

802.11F™

IEEE Trial-Use Recommended Practice for Multi-Vendor Access Point Interoperability via an Inter-Access Point Protocol Across Distribution Systems Supporting IEEE 802.11™ Operation

IEEE Computer Society

Sponsored by the
LAN/MAN Standards Committee



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

14 July 2003

Print: SH95133
PDF: SS95133



Documents
Document Sharing Hub

IEEE Trial-Use Recommended Practice for Multi-Vendor Access Point Interoperability via an Inter-Access Point Protocol Across Distribution Systems Supporting IEEE 802.11™ Operation

Sponsor

LAN/MAN Standards Committee
of the
IEEE Computer Society

Approved 12 June 2003

IEEE-SA Standards Board

Abstract: Recommended practices for implementation of an Inter-Access Point Protocol (IAPP) on a Distribution System (DS) supporting ISO/IEC 8802-11:1999 and IEEE 802.11™ wireless local access network (WLAN) links are described. The recommended DS utilizes an IAPP that provides the necessary capabilities to achieve multi-vendor Access Point (AP) interoperability within the DS. This IAPP is described for a DS consisting of IEEE 802® LAN components utilizing an Internet Engineering Task Force (IETF) Internet Protocol (IP) environment. Throughout this recommended practice, the terms ISO/IEC 8802-11:1999, IEEE 802.11, 802.11™, and IEEE Std 802.11™-1999 are used interchangeably to refer to the same document, ISO/IEC 8802-11:1999, and its amendments and supplements published at the time this recommended practice was adopted.

Keywords: IAPP, Inter-Access Point Protocol, Internet Protocol, IP, IEEE 802.11, IEEE Std 802.11-1999, ISO/IEC 8802-11:1999

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

Copyright © 2003 by the Institute of Electrical and Electronics Engineers, Inc.
All rights reserved. Published 14 July 2003. 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 0-7381-3698-0 SH95133
PDF: ISBN 0-7381-3699-9 SS95133

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

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

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 08855-1331
USA

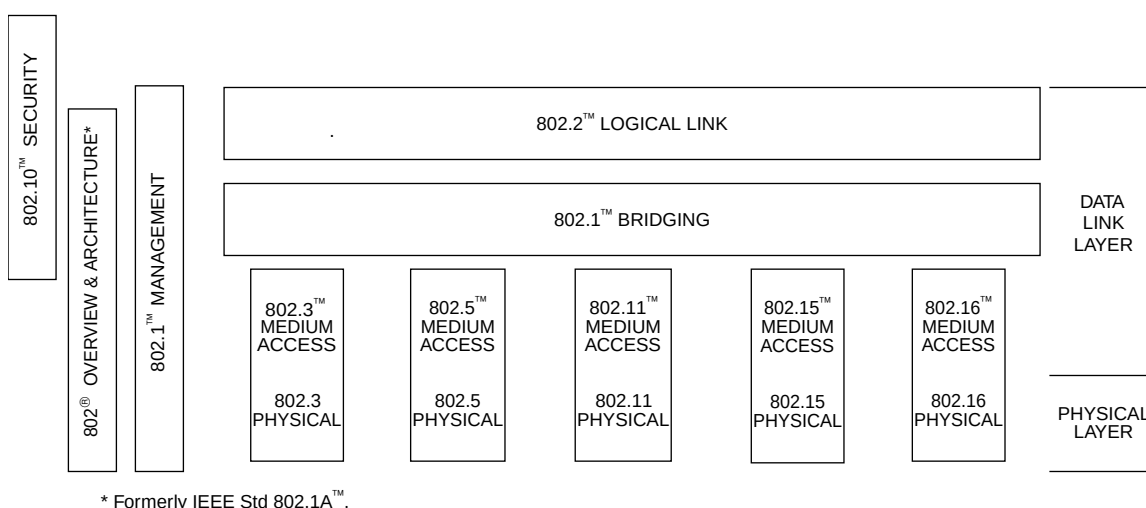
Note: Attention is called to the possibility that implementation of this standard may require use of subject matter covered by patent rights. By publication of this standard, no position is taken with respect to the existence or validity of any patent rights in connection therewith. The IEEE shall not 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. A patent holder 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 all applicants desiring to obtain such licenses. The IEEE makes no representation as to the reasonableness of rates and/or terms and conditions of the license agreements offered by patent holders. Further information may be obtained from the IEEE Standards Department.

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

Introduction

This introduction is not part of IEEE Std 802.11F-2003, IEEE Trial-Use Recommended Practice for Multi-Vendor Access Point Interoperability via an Inter-Access Point Protocol Across Distribution Systems Supporting IEEE 802.11™ Operation.

This recommended practice is part of a family of standards for local and metropolitan area networks. The relationship between the standard and other members of the family is shown below. (The numbers in the figure refer to IEEE standard designations.¹)



This family of standards deals with the Physical and Data Link layers as defined by the International Organization for Standardization (ISO) Open Systems Interconnection (OSI) Basic Reference Model (ISO/IEC 7498-1: 1994). The access standards define five types of medium access technologies and associated physical media, each appropriate for particular applications or system objectives. Some access standards have been withdrawn and other types are under investigation.

The standards defining the technologies noted above are as follows:

- IEEE Std 802:² *Overview and Architecture.* This standard provides an overview to the family of IEEE 802 Standards.
- IEEE Std 802.1B™ and 802.1k™ [ISO/IEC 15802-2] *LAN/MAN Management.* Defines an OSI management-compatible architecture and services and protocol elements for use in a LAN/MAN environment for performing remote management.
- IEEE Std 802.1D™ *Media Access Control (MAC) Bridges.* Specifies an architecture and protocol for the interconnection of IEEE 802 LANs below the MAC service boundary.

¹The IEEE standard designations referred to in the above figure and list are trademarks owned by the Institute of Electrical and Electronics Engineers, Incorporated.

