation ... 170
H.6.3 TKIP test vector ... 171
H.6.4 CCMP test vector ... 172
H.6.5 PRF test vectors ... 173
H.7 Key hierarchy test vectors ... 174
H.7.1 Pairwise key derivation ... 174

Annex I (normative) Patents ... 176

Copyright © 2004 IEEE. All rights reserved.
Documents
Document Sharing Hub
Full document details: ISO_IEC 8802-11_2005_AMD6_2006

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 6: Medium Access Control (MAC) Security Enhancements

[This amendment is based on IEEE Std 802.11™, 1999 Edition (Reaff 2003), as amended by IEEE Stds 802.11a™-1999, 802.11b™-1999, 802.11b™-1999/Cor 1-2001, 802.11d™-2001, 802.11g™-2003, and 802.11h™-2003.]

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 small corrections in existing text or tables. The editing instruction specifies the location of the change and describes what is being changed either by using ~~strikethrough~~ (to remove old material) or 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 large changes in existing text, subclauses, tables, or figures by removing existing material and replacing it with new material. Editorial notes will not be carried over into future editions.

1. Overview

1.2 Purpose

Change the fifth bullet of 1.2 as follows:

— Describes the requirements and procedures to provide ~~privacy~~confidentiality of user information being transferred over the wireless medium (WM) and authentication of IEEE 802.11 conformant devices.

End of changes to Clause 1.

Copyright © 2004 IEEE. All rights reserved.

Documents
Document Sharing Hub
Full document details: ISO_IEC 8802-11_2005_AMD6_2006

2. Normative references

Insert the following references at the appropriate locations in Clause 2:

FIPS PUB 180-1-1995, Secure Hash Standard.[1]

FIPS PUB 197-2001, Advanced Encryption Standard (AES).

IEEE P802.1X™-REV, Draft Standard for Local and Metropolitan Area Networks: Port-Based Network Access Control.[2, 3, 4]

IETF RFC 1321, The MD5 Message-Digest Algorithm, April 1992.[5]

IETF RFC 1750, Randomness Recommendations for Security, December 1994.

IETF RFC 2104, HMAC: Keyed-Hashing for Message Authentication, February 1997.

IETF RFC 2202, Test Cases for HMAC-MD5 and HMAC-SHA-1, September 1997.

IETF RFC 3394, Advanced Encryption Standard (AES) Key Wrap Algorithm, September 2002.

IETF RFC 3610, Counter with CBC-MAC (CCM), September 2003.

IETF RFC 3748, Extensible Authentication Protocol (EAP), March 2004.

End of changes to Clause 2.

3. Definitions

Delete the definition "3.40 privacy."

Change the definition for "wired equivalent privacy (WEP)" as follows:

3.49 wired equivalent privacy (WEP): ~~The~~ An optional cryptographic confidentiality algorithm specified by IEEE 802.11 that may be used to provide data confidentiality that is subjectively equivalent to the confidentiality of a wired local area network (LAN) medium that does not employ cryptographic techniques to enhance ~~privacy~~ confidentiality.

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

3.63 additional authentication data (AAD): Data that are not encrypted, but are cryptographically protected.

[1]FIPS publications are available from the National Technical Information Service (NTIS), U. S. Dept. of Commerce, 5285 Port Royal Road, Springfield, VA 22161 (http://www.ntis.org/).

[2]IEEE publications are available from the Institute of Electrical and Electronics Engineers, Inc., 445 Hoes Lane, Piscataway, NJ 08854, USA (http://standards.ieee.org/).

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

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

[5]Internet RFCs are available from the Internet Engineering Task Force at http://www.ietf.org/.

Copyright © 2004 IEEE. All rights reserved.
Documents
Document Sharing Hub
Full document details: ISO_IEC 8802-11_2005_AMD6_2006

3.64 authentication, authorization, and accounting (AAA) key: Key information that is jointly negotiated between the Supplicant and the Authentication Server (AS). This key information is transported via a secure channel from the AS to the Authenticator. The pairwise master key (PMK) may be derived from the AAA key.

3.65 authentication and key management (AKM) suite: A set of AKM suite selectors.

3.66 Authentication Server (AS): An entity that provides an authentication service to an Authenticator. This service determines, from the credentials provided by the Supplicant, whether the Supplicant is authorized to access the services provided by the Authenticator. (IEEE P802.1X-REV[6])

3.67 Authenticator: An entity at one end of a point-to-point LAN segment that facilitates authentication of the entity attached to the other end of that link. (IEEE P802.1X-REV)

3.68 Authenticator address (AA): The IEEE 802.1X Authenticator medium access control (MAC) address.

3.69 authorized: To be explicitly allowed.

3.70 big endian: The concept that, for a given multi-octet numeric representation, the most significant octet has the lowest address.

3.71 cipher suite: A set of one or more algorithms, designed to provide data confidentiality, data authenticity or integrity, and/or replay protection.

3.72 counter mode (CTR) with CBC-MAC [cipher-block chaining (CBC) with message authentication code (MAC)] (CCM): A symmetric key block cipher mode providing confidentiality using CTR and data origin authenticity using CBC-MAC.

NOTE—See IETF RFC 3610.

3.73 decapsulate: To recover an unprotected frame from a protected one.

3.74 decapsulation: The process of generating plaintext data by decapsulating an encapsulated frame.

3.75 EAPOL-Key confirmation key (KCK): A key used to integrity-check an EAPOL-Key frame.

3.76 EAPOL-Key encryption key (KEK): A key used to encrypt the Key Data field in an EAPOL-Key frame.

3.77 encapsulate: To construct a protected frame from an unprotected frame.

3.78 encapsulation: The process of generating the cryptographic payload from the plaintext data. This comprises the cipher text as well as any associated cryptographic state required by the receiver of the data, e.g., initialization vectors (IVs), sequence numbers, message integrity codes (MICs), key identifiers.

3.79 4-Way Handshake: A pairwise key management protocol defined by this amendment. It confirms mutual possession of a pairwise master key (PMK) by two parties and distributes a group temporal key (GTK).

3.80 group: The entities in a wireless network, e.g., an access point (AP) and its associated stations (STAs), or all the STAs in an independent basic service set (IBSS) network.

[6]Information on references can be found in Clause 2.

Copyright © 2004 IEEE. All rights reserved.

Documents Document Sharing Hub
Full document details: ISO_IEC 8802-11_2005_AMD6_2006

3.81 Group Key Handshake: A group key management protocol defined by this amendment. It is used only to issue a new group temporal key (GTK) to peers with whom the local station (STA) has already formed security associations.

3.82 group master key (GMK): An auxiliary key that may be used to derive a group temporal key (GTK).

3.83 group temporal key (GTK): A random value, assigned by the broadcast/multicast source, which is used to protect broadcast/multicast medium access control (MAC) protocol data units (MPDUs) from that source. The GTK may be derived from a group master key (GMK).

3.84 group temporal key security association (GTKSA): The context resulting from a successful group temporal key (GTK) distribution exchange via either a Group Key Handshake or a 4-Way Handshake.

3.85 IEEE 802.1X authentication: Extensible Authentication Protocol (EAP) authentication transported by the IEEE 802.1X protocol.

3.86 key counter: A 256-bit (32-octet) counter that is used in the pseudo-random function (PRF) to generate initialization vectors (IVs). There is a single key counter per station (STA) that is global to that STA.

3.87 key data encapsulation (KDE): Format for data other than information elements in the EAPOL-Key Data field.

3.88 key management service: A service to distribute and manage cryptographic keys within a robust security network (RSN).

3.89 little endian: The concept that, for a given multi-octet numeric representation, the least significant octet has the lowest address.

3.90 liveness: A demonstration that the peer is actually participating in this instance of communication.

3.91 message integrity code (MIC): A value generated by a symmetric key cryptographic function. If the input data are changed, a new value cannot be correctly computed without knowledge of the symmetric key. Thus, the secret key protects the input data from undetectable alteration. This is traditionally called a *message authentication code* (MAC), but the acronym MAC is already reserved for another meaning in this amendment.

3.92 Michael: The message integrity code (MIC) for the Temporal Key Integrity Protocol (TKIP).

3.93 nonce: A value that shall not be reused with a given key, including over all reinitializations of the system through all time.

3.94 pairwise: Two entities that are associated with each other, e.g., an access point (AP) and an associated station (STA), or a pair of STAs in an independent basic service set (IBSS) network. This term is used to describe the key hierarchies for keys that are shared only between the two entities in a pairwise association.

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

3.96 pairwise master key security association (PMKSA): The context resulting from a successful IEEE 802.1X authentication exchange between the peer and Authentication Server (AS) or from a preshared key (PSK).

Copyright © 2004 IEEE. All rights reserved.
Documents
Document Sharing Hub
Full document details: ISO_IEC 8802-11_2005_AMD6_2006

3.97 pairwise transient key (PTK): A value that is derived from the pairwise master key (PMK), Authenticator address (AA), Supplicant address (SPA), Anthenticator 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).

3.98 pairwise transient key security association (PTKSA): The context resulting from a successful 4-Way Handshake exchange between the peer and Authenticator.

3.99 pass-phrase: A secret text string employed to corroborate the user's identity.

3.100 per-frame encryption key: A unique encryption key constructed for each medium access control (MAC) protocol data unit (MPDU), employed by some IEEE 802.11 security protocols.

3.101 per-frame sequence counter: For Temporal Key Integrity Protocol (TKIP), the counter that is used as the nonce in the derivation of the per-frame encryption key. For CCM [counter mode (CTR) with cipher-block chaining (CBC) with message authentication code (MAC)] Protocol (CCMP), the per-frame initialization vector (IV).

3.102 pre-robust security network association (pre-RSNA): The type of association used by a pair of stations (STAs) if the procedure for establishing authentication or association between them did not include the 4-Way Handshake.

3.103 pre-robust security network association (pre-RSNA) equipment: A device that is not able to create robust security network associations (RSNAs).