²The IEEE 802 Overview and Architecture Specification, originally known as IEEE Std 802.1A, has been renumbered as IEEE Std 802. This has been done to accommodate recognition of the base standard in a family of standards. References to IEEE Std 802.1A should be considered as references to IEEE Std 802.

- IEEE Std 802.1E™
[ISO/IEC 15802-4] *System Load Protocol*. Specifies a set of services and protocol for those aspects those aspects of management concerned with the loading of systems on IEEE 802 LANs.
- IEEE Std 802.1F™ *Common Definitions and Procedures for IEEE 802 Management Information*.
- IEEE Std 802.1G™
[ISO/IEC 15802-5]: *Remote Media Access Control (MAC) Bridging*. Specifies extensions for the interconnection, using non-LAN systems communication technologies, of geographically separated IEEE 802 LANs below the level of the logical link control protocol.
- IEEE Std 802.1H™
[ISO/IEC TR 11802-5] *Recommended Practice for Media Access Control (MAC) Bridging of Ethernet V2.0 in IEEE 802 Local Area Networks*.
- IEEE Std 802.1Q™ *Virtual Bridged Local Area Networks*. Defines an architecture for Virtual Bridged LANs, the services provided in Virtual Bridged LANs, and the protocols and algorithms involved in the provision of those services.
- IEEE Std 802.2
[ISO/IEC 8802-2] *Logical Link Control*.
- IEEE Std 802.3 *CSMA/CD Access Method and Physical Layer Specifications*.
- IEEE Std 802.5
[ISO/IEC 8802-5] *Token Ring Access Method and Physical Layer Specifications*.
- IEEE Std 802.10 *Standard for Interoperable LAN Security (SILS)*. Currently approved: Secure Data Exchange (SDE).
- IEEE Std 802.11
[ISO/IEC 8802-11] *Wireless LAN Medium Access Control (MAC) Sublayer and Physical Layer Specifications*.
- IEEE Std 802.15 *Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for: Wireless Personal Area Networks*.
- IEEE Std 802.16 *Air Interface for Fixed Broadband Wireless Access Systems*.

The reader of this recommended practice is urged to become familiar with the complete family of standards.

Publication of this trial-use standard for comment and criticism has been approved by the Institute of Electrical and Electronics Engineers. Trial-use standards are effective for 24 months from the date of publication. Comments for revision will be accepted for 18 months after publication. Suggestions for revision should be directed to the Secretary, IEEE-SA Standards Board, 445 Hoes Lane, P.O. Box 1331, Piscataway, NJ 08855-1331, and should be received no later than 14 January 2005. It is expected that following the 24-month period, this trial-use standard, revised as necessary, shall be submitted to the IEEE-SA Standards Board for approval as a full-use standard.

Participants

When the IEEE 802.11 Working Group approved this recommended practice, it had the following officers:

Stuart J. Kerry, *Chair*
Al Petrick and **Harry Worstell**, *Vice-Chairs*
Tim Godfrey, *Secretary*
Brian Mathews, *Publicity Standing Committee*
Teik-Kheong Tan, *Wireless Next-Generation Standing Committee*

John Fakatselis, *Chair Task Group e*
Duncan Kitchin, *Vice-Chair Task Group e*
Matthew B. Shoemake, *Chair Task Group g*
John Terry, *Vice-Chair Task Group g*
Mika Kasslin, *Chair Task Group h*
David Halasz, *Chair Task Group i*

When the IEEE 802.11 Working Group approved this recommended practice, the Task Group F had the following officers:

David Bagby, *Chair*
Jon Rosdahl, *Secretary*
Bob O Hara, *Technical Editor*

The Chair of Task Group F would like to recognize the following people who made particularly significant contributions to the development of this recommended practice:

Bernard Aboba
Butch Anton
Bill Arbaugh
Kevin Hayes

Justin McCann
Bob Moskowitz
Bob O Hara
Richard Paine

Jon Rosdahl
Tom Tsoulogiannis
John Vollbrecht
Liwen Wu

When the IEEE 802.11 Working Group approved this recommended practice, it had the following membership:

Bernard Aboba
L Enrique Aguado
Masaaki Akahane
Areg Alimian
Richard Allen
Baruch Altman
Keith Amann
Merwyn Andrade
Carl F. Andren
David C. Andrus
Butch Anton
Mitch Aramaki
Takashi Aramaki
Larry Arnett
Geert A. Awater
David Bagby
Jay Bain
Bala Balachander
Simon Barber
Steve Bard
Michael Barkway
Gil Bar-Noy
Kevin M. Barry
Anuj Batra
Bob Beach
Randolph Beltz
Mathilde Benveniste
Stuart Biddulph

Simon Black
Simon Blake-Wilson
Timothy Blaney
Jan Boer
Jim Brennan
Ronald Brockmann
Robert Brummer
Richard Bulman, Jr.
Kevin Burak
Alistair G. Buttar
Dominick Cafarelli
Colum Caldwell
Nancy Cam-Winget
Bill Carney
Michael Carrafiello
Pat Carson
Joan Ceuterick
Hung-Kun Chen
James C. Chen
Kwang-Cheng Chen
Yi-Ming Chen
Brian Cheng
Greg Chesson
Harshal S. Chhaya
Alan Chickinsky
Aik Chindapol
Leigh M. Chinitz
Bong-Rak Choi

Sunghyun Choi
Patrick Chokron
Frank Ciotti
Ken Clements
John T. Coffey
Terry Cole
Anthony Collins
Craig Conkling
Dennis Connors
Todor Cooklev
Thomas P Costas
Wm. Caldwell Crosswy
Russell J. Cyr
Peter Dahl
Barry Davis
Rolf De Vegt
Peter de Wit
Michael Derby
Georg Dickmann
Wim Diepstraten
Haoran Duan
Jeffrey Dunnihoo
Roger Durand
Eryk Dutkiewicz
Mary DuVal
Donald E. Eastlake III
Dennis Eaton
Peter Ecclesine

Jon Edney
 Darwin Engwer
 Javier Espinoza
 Christoph Euscher
 John Fakatselis
 Lars Falk
 Augustin J. Farrugia
 Weishi Feng
 Niels T. Ferguson
 Matthew James Fischer
 Michael Fischer
 Jason Flaks
 Aharon Friedman
 Kenji Fujisawa
 Shinya Fukuoka
 Marcus Gahler
 Zvi Ganz
 James Gardner
 Atul Garg
 Vafa Ghazi
 Amar Ghori
 James Gilb
 Tim Godfrey
 Wataru Gohda
 Peter Goidas
 Andrew J. Gowans
 Rik Graulus
 Evan Green
 Larry Green
 Patrick Green
 Kerry Greer
 Daqing Gu
 Rajugopal Gubbi
 Srikanth Gummadi
 Fred Haisch
 David Halasz
 Steve D. Halford
 Neil Hamady
 Mark Hamilton
 Christopher J. Hansen
 Yasuo Harada
 Amer A. Hassan
 Kevin Hayes
 Victor Hayes
 Chris Heegard
 Robert Heile
 Juha Heiskala
 Jerry Heller
 Bent Hessen-Schmidt
 Garth Hillman
 Christopher Hinsz
 Jun Hirano
 Jin-Meng Ho
 Maarten Hoebe
 Michael Hoghooghi
 Russell Housley
 Frank P Howley, Jr
 Dave Hudak
 John Hughes
 David Hunter
 David Hytha
 Hiroshi Ide
 Masataka Iizuka
 Yasuhiko Inoue
 Katsumi Ishii
 Marc Jalfon
 Hemaprabhu Jayanna
 Jung Je Son
 Ho-In Jeon

Peter Johansson
 Sherry Johnson
 VK Jones
 Bobby Jose
 Mark F. Kahn
 Srinivas Kandala
 Jeyhan Karaoguz
 Kevin Karcz
 Mika Kasslin
 Patrick Kelly
 Richard Kennedy
 Stuart J. Kerry
 Jamshid Khun-Jush
 Ryoji Kido
 Je Woo Kim
 Joonsuk Kim
 Ziv Kimhi
 Ken Kimura
 Duncan Kitchin
 G nter Kleindl
 Roger Knobbe
 John M. Kowalski
 Bruce P. Kraemer
 Thomas Kuehnel
 Geng-Sheng Kuo
 Denis Kuwahara
 Paul A. Lambert
 David S. Landeta
 Jim Lansford
 Colin Lanzl
 Kim Laraqui
 Peter Larsson
 David J. Leach, Jr.
 Martin Lefkowitz
 Onno Letanche
 Sheung Li
 William Li
 Yunxin Li
 Jie Liang
 Isaac Lim Wei Lih
 Shawn Liu
 Jay Livingston
 Titus Lo
 Peter Loc
 Ralph Lombardo, Jr.
 Luke Ludeman
 Yeong-Chang Maa
 Akira Maeki
 Douglas Makishima
 Mahalingam Mani
 Roger Marks
 Leslie A. Martin
 Brian Mathews
 Jo-Ellen F Mathews
 Mark Mathews
 Conrad Maxwell
 Ron McCallister
 Justin McCann
 Kelly McClellan
 Gary McCoy
 Bill McFarland
 Gary McGarr
 Bill McIntosh
 Jorge Medina
 Pratik Mehta
 Robert C. Meier
 Robert Miller
 Khashayar Mirfakhraei
 Sanjay Moghe

Tim Moore
 Paul Moose
 Mike Moreton
 Robert Moskowitz
 Oliver Muelhens
 Peter Murphy
 Peter Murray
 Andrew Myles
 Marco Naeye
 Ravi Narasimhan
 Kevin Negus
 David B. Nelson
 Dan Nemits
 Chiu Ngo
 Henry Nielsen
 Toshi Nishida
 Gunnar Nitsche
 Erwin R. Noble
 Tzvetan D. Novkov
 Ivan Oakes
 Timothy O Farrell
 Bob O Hara
 Yoshihiro Ohtani
 Lior Ophir
 Dirk Ostermiller
 Richard H. Paine
 Mike Paljug
 Gregory Parks
 Gavin Parnaby
 Lizy Paul
 Sebastien Perrot
 Al Petrick
 Anselmo Pilla
 Victoria M. Poncini
 James Portaro
 Al Potter
 Mike Press
 Ron Provencio
 Henry Ptasinski
 Ali Raissinia
 Murali Ramadoss
 Noman Rangwala
 Javad Razavilar
 David Reed
 Ivan Reede
 Stanley A. Reible
 Danny Rettig
 Edward Reuss
 Bill Rhyne
 Jim Richards
 David Richkas
 Maximilian Riegel
 Carlos A. Rios
 Benno Ritter
 Kent G. Rollins
 Stefan Rommer
 Jon Rosdahl
 Rob Roy
 Gunnar Rydnell
 Kenichi Sakusabe
 Anil K. Sanwalka
 Edward Schell
 Sid Schrum
 Joe Sensoroff
 Rick Shaw
 Yangmin Shen
 Matthew Sherman
 Matthew B. Shoemake
 William Shvodian

Aman Singla
David Skellern
Donald I. Sloan
Kevin Smart
Dave Smith
H. Keith Smith
V. Srinivasa Somayazulu
Wei-Jei Song
Amjad Soomro
Gary Spiess
Geetha Srikantan
Dorothy V. Stanley
Adrian Stephens
Spencer Stephens
William M. Stevens
Carl R. Stevenson
Susan Storma
Michael Su
Barani Subbiah
Minoru Takemoto
Pek-Yew Tan
Teik-Kheong Tan
Takuma Tanimoto
Roger Teague
Carl Temme

John Terry
Yossi Texerman
Jerry A. Thrasher
James D. Tomcik
Walt Trzaskus
Allen Tsai
Chih C. Tsien
Tom Tsoulogiannis
Khaled Turki
Mike Tzamaloukas
Toru Ueda
Niels Van Erven
Wim J. van Houtum
Patrick Vandenameele
Dmitri Varsanofiev
Jagannatha L. Venkatesha
Mahesh Venkatraman
Madan Venugopal
Alex Vereshchak
Ritesh Vishwakarma
John Vollbrecht
Toan X. Vu
Tim Wakeley
Jesse R. Walker