3.104 preshared key (PSK): A static key that is distributed to the units in the system by a method outside the scope of this amendment, always by some out-of-band means.

3.105 pseudo-random function (PRF): A function that hashes various inputs to derive a pseudo-random value. To add liveness to the pseudo-random value, a nonce should be one of the inputs.

3.106 robust security network (RSN): A security network that allows only the creation of robust security network associations (RSNAs). An RSN can be identified by the indication in the RSN Information Element (IE) of Beacon frames that the group cipher suite specified is not wired equivalent privacy (WEP).

3.107 robust security network association (RSNA): The type of association used by a pair of stations (STAs) if the procedure to establish authentication or association between them includes the 4-Way Handshake. Note that the existence of a RSNA by a pair of devices does not of itself provide robust security. Robust security is provided when all devices in the network use RSNAs.

3.108 robust-security-network-association- (RSNA-) capable equipment: A station (STA) that is able to create RSNAs. Such a device can use pre-RSNAs because of configuration. Notice that RSNA-capable does not imply full compliance with the RSNA Protocol Implementation Conformance Statement (PICS). A legacy device that has been upgraded to support Temporal Key Integrity Protocol (TKIP) can be RSNA-capable, but will not be compliant with the PICS if it does not also support CCM [counter mode (CTR) with cipher-block chaining (CBC) with message authentication code (MAC)] Protocol (CCMP).

3.109 robust-security-network-association- (RSNA-) enabled equipment: A station (STA) when it is RSNA-capable and `dot11RSNAEnabled` is set to TRUE.

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

Copyright © 2004 IEEE. All rights reserved.

Documents Document Sharing Hub

Full document details: ISO_IEC 8802-11_2005_AMD6_2006

3.111 security network: A basic service set (BSS) where the station (STA) starting the BSS provides information about the security capabilities and configuration of the BSS by including the robust security network (RSN) information element in Beacon frames.

3.112 selector: An item specifying a list constituent in an IEEE 802.11 Management Message information element.

3.113 STAKey: A symmetric key used to protect direct station-to-station (STA-to-STA) communication in an infrastructure basic service set (BSS).

3.114 STAKey Handshake: A STAKey key management protocol, used to issue a new STAKey to stations (STAs) that have a pairwise transient key security association (PTKSA) with an access point (AP).

3.115 STAKey security association (STAKeySA): The security context for direct station-to-station (STA-to-STA) communication in an infrastructure basic service set (BSS). A STAKeySA includes a STAKey.

3.116 Supplicant: An entity at one end of a point-to-point LAN segment that is being authenticated by an Authenticator attached to the other end of that link. (IEEE P802.1X-REV)

3.117 Supplicant address (SPA): The Supplicant's medium access control (MAC) address**.**

3.118 temporal encryption key: The portion of a pairwise transient key (PTK) or group temporal key (GTK) used directly or indirectly to encrypt data in medium access control (MAC) protocol data units (MPDUs).

3.119 temporal key: The combination of temporal encryption key and temporal message integrity code (MIC) key.

3.120 temporal message integrity code (MIC) key: The portion of a transient key used to ensure the integrity of medium access control (MAC) service data units (MSDUs) or MAC protocol data units (MPDUs).

3.121 transition security network (TSN): A security network that allows the creation of pre-robust security network associations (pre-RSNAs) as well as RSNAs. A TSN can be identified by the indication in the robust security network (RSN) information element of Beacon frames that the group cipher suite in use is wired equivalent privacy (WEP).

End of changes to Clause 3.

4. Abbreviations and acronyms

Insert the following abbreviations in alphabetical order into Clause 4:

AA	Authenticator address
AAA	authentication, authorization, and accounting
AAD	additional authentication data
AES	advanced encryption standard
AKM	authentication and key management
AKMP	Authentication and Key Management Protocol
ANonce	Authenticator nonce
ARP	Address Resolution Protocol
AS	Authentication Server
CBC	cipher-block chaining
CBC-MAC	cipher-block chaining with message authentication code

Copyright © 2004 IEEE. All rights reserved.
Documents Document Sharing Hub
Full document details: ISO_IEC 8802-11_2005_AMD6_2006

CCM	CTR with CBC-MAC
CCMP	CTR with CBC-MAC Protocol
CTR	counter mode
EAP	Extensible Authentication Protocol (IETF RFC 3748)
EAPOL	Extensible Authentication Protocol over LANs (IEEE P802.1X-REV)
GMK	group master key
GNonce	group nonce
GTK	group temporal key
GTKSA	group temporal key security association
ICMP	Internet Control Message Protocol
KCK	EAPOL-Key confirmation key
KDE	key data encapsulation
KEK	EAPOL-Key encryption key
LFSR	linear feedback shift register
MIC	message integrity code
NTP	Network Time Protocol (IETF RFC 1305 [B12][7])
OUI	organizationally unique identifier
PAE	port access entity (IEEE P802.1X-REV)
PMK	pairwise master key
PMKID	pairwise master key identifier
PMKSA	pairwise master key security association
PN	packet number
PRF	pseudo-random function
PRNG	pseudo-random number generator
PSK	preshared key
PTK	pairwise transient key
PTKSA	pairwise transient key security association
RADIUS	remote authentication dial-in user service (IETF RFC 2865 [B14])
RSC	broadcast/multicast transmit sequence counter
RSN	robust security network
RSNA	robust security network association
SNAP	Sub-Network Access Protocol
SNonce	Supplicant nonce
SPA	Supplicant address
TKIP	Temporal Key Integrity Protocol
TSC	TKIP sequence counter
TSN	transition security network
TTAK	TKIP-mixed transmit address and key
UCT	unconditional transfer

End of changes to Clause 4.

[7]The numbers in brackets correspond to the numbers of the bibliography in Annex E.

Copyright © 2004 IEEE. All rights reserved.

Documents Document Sharing Hub
Full document details: ISO_IEC 8802-11_2005_AMD6_2006

5. General description

5.1 General description of the architecture

5.1.1 How wireless LAN systems are different

5.1.1.4 Interaction with other IEEE 802® layers

Insert the following paragraph at the end of 5.1.1.4:

In a robust security network association (RSNA), IEEE 802.11 provides functions to protect data frames, IEEE 802.1X provides authentication and a Controlled Port, and IEEE 802.11 and IEEE 802.1X collaborate to provide key management. All stations (STAs) in an RSNA have a corresponding IEEE 802.1X entity that handles these services. This amendment defines how an RSNA utilizes IEEE 802.1X to access these services.

After 5.1.1.4, insert 5.1.1.5:

5.1.1.5 Interaction with non-IEEE 802 protocols

An RSNA utilizes non-IEEE 802 protocols for its authentication and key management (AKM) services. Some of these protocols are defined by other standards organizations, such as the Internet Engineering Task Force (IETF).

5.2 Components of the IEEE 802.11 architecture

5.2.2 Distribution system (DS) concepts

After 5.2.2.1, insert 5.2.2.2:

5.2.2.2 RSNA

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 encapsulation mechanism, called CTR [counter mode] with CBC-MAC [cipher-block chaining (CBC) with message authentication code (MAC)] Protocol (CCMP), and, optionally, Temporal Key Integrity Protocol (TKIP)

An RSNA relies on several components external to the IEEE 802.11 architecture.

The first component is an IEEE 802.1X port access entity (PAE). PAEs are present on all STAs in an RSNA and control the forwarding of data to and from the medium access control (MAC). An access point (AP) always implements an Authenticator PAE and implements the EAP Authenticator role, and a STA always implements a Supplicant PAE and implements the Extensible Authentication Protocol (EAP) peer role. In an independent basic service set (IBSS), each STA implements both an Authenticator PAE and a Supplicant PAE and both the EAP Authenticator and EAP peer roles.

Copyright © 2004 IEEE. All rights reserved.
Documents Document Sharing Hub
Full document details: ISO_IEC 8802-11_2005_AMD6_2006

A second component is the Authentication Server (AS). The AS may authenticate the elements of the RSNA itself, i.e., the non-AP STAs; and APs may provide material that the RSNA elements can use to authenticate each other. The AS communicates through the IEEE 802.1X Authenticator with the IEEE 802.1X Supplicant on each STA, enabling the STA to be authenticated to the AS and vice versa. An RSNA depends upon the use of an EAP method that supports mutual authentication of the AS and the STA. In certain applications, the AS may be integrated into the same physical device as the AP, or into a STA in an IBSS.

5.3 Logical service interfaces

Change item g) in the list of architectural services in 5.3 as follows:

g) ~~Privacy~~Confidentiality

5.3.1 Station service (SS)

Change item c) in the list of SSs in 5.3.1 as follows:

c) ~~Privacy~~Confidentiality

5.4 Overview of the services

5.4.2 Services that support the distribution service

5.4.2.2 Association

Insert the following paragraph after the second paragraph of 5.4.2.2:

Within a robust security network (RSN), this is different. In an RSNA, the IEEE 802.1X Port determines when to allow data traffic across an IEEE 802.11 link. A single IEEE 802.1X Port maps to one association, and each association maps to an IEEE 802.1X Port. An IEEE 802.1X Port consists of an IEEE 802.1X Controlled Port and an IEEE 802.1X Uncontrolled Port. The IEEE 802.1X Controlled Port is blocked from passing general data traffic between two STAs until an IEEE 802.1X authentication procedure completes successfully over the IEEE 802.1X Uncontrolled Port. Once the AKM completes successfully, data protection is enabled to prevent unauthorized access, and the IEEE 802.1X Controlled Port unblocks to allow protected data traffic. IEEE 802.1X Supplicants and Authenticators exchange protocol information via the IEEE 802.1X Uncontrolled Port. It is expected that most other protocol exchanges will make use of the IEEE 802.1X Controlled Ports. However, a given protocol may need to bypass the authorization function and make use of the IEEE 802.1X Uncontrolled Port.