Thierry Walrant
Christopher Ware
Fujio Watanabe
Mark Webster
Mathew Welborn
Menzo Wentink
Doug Whiting
Peter K. Williams
Richard G.C. Williams
Steven D. Williams
Harry Worstell
Charles R. Wright
Liwen Wu
Yang Xiao
Shugong Xu
Hidehiro Yamashita
Wen-Ping Ying
Kit Yong
Albert Young
Heejung Yu
Patrick Yu
Chris Zegelin
Glen Zorn
Arnoud Zwemmer
Jim Zyren

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

Butch Anton
David Bagby
Morris Balamut
John Barnett
Mitchell Buchman
Todd Cooper
Kimara Chin
Keith Chow
Terry Cole
Michael Coletta
Todor Cooklev
Thomas Dineen
Dr. Sourav Dutta
Peter Ecclesine
Richard Fulsom
Michele Gammel
Andrew Germano
Tim Godfrey
Rajugopal Gubbi
Robert Heile
Gerald Heller

Tony Jeffree
Srinivas Kandala
Stuart Kerry
Cees Klik
Pi-Cheng Law
Daniel Levesque
Kyle Maus
George Miao
Apurva Mody
Mike Moreton
Charles Ngethe
Paul Nikolich
Erwin Noble
Ellis Nolley
Bob O'Hara
Satoshi Oyama
Sebastien Perrot
Al Petrick
Subbu Ponnuswamy
Hugo Pues
Vikram Punj

Charles Rice
Maximilian Riegel
Jon Rosdahl
Thomas Ruf
Osman Sakr
Douglas Sanderson
Durga Prasad Satapathy
Michael Seals
Matthew J. Sherman
Gil Shultz
Kevin Smart
Amjad Soomro
Jerry Thrasher
Dmitri Varsanofiev
Jay Warrior
William Watt
Hung-yu Wei
Harry Worstell
Jung Yee
Oren Yuen
Arnoud Zwemmer

When the IEEE-SA Standards Board approved this recommended practice on 12 June 2003, it had the following membership:

Don Wright, *Chair*
Howard M. Frazier, *Vice Chair*
Judith Gorman, *Secretary*

H. Stephen Berger
Joe Bruder
Bob Davis
Richard DeBlasio
Julian Forster*
Toshio Fukuda
Arnold M. Greenspan
Raymond Hapeman

Donald M. Heirman
Laura Hitchcock
Richard H. Hulett
Anant Jain
Lowell G. Johnson
Joseph L. Koepfinger*
Tom McGean
Steve Mills

Daleep C. Mohla
William J. Moylan
Paul Nikolic
Gary Robinson
Malcolm V. Thaden
Geoffrey O. Thompson
Doug Topping
Howard L. Wolfman

*Member Emeritus

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

Alan Cookson, *NIST Representative*
Satish K. Aggarwal, *NRC Representative*

Andrew Ickowicz
IEEE Standards Project Editor

Contents

1.	Overview	1
1.1	Scope.....	1
1.2	Purpose.....	1
1.3	Inter-AP recommended practice overview	2
1.4	Inter-AP security risks	4
2.	References	4
3.	Definitions, abbreviations, and acronyms	5
4.	IAPP service definition	6
4.1	IAPP-INITIATE.request.....	7
4.2	IAPP-INITIATE.confirm.....	8
4.3	IAPP-TERMINATE.request.....	9
4.4	IAPP-TERMINATE.confirm.....	9
4.5	IAPP-ADD.request	10
4.6	IAPP-ADD.confirm	11
4.7	IAPP-ADD.indication.....	12
4.8	IAPP-MOVE.request	13
4.9	IAPP-MOVE.confirm	14
4.10	IAPP-MOVE.indication.....	15
4.11	IAPP-MOVE.response.....	16
4.12	IAPP-CACHE-NOTIFY.request	17
4.13	IAPP-CACHE-NOTIFY.confirm	18
4.14	IAPP-CACHE-NOTIFY.indication	19
4.15	IAPP-CACHE-NOTIFY.response	20
4.16	Message sequence charts	21
5.	Operation of the IAPP	34
5.1	IAPP protocol overview.....	34
5.2	Formation and maintenance of the ESS.....	36
5.3	RADIUS protocol usage	36
5.4	Support for IEEE 802.11 context transfer.....	45
5.5	AP to AP interactions.....	45
5.6	Proactive caching	47
5.7	AP specific MIB	48
5.8	Single station association.....	49
6.	Packet formats	49
6.1	General IAPP packet format	49
6.2	ADD-notify packet.....	50
6.3	Layer 2 Update frame	51
6.4	MOVE-notify packet	51
6.5	MOVE-response packet.....	52
6.6	CACHE-notify packet.....	53
6.7	CACHE-response packet	54
6.8	Send-Security-Block packet.....	55
6.9	ACK-Security-Block packet.....	57
6.10	Information element definitions.....	57
	Annex A (normative) IAPP Management Information Base	61

IEEE Trial-Use Recommended Practice for Multi-Vendor Access Point Interoperability via an Inter-Access Point Protocol Across Distribution Systems Supporting IEEE 802.11™ Operation

1. Overview

1.1 Scope

The scope of this document is to describe recommended practices for implementation of an Inter-Access Point Protocol (IAPP) on a Distribution System (DS) supporting ISO/IEC 8802-11:1999 and IEEE 802.11™ wireless local access network (WLAN) links. The recommended DS utilizes an IAPP that provides the necessary capabilities to achieve multi-vendor Access Point (AP) interoperability within the DS. This IAPP is described for a DS consisting of IEEE 802® LAN components utilizing an Internet Engineering Task Force (IETF) Internet Protocol (IP) environment. Throughout this recommended practice, the terms *ISO/IEC 8802-11:1999*, *IEEE 802.11*, *802.11™*, and *IEEE Std 802.11™-1999* are used interchangeably to refer to the same document, ISO/IEC 8802-11:1999, and its amendments and supplements published at the time this recommended practice was adopted.