NOTE—See IEEE P802.1X-REV for a discussion of Controlled Port and Uncontrolled Port.

5.4.2.3 Reassociation

Insert the following paragraph at the end of 5.4.2.3:

No facilities are provided to move an RSNA during reassociation. Therefore, the old RSNA will be deleted, and a new RSNA will need to be constructed.

Change the title of 5.4.3 as follows:

5.4.3 Access control and confidentiality ~~control~~services

Change the second paragraph of 5.4.3 as follows:

Copyright © 2004 IEEE. All rights reserved.

Documents Document Sharing Hub
Full document details: ISO_IEC 8802-11_2005_AMD6_2006

Two services are provided to bring the IEEE 802.11 functionality in line with wired local area network (LAN) assumptions: authentication and ~~privacy~~confidentiality. Authentication is used instead of the wired media physical connection. ~~Privacy~~ Data confidentiality is used to provide the confidential aspects of closed wired media.

Insert the following paragraphs at the end of 5.4.3:

In a wireless LAN (WLAN) that does not support RSNA, two services, authentication and confidentiality, are defined. IEEE 802.11 authentication is used instead of the wired media physical connection. WEP encryption was defined to provide the confidentiality aspects of closed wired media.

An RSNA uses the IEEE 802.1X authentication service along with TKIP and CCMP to provide access control. The IEEE 802.11 station management entity (SME) provides key management via an exchange of IEEE 802.1X EAPOL-Key frames. Confidentiality and data integrity are provided by RSN key management together with the TKIP and CCMP.

5.4.3.1 Authentication

Replace the text of 5.4.3.1 with the following:

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

IEEE 802.11 attempts to control LAN access via the authentication service. IEEE 802.11 authentication is an SS. This service may be used by all STAs to establish their identity to STAs with which they communicate, in both extended service set (ESS) and IBSS networks. If a mutually acceptable level of authentication has not been established between two STAs, an association shall not be established.

IEEE 802.11 defines two authentication methods: Open System authentication and Shared Key authentication. Open System authentication admits any STA to the DS. Shared Key authentication relies on WEP to demonstrate knowledge of a WEP encryption key. The IEEE 802.11 authentication mechanism also allows definition of new authentication methods.

An RSNA also supports authentication based on IEEE 802.1X, or preshared keys (PSKs). IEEE 802.1X authentication utilizes the EAP to authenticate STAs and the AS with one another. This amendment does not specify an EAP method that is mandatory to implement. See 8.4.4 for a description of the IEEE 802.1X authentication and PSK usage within an IEEE 802.11 IBSS.

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

The Open System authentication algorithm is used in both basic service set (BSS) and IBSS RSNAs, although Open System authentication is optional in an RSNA IBSS. RSNA disallows the use of Shared Key authentication.

Management information base (MIB) functions are provided in Annex D to support the standardized authentication schemes.

A STA may be authenticated with many other STAs at any given instant.

Copyright © 2004 IEEE. All rights reserved.
Documents
Document Sharing Hub
Full document details: ISO_IEC 8802-11_2005_AMD6_2006

5.4.3.2 Deauthentication

Change the text of 5.4.3.2 as follows:

The deauthentication service is invoked when an existing Open System or Shared Key authentication is to be terminated. Deauthentication is an SS.

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

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

In an RSNA, deauthentication also destroys any related PTKSA, group temporal key security association (GTKSA), and STAKey security associations (STAKeySAs) that exist in the STA and closes the associated IEEE 802.1X Controlled Port. If pairwise master key (PMK) caching is not enabled, deauthentication also destroys the pairwise master key security association (PMKSA) from which the deleted PTKSA was derived.

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

Change the title and text of 5.4.3.3 as follows:

5.4.3.3 ~~Privacy~~Confidentiality

In a wired LAN, only those stations physically connected to the wire ~~may hear~~ can send or receive LAN traffic. With a wireless shared medium, this is not the case. Any IEEE 802.11-compliant STA ~~may hear~~ can receive all like-PHY IEEE 802.11 traffic that is within range and can transmit to any other IEEE 802.11 STA within range. Thus the connection of a single wireless link (without ~~privacy~~confidentiality) to an existing wired LAN may seriously degrade the security level of the wired LAN.

To bring the ~~functionality~~ security of the wireless LAN up to the level implicit in wired LAN design, IEEE 802.11 provides the ability to ~~encrypt~~ protect the contents of messages. This functionality is provided by the ~~privacy~~confidentiality service. ~~Privacy~~Confidentiality is an SS.

~~IEEE 802.11 specifies an optional privacy algorithm, WEP, that is designed to satisfy the goal of wired LAN "equivalent" privacy. The algorithm is not designed for ultimate security but rather to be "at least as secure as a wire." See Clause 8 for more details.~~

~~IEEE 802.11 uses the WEP mechanism (see Clause 8) to perform the actual encryption of messages. MIB functions are provided to support WEP.~~

~~Note that privacy may only be invoked for data frames and some Authentication Management frames. All stations initially start "in the clear" in order to set up the authentication and privacy services.~~

Copyright © 2004 IEEE. All rights reserved.

Documents Document Sharing Hub
Full document details: ISO_IEC 8802-11_2005_AMD6_2006

IEEE 802.11 provides three cryptographic algorithms to protect data traffic: WEP, TKIP, and CCMP. WEP and TKIP are based on the RC4[8] algorithm, and CCMP is based on the advanced encryption standard (AES). A means is provided for STAs to select the algorithm(s) to be used for a given association.

The default ~~privacy~~confidentiality state for all IEEE 802.11 STAs is "in the clear." If the ~~privacy~~confidentiality service is not invoked, all messages shall be sent ~~unencrypted~~unprotected. If this ~~default~~ policy is ~~not~~ unacceptable to ~~one party or the other, data frames shall not be successfully communicated between the LLC entities.~~ the sender, it shall not send data frames; and if the policy is unacceptable to the receiver, it shall discard any received data frames. ~~Unencrypted~~ Unprotected data frames received at a station configured for mandatory ~~privacy~~confidentiality, as well as protected~~encrypted~~ data frames using a key not available at the receiving station, are discarded without an indication to logical link control (LLC) (or without indication to distribution services in the case of "To DS" frames received at an AP). These frames are acknowledged on the WM [if received without frame check sequence (FCS) error] to avoid wasting WM bandwidth on retries.

After 5.4.3.3, insert 5.4.3.4 through 5.4.3.6:

5.4.3.4 Key management

The enhanced confidentiality, data authentication, and replay protection mechanisms require fresh cryptographic keys. The procedures defined in this amendment provide fresh keys by means of protocols called the 4-Way Handshake and Group Key Handshake.

5.4.3.5 Data origin authenticity

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

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

5.4.3.6 Replay detection

The replay detection mechanism defines a means by which a STA that receives a data frame from another STA can detect whether the data frame is an unauthorized retransmission. This mechanism is provided for STAs that use CCMP or TKIP.

5.6 Differences between ESS and IBSS LANs

Insert the following paragraph at the end of 5.6:

In an IBSS, each STA must enforce its own security policy. In an ESS, an AP can enforce a uniform security policy across all STAs.

[8]Details of the RC4 algorithm are available from RSA Security, Inc. Contact RSA for algorithm details and the uniform RC4 license terms that RSA offers to anyone wishing to use RC4 for the purpose of implementing the IEEE 802.11 WEP option. If necessary, contact the IEEE Standards Department Intellectual Property Rights Administrator for details on how to communicate with RSA.

Copyright © 2004 IEEE. All rights reserved.
Documents Document Sharing Hub
Full document details: ISO_IEC 8802-11_2005_AMD6_2006

5.7 Message information contents that support the services

Change the title and text of 5.7.5 as follows:

5.7.5 ~~Privacy~~Confidentiality

For a STA to invoke a ~~the WEP privacy~~ confidentiality algorithm (as controlled by MLME-SETKEYS, see Clause 10, or the related MIB attributes, see Clause 11), the ~~privacy~~ confidentiality service ~~causes MPDU encryption~~ selects the confidentiality algorithm and sets the ~~WEP frame header~~Protected Frame bit appropriately (see Clause 7).

5.7.6 Authentication

Change the first paragraph in 5.7.6 as follows:

For a STA to authenticate with another STA using either Open System or Shared Key authentication, the authentication service causes one or more authentication management frames to be exchanged. The exact sequence of frames and their content are dependent on the authentication scheme invoked. For ~~all~~both of these authentication schemes, the authentication algorithm is identified within the management frame body.

5.7.7 Deauthentication

Change the first paragraph in 5.7.7 as follows:

For a STA to invalidate an active authentication that was established using Open System or Shared Key authentication, the following message is sent:

5.8 Reference model

Replace Figure 11 with the following:

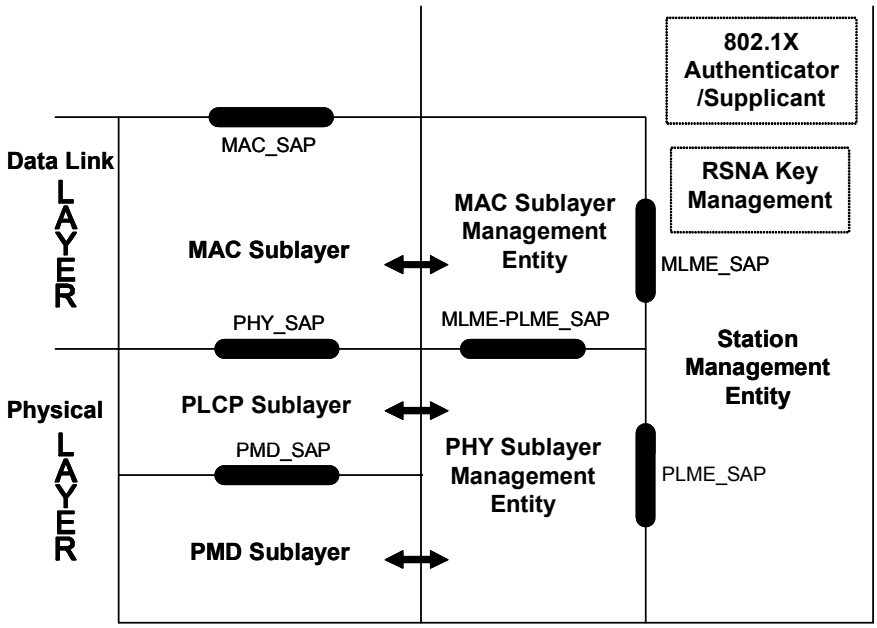

Figure 11—Portion of the ISO/IEC basic reference model covered in this standard

Copyright © 2004 IEEE. All rights reserved.