1.2 Purpose

IEEE 802.11 specifies the MAC and PHY layers of a WLAN system and includes the basic architecture of such systems, including the concepts of APs and DSs. Implementations of these concepts were purposely not defined by IEEE 802.11 because there are many ways to create a WLAN system. Additionally, many of the possible implementation approaches involve higher network layers. While this leaves great flexibility in DS and AP functional design, the associated cost is that physical AP devices are unlikely to interoperate across a DS. In particular, the enforcement of the restriction that a station (STA) has a single association at a given time is unlikely to be achieved.

As IEEE 802.11 systems have grown in popularity, it has become clear that there are a small number of DS environments that comprise the bulk of the commercial and private WLAN system installations.

This recommended practice specifies the information to be exchanged between APs amongst themselves and higher-layer management entities to support the 802.11 DS functions. The information exchanges are specified for DSs built on the IETF IP in a manner sufficient to enable the interoperation of DSs containing APs from different vendors that adhere to the recommended practice.

1.3 Inter-AP recommended practice overview

This recommended practice describes a service access point (SAP), service primitives, a set of functions and a protocol that will allow APs to interoperate on a common DS, using the Transmission Control Protocol over IP (TCP/IP) or User Datagram Protocol over IP (UDP/IP) to carry IAPP packets between APs, as well as describing the use of the Remote Authentication Dial-in User Service (RADIUS) Protocol, so APs may obtain information about one another. A proactive caching mechanism is also described that provides faster roaming times by sending STA context to neighboring APs. The devices in a network that might use the IAPP are 802.11 APs. Other devices in a network that are affected by the operation of the IAPP are layer 2 networking devices, such as bridges and switches.

Throughout this recommended practice, reference is made to an “AP management entity (APME).” These are references to a function that is external to the IAPP, though likely still a function of the AP device. Typically, this management entity is the main operational program of the AP, implementing an AP manufacturer’s proprietary features and algorithms, and incorporating the station management entity (SME) of 802.11. Figure 1 depicts an architecture of a typical AP in which the IAPP operates. The grey areas indicate areas where there is an absence of connection between blocks. The IAPP services are accessed by the APME through the IAPP SAP. The IAPP SAP is shown in Figure 1, as the small block between the APME and the IAPP blocks. IAPP service primitives are defined that allow the AP management entity to cause the IAPP to perform some function or to communicate with other APs in the DS or with a RADIUS server. Other service primitives indicate to the AP management entity that operations have taken place at other APs in the DS that can have an effect on information local to the AP.

The invocation of some IAPP service primitives relies on the RADIUS protocol to implement certain functions that are required for the correct and secure operation of the IAPP. In particular, the IAPP entity must be able to find and use a RADIUS server to look up the IP addresses of other APs in the ESS when given the Basic Service Set Identifier (BSSIDs) of those other APs (if a local capability to perform such a translation is not present), and to obtain security information to protect the content of certain IAPP packets. The RADIUS server must provide extensions for IAPP-specific operations. There is currently work being performed in the IETF on RADIUS client configuration. Refer to RADIUS Client Kickstart by Robert Moskowitz¹ on the topic. This work may be useful in conjunction with this recommended practice.

¹Information on references can be found in Clause 2.

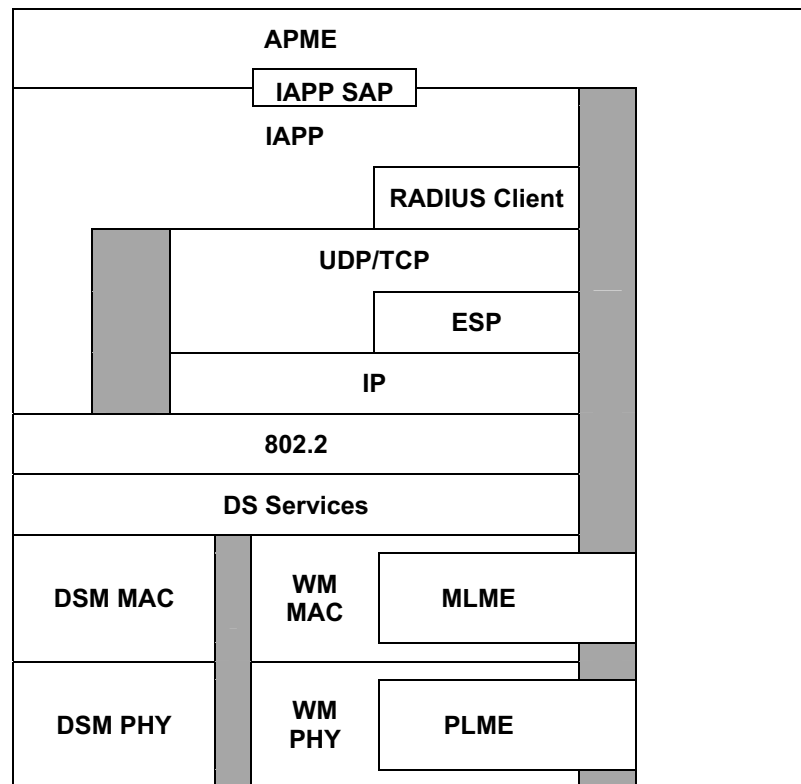


Figure 1—AP architecture with IAPP

The IAPP is not a routing protocol. The IAPP does not deal directly with the delivery of 802.11 data frames to the STA; instead the DS utilizes existing network functionality for data frame delivery. The data delivery service of the DS will function as desired when the STAs maintain a network layer address, e.g., IP address, or addresses that are valid for their point of connection to the network, i.e., when a STA associates or reassociates, the STA must ascertain that its network layer address(es) is configured such that the normal routing functions of the network attaching to the BSS will correctly deliver the STA's traffic to the BSS to which it is associated. If the mobile device incorporating the STA determines that the network layer address(es) is not configured so as to allow the normal routing functions of the network to deliver the STA's traffic to the BSS to which it is associated, the STA must obtain such an address(es), before any network traffic can be delivered to it. A STA can meet the local IP address requirement in many ways. Two mechanisms for a STA to accomplish this are to renew a Dynamic Host Configuration Protocol (DHCP) lease for its IP address and to use Mobile IP to obtain a local IP address. Other mechanisms are possible that meet this requirement.