Documents Document Sharing Hub
Full document details: ISO_IEC 8802-11_2005_AMD6_2006

Insert the following paragraph at the end of 5.8:

There is an interface between the IEEE 802.1X Supplicant/Authenticator and the SME shown in Figure 11. This interface is described in IEEE P802.1X-REV.

After 5.8, insert 5.9 through 5.9.5 and renumber the figures as necessary:

5.9 IEEE 802.11 and IEEE 802.1X

An RSNA relies on IEEE 802.1X to provide authentication services and uses the IEEE 802.11 key management scheme defined in 8.5. The IEEE 802.1X access control mechanisms apply to the association between a STA and an AP and to the relationship between the IBSS STA and STA peer. The AP's SME performs the Authenticator and, optionally, the Supplicant and AS roles. In an ESS, a non-AP STA's SME performs the Supplicant role. In an IBSS, a STA's SME takes on both the Supplicant and Authenticator roles and may take on the AS role.

5.9.1 IEEE 802.11 usage of IEEE 802.1X

IEEE 802.11 depends upon IEEE 802.1X to control the flow of MAC service data units (MSDUs) between the DS and STAs by use of the IEEE 802.1X Controlled/Uncontrolled Port model. IEEE 802.1X authentication frames are transmitted in IEEE 802.11 data frames and passed via the IEEE 802.1X Uncontrolled Port. The IEEE 802.1X Controlled Port is blocked from passing general data traffic between two STAs until an IEEE 802.1X authentication procedure completes successfully over the IEEE 802.1X Uncontrolled Port. It is the responsibility of both the Supplicant and the Authenticator to implement port blocking. Each association between a pair of STAs creates a unique pair of IEEE 802.1X Ports, and authentication takes place relative to those ports alone.

IEEE 802.11 depends upon IEEE 802.1X and the 4-Way Handshake and Group Key Handshake, described in Clause 8, to establish and change cryptographic keys. Keys are established after authentication has completed. Keys may change for a variety of reasons, including expiration of an IEEE 802.1X authentication timer, key compromise, danger of compromise, or policy.

5.9.2 Infrastructure functional model overview

This subclause summarizes the system setup and operation of an RSN, in two cases: when an IEEE 802.1X AS is used and when a PSK is used. For an ESS, the AP includes an Authenticator, and each associated STA includes a Supplicant.

5.9.2.1 AKM operations with AS

The following AKM operations are carried out when an IEEE 802.1X AS is used:

a) Prior to any use of IEEE 802.1X, IEEE 802.11 assumes that the Authenticator and AS have established a secure channel. The security of the channel between the Authenticator and the AS is outside the scope of this amendment.

   Authentication credentials must be distributed to the Supplicant and AS prior to association.

b) A STA discovers the AP's security policy through passively monitoring Beacon frames or through active probing (shown in Figure 11a). If IEEE 802.1X authentication is used, the EAP authentication process starts when the AP's Authenticator sends the EAP-Request (shown in Figure 11b) or the STA's Supplicant sends the EAPOL-Start message. EAP authentication frames pass between the Supplicant and AS via the Authenticator and Supplicant's Uncontrolled Ports. This is shown in Figure 11b.

Copyright © 2004 IEEE. All rights reserved.
Documents Document Sharing Hub
Full document details: ISO_IEC 8802-11_2005_AMD6_2006

c) The Supplicant and AS authenticate each other and generate a PMK. The PMK is sent from the AS to the Authenticator over the secure channel. See Figure 11b.

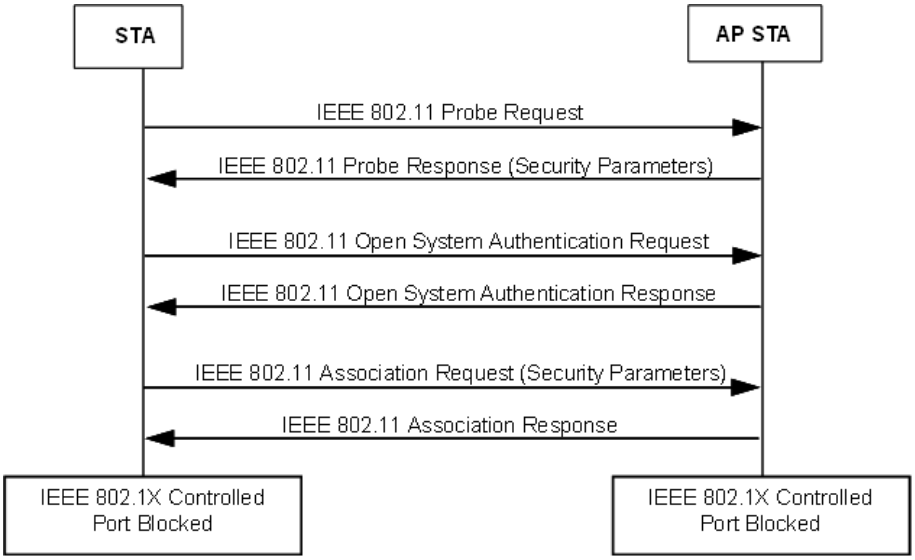

Figure 11a—Establishing the IEEE 802.11 association

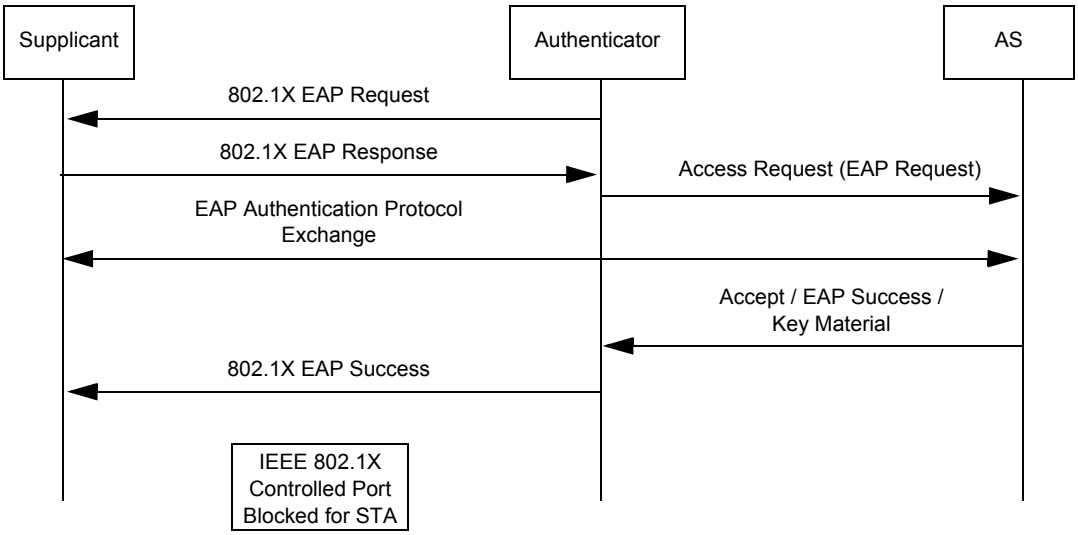

Figure 11b—IEEE 802.1X EAP authentication

A 4-Way Handshake utilizing EAPOL-Key frames is initiated by the Authenticator to do the following:

— Confirm that a live peer holds the PMK.

— Confirm that the PMK is current.

— Derive a fresh pairwise transient key (PTK) from the PMK.

Copyright © 2004 IEEE. All rights reserved.

Documents
Document Sharing Hub
Full document details: ISO_IEC 8802-11_2005_AMD6_2006

— Install the pairwise encryption and integrity keys into IEEE 802.11.
— Transport the group temporal key (GTK) and GTK sequence number from Authenticator to Supplicant and install the GTK and GTK sequence number in the STA and, if not already installed, in the AP.
— Confirm the cipher suite selection.

Upon successful completion of the 4-Way Handshake, the Authenticator and Supplicant have authenticated each other; and the IEEE 802.1X Controlled Ports are unblocked to permit general data traffic. See Figure 11c.