With the requirement that STAs maintain a valid network layer address, APs function much the same as IEEE 802.1D™ bridges. Additionally, the IAPP supports the following functions:

- DS Services, as defined in ISO/IEC 8802-11:1999.
- Address mapping of wireless medium addresses of APs (their BSSID) to DS network layer addresses (IP addresses).
- Formation of a DS.
- Maintenance of the DS.
- Enforcement of the restriction of ISO/IEC 8802-11:1999 that a STA may have only a single association at any given time.
- Transfer of STA context information between APs.

IAPP transactions are over the DS. Hence, IAPP is independent of the security scheme defined in ISO/IEC 8802-11:1999.

This recommended practice makes use of the IETF RFCs listed in Clause 2 to implement many of its functions. It also relies on a STA making use of the 802.11 Reassociation Request frame when roaming from one AP to another, in order to provide the most complete services to the APs using the IAPP. When a STA uses the 802.11 Association Request, rather than the Reassociation Request, the IAPP may not be able to notify the AP at which the STA was previously associated of the new association. This may result in the old AP (indicated in the “current AP” field of the reassociation request frame) maintaining context for the STA that has roamed to a new AP for a longer time than is strictly necessary. This may cause undue waste of resources at the old AP, as well as limiting the ability of the IAPP to help enforce the single STA association requirement of 802.11.

One issue that AP designers should address that can cause significant problems in a WLAN is the continued operation of an AP when it has lost its link to the DS. When an AP continues to accept associations without a link to the DS, it is a black hole in the WLAN, where STAs associate and cannot communicate with anything beyond the AP’s BSS. When an AP loses its link to the DS, it should cease transmitting Beacons, disassociate all associated stations, and cease responding to Probe Request, Authentication, and Association Request frames.

1.4 Inter-AP security risks

Inter-AP communications present opportunities to an attacker. The attacker can use IAPP or forged 802.11 MAC management frames as a Denial-of-Service (DoS) attack against a STA state in its AP. It can capture MOVE packets to gather information on the STA that is roaming. It can act as a rogue AP in the ESS.

A bogus MOVE or ADD-Notify might cause an AP to drop all state it has with a STA. Since these IAPP packets are transmitted over IP, they could be introduced anywhere, from any device that has the necessary knowledge. This attack can best be eliminated by providing packet authentication to all MOVE and ADDs. The protection for the MOVEs can be provided by IP Encapsulating Security Payload (ESP) (RFC 2406:1998) pair-wise Security Associations (SA). The protection for the ADDs requires a group ESP SA. The content of the MOVE can be encrypted by the same ESP pair-wise SAs, protecting it from scrutiny of an attacker.

The use of ESP with RADIUS for the Key Management provides for discovery of Rogue APs. The use of ESP for IAPP MOVEs prevents a STA from roaming from a Rogue AP to a valid AP in the ESS. It also blocks the move of the STA context information to a Rogue AP if the STA roams to it. The RADIUS Access-Request provides the RADIUS server with knowledge of the presence of a Rogue AP.

2. References

The following standards contain provisions which, through references in this text, constitute provisions of this recommended practice. At the time of publication, the editions indicated were valid. All standards are subject to revision. When a standard is superseded by an approved revision, the revision applies.

IEEE Std 802.11, 1999 Edition (R2003) (ISO/IEC 8802-11: 1999), IEEE Standard for Information Technology—Telecommunications and Information Exchange between Systems—Local and Metropolitan Area Network—Specific Requirements—Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications.^{2, 3}

²The IEEE standards referred to in Clause 2 are trademarks belonging to the Institute of Electrical and Electronics Engineers, Inc.

³IEEE publications are available from the Institute of Electrical and Electronics Engineers, 445 Hoes Lane, P.O. Box 1331, Piscataway, NJ 08855-1331, USA (<http://www.standards.ieee.org/>).

IEEE Std 802.1X™-2001, IEEE Standards for Local and Metropolitan Area Networks: Port-Based Network Access Control.

IEEE Std 802.2™-1998 (ISO/IEC 8802-2:1998), IEEE Standard for Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements—Part 2: Logical Link Control.

IETF Internet Draft (October 2002)– RADIUS Client Kickstart.⁴

RFC 768:1980, User Datagram Protocol.⁵

RFC 791:1981, Internet Protocol—DARPA Internet Program Protocol Specification.

RFC 1112:1989, Host Extensions for IP Multicasting.

RFC 1305:1992, Network Time Protocol Specification, Implementation and Analysis.

RFC 1812:1995, Requirements for IP Version 4 Routers.

RFC 2002:1996, IP Mobility Support.

RFC 2131:1997, Dynamic Host Configuration Protocol.

RFC 2181:1997, Clarifications to the DNS Specification.

RFC 2390:1998, Inverse Address Resolution Protocol.

RFC 2406:1998, IP Encapsulating Security Payload (ESP).

RFC 2407:1998, The Internet IP Security Domain of Interpretation for ISAKMP.

RFC 2411:1998, IP Security—Document Roadmap.

RFC 2548:1999, Microsoft Vendor-specific RADIUS Attributes.

RFC 2857:2000, The Use of HMAC-RIPEMD-160-96 within ESP and AH.

RFC 2865:2000, Remote Authentication Dial In User Service (RADIUS).

RFC 2869:2000, RADIUS Extensions.

RFC 3162:2001, RADIUS in IPv6.