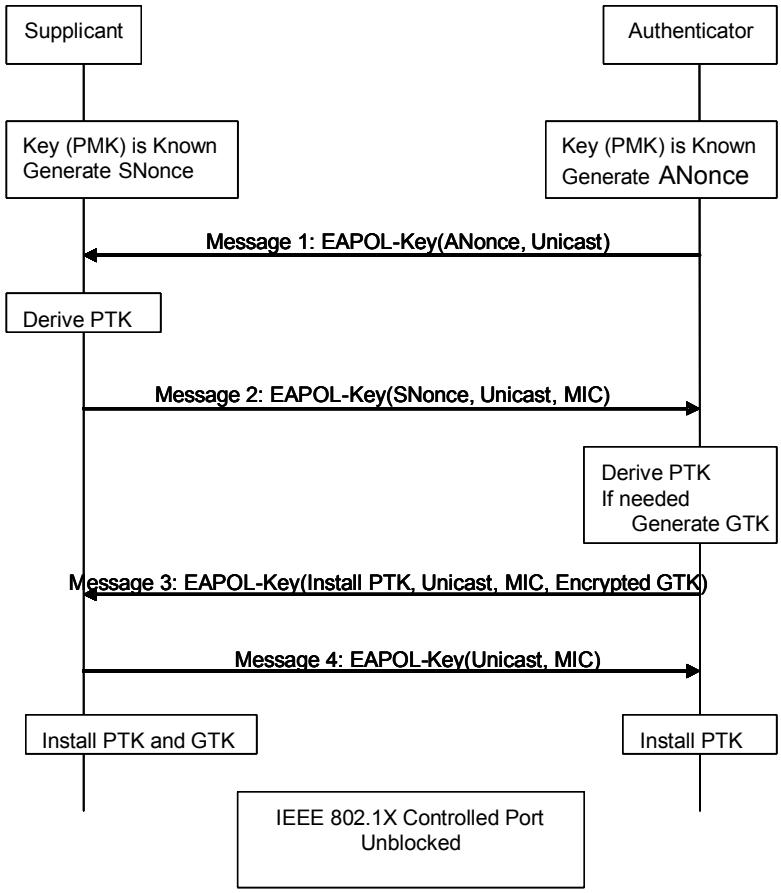

Figure 11c—Establishing pairwise and group keys

If the Authenticator later changes the GTK, it sends the new GTK and GTK sequence number to the Supplicant using the Group Key Handshake to allow the Supplicant to continue to receive broadcast/multicast messages and, optionally, to transmit and receive unicast frames. EAPOL-Key frames are used to carry out this exchange. See Figure 11d.

Copyright © 2004 IEEE. All rights reserved.
Documents
Document Sharing Hub
Full document details: ISO_IEC 8802-11_2005_AMD6_2006

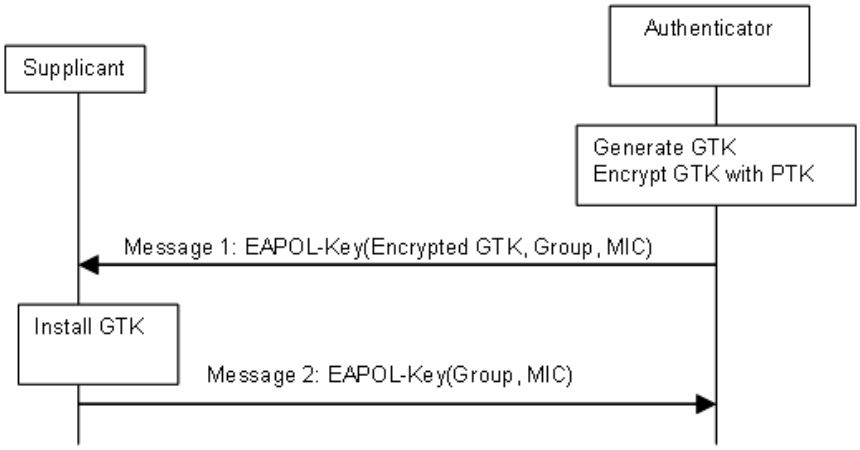

Figure 11d—Delivery of subsequent group keys

5.9.2.2 Operations with PSK

The following AKM operations are carried out when the PMK is a PSK:

— A STA discovers the AP's security policy through passively monitoring Beacon frames or through active probing (shown in Figure 11a). A STA associates with an AP and negotiates a security policy. The PMK is the PSK.

— The 4-Way Handshake using EAPOL-Key frames is used just as with IEEE 802.1X authentication, when an AS is present. See Figure 11c.

— The GTK and GTK sequence number are sent from the Authenticator to the Supplicant just as in the AS case. See Figure 11c and Figure 11d.

5.9.3 IBSS functional model description

This subclause summarizes the system setup and operation of an RSNA in an IBSS. An IBSS RSNA is specified in 8.4.7.

5.9.3.1 Key usage

In an IBSS, the unicast data frames between two STAs are protected with a pairwise key. The key is part of the PTK, which is derived during a 4-Way Handshake.

In an IBSS, the broadcast/multicast data frames are protected by a key, e.g., named B1, that is generated by the STA transmitting the broadcast/multicast frame. To allow other STAs to decrypt broadcast/multicast frames, B1 must be sent to all the other STAs in the IBSS. B1 is sent in an EAPOL-Key frame, encrypted under the EAPOL-Key encryption key (KEK) portion of the PTK, and protected from modification by the EAPOL-Key confirmation key (KCK) portion of the PTK.

In an IBSS, a STA's SME responds to Deauthentication frames from a STA by deleting the PTKSA associated with that STA.

5.9.3.2 Sample IBSS 4-Way Handshakes

In this example (see Figure 11e), there are three STAs: S1, S2, S3. The broadcast/multicast frames sent by S1 are protected by B1; similarly B2 for S2, and B3 for S3.

Copyright © 2004 IEEE. All rights reserved.

Documents
Document Sharing Hub
Full document details: ISO_IEC 8802-11_2005_AMD6_2006

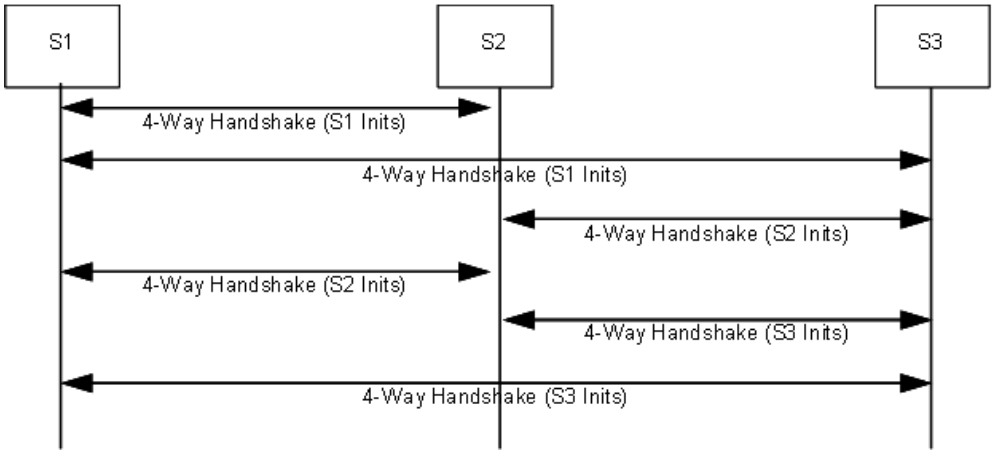

Figure 11e—Sample 4-Way Handshakes in an IBSS

For stations S2 and S3 to decrypt broadcast/multicast frames from S1, B1 must be sent to S2 and S3. This is done using the 4-Way Handshake initially and using the Group Key Handshake for GTK updates.

The 4-Way Handshake from S1 to S2 allows S1 to send broadcast/multicast frames to S2, but does not allow S2 to send broadcast/multicast frames to S1 because S2 has a different transmit GTK. Therefore, S2 needs to initiate a 4-Way Handshake to S1 to allow S1 to decrypt S2's broadcast/multicast frames. Similarly, S2 also needs to initiate a 4-Way Handshake to S3 to enable S3 to receive broadcast/multicast messages from S2.

In a similar manner S3 needs to complete the 4-Way Handshake with S1 and S2 to deliver B3 to S1 and S2.

In this example, there are six 4-Way Handshakes. In general, N STA Supplicants require $N(N-1)$ 4-Way Handshakes.

NOTE—In principle the KCK and KEK from a single 4-Way Handshake can be used for the Group Key Handshake in both directions, but using two 4-Way Handshakes means the Authenticator key state machine does not need to be different between IBSS and ESS.[9]

The Group Key Handshake can be used to send the GTKs to the correct STAs. The 4-Way Handshake is used to derive the pairwise key and to send the initial GTK. Because in an IBSS there are two 4-Way Handshakes between any two STA Supplicants and Authenticators, the pairwise key used between any two STAs is from the 4-Way Handshake initiated by the STA Authenticator with the higher MAC address (see 8.5.1 for the notion of address comparison). The KCK and KEK used for a Group Key Handshake are the KCK and KEK derived by the 4-Way Handshake initiated by the same Authenticator that is initiating the Group Key Handshake.

In an IBSS, a secure link exists between two stations when both 4-Way Handshakes have completed successfully. The Supplicant and Authenticator 4-Way Handshake state machines interact so the IEEE 802.1X variable portValid is not set until both 4-Way Handshakes complete.

If a fourth STA comes within range and its SME decides to initiate a security association with the three peers, its Authenticator initiates 4-Way Handshakes with each of the other three STA Supplicants. Similarly, the original three STA Authenticators in the IBSS need to initiate 4-Way Handshakes to the fourth STA

[9]Notes in text, tables, and figures are given for information only and do not contain requirements needed to implement this amendment.

Copyright © 2004 IEEE. All rights reserved.
Documents
Document Sharing Hub
Full document details: ISO_IEC 8802-11_2005_AMD6_2006

Supplicant. A STA learns that a peer STA is RSNA-enabled and the peer's security policy (e.g., whether the Authentication and Key Management Protocol (AKMP) is PSK or IEEE 802.1X authentication) from the Beacon or Probe Response frame. The initiation may start for a number of reasons:

a) The fourth STA receives a Beacon or Probe Response frame from a MAC address with which it has not completed a 4-Way Handshake.

b) A STA's SME receives a MLME-PROTECTEDFRAMEDROPPED.indication primitive from a MAC address with which it has not completed a 4-Way Handshake. This could be a multicast/broadcast data frame transmitted by any of the STAs. If the SME wants to set up a security association to the peer STA, but does not know the security policy of the peer, it should send a Probe Request frame to the peer STA to find its security policy before setting up a security association to the peer STA.

c) A STA's SME receives Message 1 of the 4-Way Handshake sent to a STA because the initiator received a broadcast data frame, Beacon frame, or Probe Response frame from that STA. If a STA received a 4-Way Handshake, wants to set up a security association to the peer STA, but does not know the security policy of the peer, it should send a Probe Request frame to the peer STA to find its security policy before setting up a security association to the peer STA.

5.9.3.3 IBSS IEEE 802.1X Example

When IEEE 802.1X authentication is used, each STA will need to include an IEEE 802.1X Authenticator and AS. A STA learns that a peer STA is RSNA-enabled and the peer's security policy (e.g., whether the AKMP is PSK or IEEE 802.1X authentication) from the Beacon or Probe Response frame.

Each STA's Supplicant will send an EAPOL-Start message to every other station to which it wants to authenticate, and each STA's Authenticator will respond with the identity of the credential it wants to use.

The EAPOL-Start and EAP-Request/Identity messages are initiated when a protected data frame (indicated via a MLME-PROTECTEDFRAMEDROPPED.indication primitive), an IEEE 802.1X message, Beacon frame, or Probe Response frame is received from a MAC address with which the STA has not completed IEEE 802.1X authentication. If the SME wants to set up a security association to the peer STA, but does not know the security policy of the peer, it should send a Probe Request frame to the peer STA to find its security policy before setting up a security association to the peer STA.

Although Figure 11f shows the two IEEE 802.1X exchanges serialized, they may occur interleaved.

5.9.4 Authenticator-to-AS protocol

The Authenticator-to-AS authentication definition is out of the scope of this amendment, but, to provide security assurances, the protocol must support the following functions:

a) Mutual authentication between the Authenticator and AS

b) A channel for the Supplicant/AS authentication

c) The ability to pass the generated key from the AS to the Authenticator in a manner that provides authentication of the key source, ensures integrity of the key transfer, and preserves confidentiality of the key from all other parties

Suitable protocols include, but are not limited to, remote authentication dial-in user service (RADIUS) (IETF RFC 2865 [B14]) and Diameter (IETF RFC 3588 [B15]).

Copyright © 2004 IEEE. All rights reserved.

Documents Document Sharing Hub

Full document details: ISO_IEC 8802-11_2005_AMD6_2006

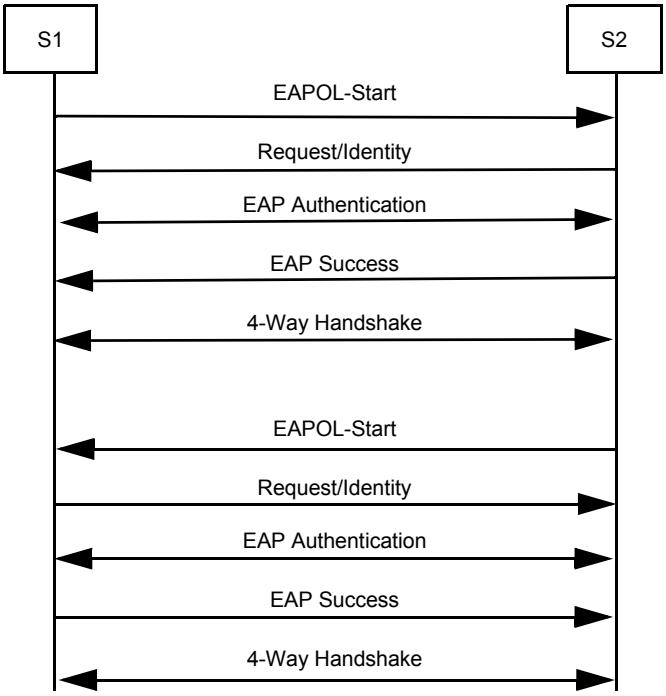

Figure 11f—Example using IEEE 802.1X authentication

5.9.5 PMKSA caching

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

The STA may supply a list of PMK or PSK key identifiers in the (Re)Association Request frame. Each key identifier names a PMKSA; the PMKSA may contain a single PMK. The Authenticator specifies the selected PMK or PSK key identifier in Message 1 of the 4-Way Handshake. The selection of the key identifiers to be included within the (Re)Association Request frame and Message 1 of the 4-Way Handshake is out of the scope of this amendment.

End of changes to Clause 5.

6. MAC service definition

6.1 Overview of MAC services

6.1.2 Security services

Change the text of 6.1.2 as follows:

Security services in IEEE 802.11 are provided by the authentication service and the WEP, TKIP, and CCMP mechanisms. The scope of the security services provided is limited to station-to-station data exchange. The ~~privacy~~ confidentiality service offered by an IEEE 802.11 WEP, TKIP, and CCMP implementation is the encryption of the MSDU. For the purposes of this standard, WEP, TKIP, and CCMP are ~~is~~ viewed as ~~a~~

Copyright © 2004 IEEE. All rights reserved.
Documents
Document Sharing Hub
Full document details: ISO_IEC 8802-11_2005_AMD6_2006

logical services located within the MAC sublayer as shown in the reference model, Figure 11. Actual implementations of the WEP, TKIP, and CCMP services are transparent to the LLC and other layers above the MAC sublayer.

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

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

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

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

After 6.1.3, insert 6.1.4 and renumber the figures as necessary:

6.1.4 MAC data service architecture

The MAC data plane architecture (i.e., processes that involve transport of all or part of an MSDU) is shown in Figure 11g. During transmission, an MSDU goes through some or all of the following processes: frame delivery deferral during power save mode, sequence number assignment, fragmentation, encryption, integrity protection, and frame formatting. IEEE 802.1X may block the MSDU at the Controlled Port.

During reception, a received data frame goes through processes of MPDU header + cyclic redundancy code (CRC) validation, duplicate removal, decryption, defragmentation, integrity checking, and replay detection. The IEEE 802.1X Controlled/Uncontrolled Ports discard the MSDU if the Controlled Port is not enabled or if the MSDU does not represent an IEEE 802.1X frame. TKIP and CCMP MPDU frame order enforcement occurs after decryption, but prior to MSDU defragmentation; therefore, defragmentation will fail if MPDUs arrive out of order.

Copyright © 2004 IEEE. All rights reserved.

Documents Document Sharing Hub
Full document details: ISO_IEC 8802-11_2005_AMD6_2006

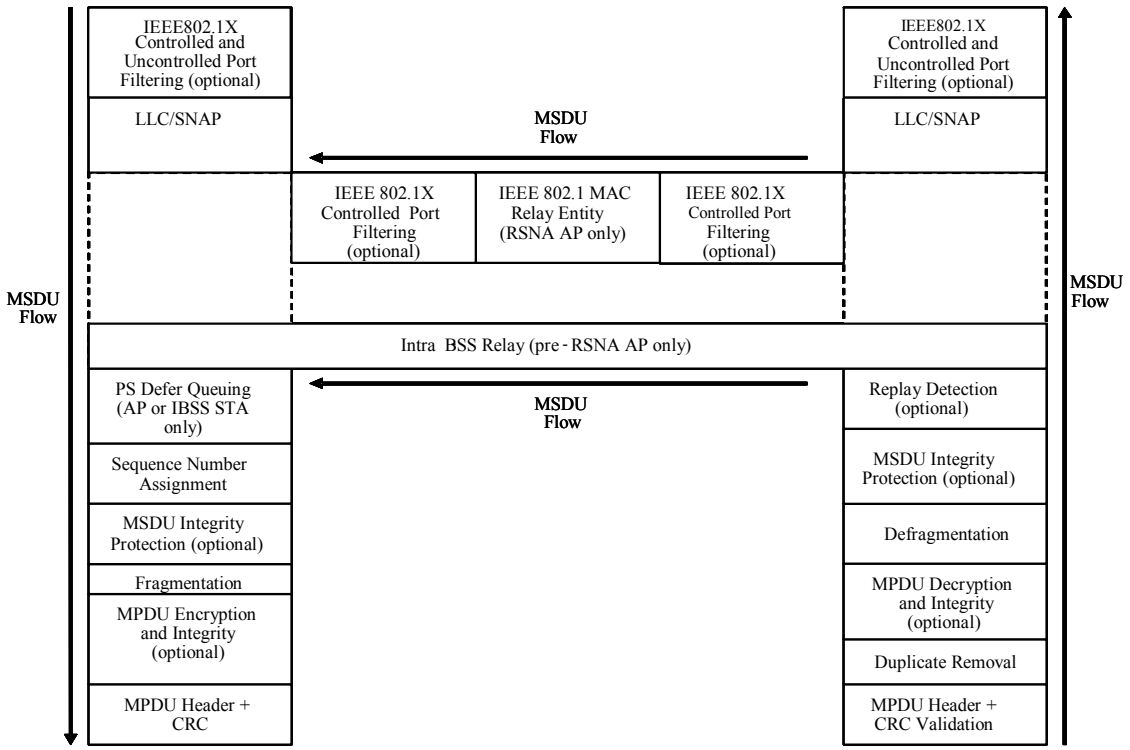

Figure 11g—MAC data plane architecture

End of changes to Clause 6.

7. Frame formats

7.1 MAC frame formats

7.1.3 Frame fields

7.1.3.1 Frame Control field

Change the text of 7.1.3.1 as follows:

The Frame Control field consists of the following subfields: Protocol Version, Type, Subtype, To DS, From DS, More Fragments, Retry, Power Management, More Data, ~~Wired Equivalent Privacy (WEP)~~ Protected Frame, and Order. The format of the Frame Control field is illustrated in Figure 13.

Copyright © 2004 IEEE. All rights reserved.
Documents Document Sharing Hub
Full document details: ISO_IEC 8802-11_2005_AMD6_2006

Change Figure 13 as shown:

B0 B1	B2 B3	B4 B7	B8	B9	B10	B11	B11	B13	B14	B15
Protocol Version	Type	Subtype	To DS	From DS	More Frag	Retry	Pwr Mgt	More Data	~~WEP~~ Protected Frame	Order
Bits : 2	2	4	1	1	1	1	1	1	1	1

Figure 13—Frame Control field

Change the title and text of 7.1.3.1.9 as follows:

7.1.3.1.9 ~~WEP~~Protected Frame field

The ~~WEP~~ Protected Frame field is 1 bit in length. ~~It~~ The Protected Frame field is set to 1 if the Frame Body field contains information that has been processed by ~~the WEP~~ a cryptographic encapsulation algorithm. The ~~WEP~~ Protected Frame field is set to 1 only within data frames ~~of type Data~~ and within management frames of ~~type Management,~~ subtype Authentication. The ~~WEP~~ Protected Frame field is set to 0 in all other frames. When the ~~WEP bit~~ Protected Frame field is set to 1~~, the Frame Body field is expanded as defined in 8.2.5~~ in a data frame, the Frame Body field is protected utilizing the cryptographic encapsulation algorithm and expanded as defined in Clause 8. Only WEP is allowed as the cryptographic encapsulation algorithm for management frames of subtype Authentication.