3. Definitions, abbreviations, and acronyms

AAA	Authentication, Authorization, and Accounting
AP	Access Point
APME	Access Point Management Entity
BSS	Basic Service Set

⁴This internet draft is available from the Internet Engineering Task Force (IETF) <http://www.ietf.org/internet-drafts/draft-moskowitz-radius-client-kickstart-00.txt>.

⁵Requests for Comments (RFCs) are available from the Internet Engineering Task Force (IETF) at <http://www.ietf.org/rfc>.

BSSID	Basic Service Set Identifier
DHCP	Dynamic Host Configuration Protocol
DS	Distribution System
DSM	Distribution System Medium
ESP	IP Encapsulating Security Payload
ESS	Extended Service Set
IANA	Internet Assigned Numbers Authority
IAPP	Inter-Access Point Protocol
IETF	Internet Engineering Task Force
IP	Internet Protocol
LLC	Logical Link Control
MAC	Medium Access Control
MLME	MAC Layer Management Entity
PAE	Port Access Entity
PHY	Physical layer
PLME	PHY Layer Management Entity
RADIUS	Remote Authentication Dial In User Service
SA	Security Association
SAP	Service Access Point
SME	Station Management Entity
SPI	Security Parameter Index
SSID	Service Set Identifier
STA	Station
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
URL	Uniform Resource Locator
VSA	Vendor-specific attribute
WM	Wireless Medium
XID	Exchange Identifier

4. IAPP service definition

The IAPP entity provides services to an AP in which it resides through the IAPP SAP. The SAP allows the management entity of the AP (APME) to invoke IAPP services and receive indications of service invocations at other APs in a single ESS. This clause defines the services that are available at the SAP. There are four types of service primitives that exist at the SAP. They are requests, confirms, indications, and responses. Service requests and responses are submitted to the IAPP entity by the entity at the next higher layer. In this document, the next higher layer is the APME. Service confirms and indications are delivered by the IAPP entity to the entity at the next higher layer.

This clause provides an abstract description of the services that an implementation should provide in order to interoperate with other implementations of the IAPP. This is not an exposed interface. A diagram of the relationships between the primitives is shown in Figure 2.

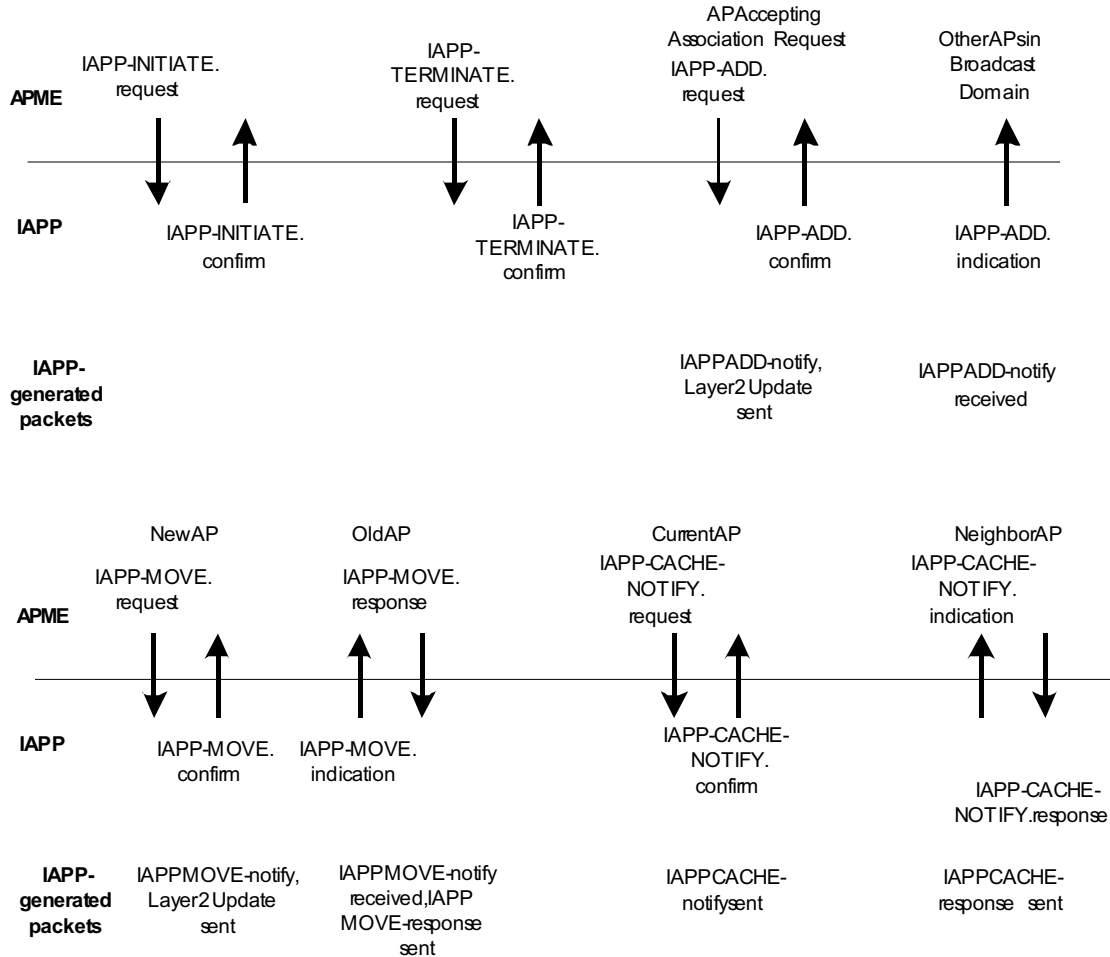


Figure 2—Primitive relationships

4.1 IAPP-INITIATE.request

4.1.1 Function

This service primitive causes the AP to initialize the IAPP entity, including its data structures, functions, and protocol.

4.1.2 Semantics of the service primitive

The IAPP-INITIATE.request has the following semantics:

```
IAPP-INITIATE.request {
    TCP Port,
    UDP Port,
    IP Address,
    BSSID Secret
}
```

The UDP Port parameter is the UDP port number to be opened for the IAPP for transmission and reception of IAPP packets. The port assigned by IANA for this protocol is 3517.