7.2 Format of individual frame types

7.2.2 Data frames

Change the first paragraph after the lettered list in 7.2.2 as follows:

The frame body consists of the MSDU or a fragment thereof, and a ~~WEP IV and ICV~~ security header and trailer (if and only if the ~~WEP~~ Protected Frame subfield in the Frame Control field is set to 1). The frame body is null (0 octets in length) in data frames of subtypes Null Function (no data), CF-Ack (no data), CF-Poll (no data), and CF-Ack+CF-Poll (no data).

7.2.3 Management frames

7.2.3.1 Beacon frame format

Insert the order 21 information field in Table 5:

Table 5—Beacon frame body

21	RSN	The RSN information element is only present within Beacon frames generated by STAs that have `dot11RSNAEnabled` set to TRUE.

Copyright © 2004 IEEE. All rights reserved.

AVA Documents Document Sharing Hub
Full document details: ISO_IEC 8802-11_2005_AMD6_2006

7.2.3.4 Association Request frame format

Insert the order 8 information field in Table 7:

Table 7—Association Request frame body

8	RSN	The RSN information element is only present within Association Request frames generated by STAs that have `dot11RSNAEnabled` set to TRUE.

7.2.3.6 Reassociation Request frame format

Insert the order 9 information field to Table 9:

Table 9—Reassociation Request frame body

9	RSN	The RSN information element is only present within Reassociation Request frames generated by STAs that have `dot11RSNAEnabled` set to TRUE.

7.2.3.9 Probe Response frame format

Insert the order 21 and 22–n information fields in Table 12:

Table 12—Probe Response frame body

21	RSN	The RSN information element is only present within Probe Response frames generated by STAs that have `dot11RSNAEnabled` set to TRUE.
22–*n*	Requested information elements	Elements requested by the Request information element of the Probe Request frame.

7.2.3.10 Authentication frame format

Insert the following text after the first sentence of 7.2.3.10:

Only Authentication frames with the authentication algorithm set to Open System authentication may be used within an RSNA. RSNA STAs shall not associate if shared authentication was invoked prior to RSN association.

Copyright © 2004 IEEE. All rights reserved.
Documents
Document Sharing Hub
Full document details: ISO_IEC 8802-11_2005_AMD6_2006

7.3 Management frame body components

7.3.1 Fixed fields

7.3.1.4 Capability Information field

Change the sixth and seventh paragraphs in 7.3.1.4 as follows:

APs set the Privacy subfield to 1 within transmitted Beacon, Probe Response, Association Response, and Reassociation Response management frames if ~~WEP encryption~~ data confidentiality is required for all data type frames exchanged within the BSS. If ~~WEP encryption~~ data confidentiality is not required, ~~APs set~~ the Privacy subfield is set to 0 ~~within these management frames~~.

In an RSNA, non-AP STAs in an ESS set the Privacy subfield to 0 within transmitted Association and Reassociation Request management frames. APs ignore the Privacy subfield within received Association and Reassociation Request management frames.

STAs within an IBSS set the Privacy subfield to 1 in transmitted Beacon or Probe Response management frames if ~~WEP encryption~~ data confidentiality is required for all data type frames exchanged within the IBSS. If ~~WEP encryption~~ data confidentiality is not required, STAs in an IBSS set the Privacy subfield ~~is set~~ to 0 within these management frames.

STAs that include the RSN information element in Beacon and Probe Response frames shall set the Privacy subfield to 1 in any frame that includes the RSN information element.

7.3.1.7 Reason Code field

Insert reason codes 12 through 24 and change the final Reserved reason code row in Table 18 as follows:

Table 18—Reason codes

Reason code	Meaning
12	Reserved
13	Invalid information element
14	MIC failure
15	4-Way Handshake timeout
16	Group Key Handshake timeout
17	Information element in 4-Way Handshake different from (Re)Association Request/Probe Response/Beacon frame
18	Invalid group cipher
19	Invalid pairwise cipher
20	Invalid AKMP
21	Unsupported RSN information element version
22	Invalid RSN information element capabilities
23	IEEE 802.1X authentication failed

Copyright © 2004 IEEE. All rights reserved.

Documents Document Sharing Hub
Full document details: ISO_IEC 8802-11_2005_AMD6_2006

Table 18—Reason codes *(continued)*

Reason code	Meaning
24	Cipher suite rejected per security policy
25–65 535	Reserved

7.3.1.9 Status Code field

Insert reason codes 27 through 46 and change the final Reserved reason code row in Table 19 as follows:

Table 19—Status codes

Status code	Meaning
27–39	Reserved
40	Invalid information element
41	Invalid group cipher
42	Invalid pairwise cipher
43	Invalid AKMP
44	Unsupported RSN information element version
45	Invalid RSN information element capabilities
46	Cipher suite rejected per security policy
47–65 535	Reserved

7.3.2 Information elements

Replace element identifiers (IDs) 43 through 49 in Table 20 as follows:

Table 20—Element IDs

Information element	Element ID
Reserved	43–47
RSN	48
Reserved	49

Copyright © 2004 IEEE. All rights reserved.
Documents
Document Sharing Hub
Full document details: ISO_IEC 8802-11_2005_AMD6_2006

After 7.3.2.24, insert 7.3.2.25 through 7.3.2.25.5 and renumber tables and figures as necessary:

7.3.2.25 RSN information element

The RSN information element contains authentication and pairwise cipher suite selectors, a single group cipher suite selector, an RSN Capabilities field, the PMK identifier (PMKID) count, and PMKID list. See Figure 46ta. All STAs implementing RSNA shall support this element. The size of the RSN information element is limited by the size of an information element, which is 255 octets. Therefore, the number of pairwise cipher suites, AKM suites, and PMKIDs is limited.

Element ID 1 octet	Length 1 octet	Version 2 octets	Group Cipher Suite 4 octets	Pairwise Cipher Suite 2 octets	Pairwise Cipher Suite List 4-*m* octets	AKM Suite Count 2 octets	AKM Suite List 4-*n* octets	RSN Capabilities 2 octets	PMKID Count 2 octets	PMKID List 16-*s* octets

Figure 46ta—RSN information element format

In Figure 46ta, *m* denotes the pairwise cipher suite count, *n* the AKM suite count, and *s* is the PMKID count.

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

Element ID shall be 48 decimal (30 hex).

Length gives the number of octets in the information field (field(s) following the Element ID and Length fields) of the information element.

The Version field indicates the version number of the RSNA protocol. The range of Version field values a STA supports shall be contiguous. Values 0 and 2 or higher of the Version field are reserved. RSN Version 1 is defined in this amendment.

NOTE—The following represent sample information elements:

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

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

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

```
30, // information element id, 48 expressed as Hex value
14, // length in octets, 20 expressed as Hex value
01 00, // Version 1
00 0F AC 04, // CCMP as group cipher suite
01 00, // pairwise cipher suite count
00 0F AC 04, // CCMP as pairwise cipher suite
01 00, // authentication count
00 0F AC 01 // 802.1X authentication
01 00 // Preauthentication capabilities
```

Copyright © 2004 IEEE. All rights reserved.

Documents Document Sharing Hub
Full document details: ISO_IEC 8802-11_2005_AMD6_2006

802.1X authentication, Use GTK for pairwise cipher suite, WEP-40 group cipher suites, optional RSN Capabilities field omitted:

30, // information element id, 48 expressed as Hex value
12, // length in octets, 18 expressed as Hex value
01 00, // Version 1
00 0F AC 01, // WEP-40 as group cipher suite
01 00, // pairwise cipher suite count
00 0F AC 00, // Use group key as pairwise cipher suite
01 00, // authentication count
00 0F AC 01 // 802.1X authentication

802.1X authentication, Use CCMP for pairwise cipher suite, CCMP group cipher suites, preauthentication and a PMKID.

30, // information element id, 48 expressed as Hex value
26 // length in octets, 38 expressed as Hex value
01 00, // Version 1
00 0F AC 04, // CCMP as group cipher suite
01 00, // pairwise cipher suite count
00 0F AC 04, // CCMP as pairwise cipher suite
01 00, // authentication count
00 0F AC 01 // 802.1X authentication
01 00 // Preauthentication capabilities
01 00 // PMKID Count
01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 10 // PMKID

7.3.2.25.1 Cipher suites

The Group Cipher Suite field contains the cipher suite selector used by the BSS to protect broadcast/multicast traffic.

The Pairwise Cipher Suite Count field indicates the number of pairwise cipher suite selectors that are contained in the Pairwise Cipher Suite List field.

The Pairwise Cipher Suite List field contains a series of cipher suite selectors that indicate the pairwise cipher suites contained in the RSN information element.

A suite selector has the format shown in Figure 46tb.

OUI 3 octets	Suite Type 1 octet

Figure 46tb—Suite selector format

The order of the organizationally unique indentifier (OUI) field shall follow the ordering convention for MAC addresses from 7.1.1.

Table 20da provides the cipher suite selectors defined by this amendment.

Table 20da—Cipher suite selectors

OUI	Suite type	Meaning
00-0F-AC	0	Use group cipher suite
00-0F-AC	1	WEP-40

Copyright © 2004 IEEE. All rights reserved.
Documents
Document Sharing Hub
Full document details: ISO_IEC 8802-11_2005_AMD6_2006

Table 20da—Cipher suite selectors *(continued)*

OUI	Suite type	Meaning
00-0F-AC	2	TKIP
00-0F-AC	3	Reserved
00-0F-AC	4	CCMP – default in an RSNA
00-0F-AC	5	WEP-104
00-0F-AC	6–255	Reserved
Vendor OUI	Other	Vendor specific
Other	Any	Reserved

The cipher suite selector 00-0F-AC:4 (CCMP) shall be the default cipher suite value.

The cipher suite selectors 00-0F-AC:1 (WEP-40) and 00-0F-AC:5 (WEP-104) are only valid as a group cipher suite in a transition security network (TSN) to allow pre-RSNA devices to join the BSS.

Use of CCMP as the group cipher suite with TKIP as the pairwise cipher suite shall not be supported.

NOTE—If the STAs can support CCMP, then there is no need for a weaker data confidentiality protocol.

The cipher suite selector 00-0F-AC:0 (Use group cipher suite) is only valid as the pairwise cipher suite. An AP may specify the selector 00-0F-AC:0 (Use group cipher suite) for a pairwise cipher suite if it does not support any pairwise cipher suites. If an AP specifies 00-0F-AC:0 (Use group cipher suite) as the pairwise cipher selection, this shall be the only pairwise cipher selection the AP advertises.

If CCMP is enabled, then the AP supports pairwise keys, and thus the suite selector 00-0F-AC:0 (Use group cipher suite) shall not be a valid option.

Table 20db indicates the circumstances under which each cipher suite shall be used.

Table 20db—Cipher suite usage

Cipher suite selector	GTK	PTK
Use group key	No	Yes
WEP-40	Yes	No
WEP-104	Yes	No
TKIP	Yes	Yes
CCMP	Yes	Yes

7.3.2.25.2 AKM suites

The AKM Suite Count field indicates the number of AKM suite selectors that are contained in the AKM Suite List field.

Copyright © 2004 IEEE. All rights reserved.

Documents Document Sharing Hub
Full document details: ISO_IEC 8802-11_2005_AMD6_2006

The AKM Suite List field contains a series of AKM suite selectors contained in the RSN information element. In an IBSS, only a single AKM suite selector may be specified because STAs in an IBSS must use the same AKM suite and because there is no mechanism to negotiate the AKMP in an IBSS (see 8.4.4).

Each AKM suite selector specifies an AKMP. Table 20dc gives the AKM suite selectors defined by this amendment.

Table 20dc—AKM suite selectors

OUI	Suite type	Meaning	
		Authentication type	Key management type
00-0F-AC	0	Reserved	Reserved
00-0F-AC	1	Authentication negotiated over IEEE 802.1X or using PMKSA caching as defined in 8.4.6.2 – RSNA default	RSNA key management as defined in 8.5 or using PMKSA caching as defined in 8.4.6.2 – RSNA default
00-0F-AC	2	PSK	RSNA key management as defined in 8.5, using PSK
00-0F-AC	3–255	Reserved	Reserved
Vendor OUI	Any	Vendor specific	Vendor specific
Other	Any	Reserved	Reserved

The AKM suite selector value 00-0F-AC:1 (Authentication negotiated over IEEE 802.1X) with (RSNA key management as defined in 8.5 or using PMKSA caching as defined in 8.4.6.2) shall be the assumed default when the AKM suite selector field is not supplied.

NOTE—The selector value 00-0F-AC:1 specifies only that IEEE 802.1X is used as the authentication transport. IEEE 802.1X selects the authentication mechanism.

The AKM suite selector value 00-0F-AC:2 (PSK) is used when a PSK is used with RSNA key management.

NOTE—Selector values 00-0F-AC:1 and 00-0F-AC:2 can simultaneously be enabled by an Authenticator.

7.3.2.25.3 RSN capabilities

The RSN Capabilities field indicates requested or advertised capabilities. The value of each of the RSN Capabilities fields shall be taken to be 0 if the RSN Capabilities field is not available in the RSN information element.

The length of the RSN Capabilities field is 2 octets. The format of the RSN Capabilities field is as illustrated in Figure 46tc and described after the figure.

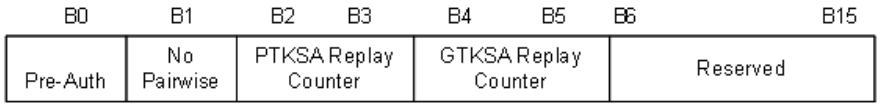

Figure 46tc—RSN Capabilities field format

Copyright © 2004 IEEE. All rights reserved.
Documents Document Sharing Hub
Full document details: ISO_IEC 8802-11_2005_AMD6_2006

— Bit 0: Pre-Authentication. An AP sets the Pre-Authentication subfield of the RSN Capabilities field to 1 to signal it supports preauthentication (see 8.4.6.1) and sets the subfield to 0 when it does not support preauthentication. A non-AP STA sets the Pre-Authentication subfield to 0.

— Bit 1: No Pairwise. If a STA can support WEP default key 0 simultaneously with a pairwise key (see 8.5.1), then the STA sets the No Pairwise subfield of the RSN Capabilities field to 0.

If a STA cannot support WEP default key 0 simultaneously with a pairwise key (see 8.5.1), then the STA sets the No Pairwise subfield of the RSN Capabilities field to 1.

The No Pairwise subfield describes a capability of a non-AP STA. STAs in an IBSS and APs set the No Pairwise subfield to 0.

The No Pairwise subfield shall be set only in a TSN and when the pairwise cipher suite selected by the STA is TKIP.

— Bits 2–3: PTKSA Replay Counter. A STA sets the PTKSA Replay Counter subfield of the RSN Capabilities field to the value contained in `dot11RSNAConfigNumberofPTKSAReplay-Counters`. The least significant bit (LSB) of `dot11RSNAConfigNumberofPTKSA-ReplayCounters` is put in bit 2. See 8.3.2.6 and 8.3.3.4.3. The meaning of the value in the PTKSA/GTKSA/STAKeySA Replay Counter subfield is defined in Table 20dd. The number of replay counters per STAKeySA is the same as the number of replay counters per PTKSA or GTKSA.

Table 20dd—PTKSA/GTKSA/STAKeySA replay counters usage

Replay counter value	Meaning
0	1 replay counter per PTKSA/GTKSA/STAKeySA
1	2 replay counters per PTKSA/GTKSA/STAKeySA
2	4 replay counters per PTKSA/GTKSA/STAKeySA
3	16 replay counters per PTKSA/GTKSA/STAKeySA

— Bits 4–5: GTKSA Replay Counter. A STA sets the GTKSA Replay Counter subfield of the RSN Capabilities field to the value contained in `dot11RSNAConfigNumberofGTKSAReplay-Counters`. The LSB of `dot11RSNAConfigNumberofGTKSAReplayCounters` is put in bit 4. See 8.3.2.6 and 8.3.3.4.3. The meaning of the value in the GTKSA Replay Counter subfield is defined in Table 20dd.

— Bits 6–15: Reserved. The remaining subfields of the RSN Capabilities field are reserved and shall be set to 0 on transmission and ignored on reception.

7.3.2.25.4 PMKID

The PMKID Count and List fields shall be used only in the RSN information element in the (Re)Association Request frame to an AP. The PMKID Count specifies the number of PMKIDs in the PMKID List field. The PMKID list contains 0 or more PMKIDs that the STA believes to be valid for the destination AP. The PMKID can refer to

a) A cached PMKSA that has been obtained through preauthentication with the target AP

b) A cached PMKSA from an EAP authentication

c) A PMKSA derived from a PSK for the target AP

Copyright © 2004 IEEE. All rights reserved.

Documents Document Sharing Hub

Full document details: ISO_IEC 8802-11_2005_AMD6_2006

See 8.5.1.2 for the construction of the PMKID.

NOTE—A STA can choose not to insert a PMKID in the PMKID List field if the STA does not want to use that PMKSA.

End of changes to Clause 7.

Replace Clause 8 in its entirety with the following text:

8. Security

8.1 Framework

This amendment defines two classes of security algorithms for IEEE 802.11 networks:

— Algorithms for creating and using a RSNA, called *RSNA algorithms*

— Pre-RSNA algorithms

NOTE—This amendment does not prohibit STAs from simultaneously operating pre-RSNA and RSNA algorithms.

8.1.1 Security methods

Pre-RSNA security comprises the following algorithms:

— WEP, described in 8.2.1

— IEEE 802.11 entity authentication, described in 8.2.2

RSNA security comprises the following algorithms:

— TKIP, described in 8.3.2

— CCMP, described in 8.3.3

— RSNA establishment and termination procedures, including use of IEEE 802.1X authentication, described in 8.4

— Key management procedures, described in 8.5

8.1.2 RSNA equipment and RSNA capabilities

RSNA-capable equipment can create RSNAs. When `dot11RSNAEnabled` is true, RSNA-capable equipment shall include the RSN information element in Beacon, Probe Response, and (Re)Association Request frames and in Message 2 and Message 3 of the 4-Way Handshake. Pre-RSNA equipment is not capable of creating RSNAs.

8.1.3 RSNA establishment

A STA's SME establishes an RSNA in one of four ways:

a) When using IEEE 802.1X AKM in an ESS, an RSNA-capable STA's SME establishes an RSNA as follows:

   1) It identifies the AP as RSNA-capable from the AP's Beacon or Probe Response frames.

   2) It shall invoke Open System authentication.

   3) It negotiates cipher suites during the association process, as described in 8.4.2 and 8.4.3.

   4) It uses IEEE 802.1X to authenticate, as described in 8.4.6 and 8.4.7.

   5) It establishes temporal keys by executing a key management algorithm, using the protocol defined by 8.5.

Copyright © 2004 IEEE. All rights reserved.
Documents
Document Sharing Hub
Full document details: ISO_IEC 8802-11_2005_AMD6_2006