The TCP Port parameter is the TCP port number that the IAPP entity opens to listen for new IAPP TCP connections from the IAPP entities of other APs. The port assigned by IANA for this protocol is 3517.

The IP address is the IP address or fully qualified domain name of the RADIUS server.

The BSSID Secret is used to provide integrity, authentication, and confidentiality of the security block sent between the RADIUS server and the AP. See 5.3. If RADIUS is not used, this parameter is null.

4.1.3 When generated

This service primitive is generated by an APME to initiate the operation of the IAPP. At the time the IAPP-INITIATE.request is generated, the BSS controlled by this AP should not be operating, and no STAs should be associated with this AP. If necessary, the APME can issue an 802.11 MLME-RESET.request prior to generation of the IAPP-INITIATE.request.

4.1.4 Effect of receipt

Upon receipt of this service primitive from an APME, the action of the IAPP entity depends on the service level that is implemented. See 5.2. For level 1, there is no RADIUS usage. For levels 2 and 3, the IAPP entity sends the RADIUS Initiate-Request and receives the RADIUS Initiate-Accept or Initiate-Reject. If the Initiate-Accept is received, then the IAPP entity initializes its data structures, functions, and protocols. The port for the IAPP should be opened by the IAPP entity at this time. The previous information in any IAPP data structures is lost. If an Initiate-Reject is received, the IAPP does not start.

4.2 IAPP-INITIATE.confirm

4.2.1 Function

This service primitive notifies an APME that the actions begun by an IAPP-INITIATE.request have been completed.

4.2.2 Semantics of the service primitive

The IAPP-INITIATE.confirm primitive has the following semantics:

```
IAPP-INITIATE.confirm {  
    Status  
}
```

The Status parameter indicates the result of the corresponding IAPP-INITIATE.request. The allowable value for the Status parameter are SUCCESSFUL, RUNNING, and FAILURE. SUCCESSFUL status should be returned if the IAPP entity is able to complete its initialization and open the requested port for the IAPP. RUNNING status should be returned if the IAPP entity receives an IAPP-INITIATE.request when the entity is already running. When RUNNING status has been returned, the IAPP ignored the parameters from the corresponding IAPP-INITIATE.request and the operation of the IAPP was unaffected. FAILURE status should be returned otherwise.

4.2.3 When generated

This service primitive is generated when the actions begun by an IAPP-INITIATE.request are completed or the invocation of that primitive has failed.

4.2.4 Effect of receipt

Upon receipt of the IAPP-INITIATE.confirm(Status=SUCCESSFUL) corresponding to a previously issued IAPP-INITIATE.request, an APME should initialize the operation of the AP by issuing an 802.11 MLME-START.request primitive to the local 802.11 MLME. The APME should not issue an 802.11 MLME-START.request until an IAPP-INITIATE.confirm(Status=SUCCESSFUL) is received, i.e., to ensure that all associations in this BSS are reported to the ESS using IAPP, the AP should not begin operating until after the IAPP-INITIATE.confirm(Status=SUCCESSFUL) is received.

4.3 IAPP-TERMINATE.request

4.3.1 Function

This service primitive causes the IAPP entity to cease operation of the IAPP functions and protocol.

4.3.2 Semantics of the service primitive

The IAPP-TERMINATE.request primitive has the following semantics:

```
IAPP-TERMINATE.request {  
    }  
}
```

4.3.3 When generated

This service primitive is generated by an APME when it is desired to terminate the operation of the IAPP entity. The APME should terminate operation of the local BSS, including disassociation of any associated STAs and ceasing of beacon transmissions, prior to terminating IAPP operation. The sole or final action by the APME in termination of local BSS operation should be issuance of an MLME-RESET.request. The IAPP-TERMINATE.request should be generated upon receipt of the corresponding MLME-RESET.confirm.

4.3.4 Effect of receipt

The UDP and TCP ports for the IAPP should be closed and the IAPP entity should cease operations.

4.4 IAPP-TERMINATE.confirm

4.4.1 Function

This service primitive notifies an APME that the actions begun by an IAPP-TERMINATE.request have been completed.

4.4.2 Semantics of the service primitive

The IAPP-TERMINATE.confirm primitive has the following semantics:

```
IAPP-TERMINATE.confirm {  
    Status  
}
```

The Status parameter indicates the result of the corresponding IAPP-TERMINATE.request. The allowable value for the Status parameter is SUCCESSFUL.

4.4.3 When generated

This service primitive is generated by the IAPP entity when the actions begun by an IAPP-TERMINATE.request are completed.

4.4.4 Effect of receipt

Upon receipt of the IAPP-TERMINATE.confirm corresponding to a previously issued IAPP-TERMINATE.request, the APME should make no further service requests to the IAPP SAP without starting the IAPP entity again, using the IAPP-INITIATE.request primitive. Furthermore, the APME should not issue an MLME-START.request primitive prior to receipt of the subsequent IAPP-INITIATE.confirm primitive which indicates that the IAPP has been restarted successfully.

4.5 IAPP-ADD.request

4.5.1 Function

This service primitive is used when a STA associates with the AP using an 802.11 association request frame. The function of the IAPP-ADD.request primitive is two-fold. One purpose of this primitive is to cause the forwarding tables of layer 2 internetworking devices, e.g. bridges and switches, to be updated. This updates the layer 2 internetworking devices before a transmission from the associating STA, which might occur some arbitrary amount of time after the association. The second purpose of this primitive is to notify other APs within the multicast domain, i.e., that portion of a network in which a layer two frame addressed to a multicast address can be received, of the STA's new association, to allow those APs to clean up context information left behind by STAs that do not properly reassociate when moving from one AP to another, but rather only use the 802.11 Association Request.

4.5.2 Semantics of the service primitive

The IAPP-ADD.request primitive has the following semantics:

```
IAPP-ADD.request {  
    MAC Address,  
    Sequence Number,  
    Timeout  
}
```

The MAC Address is the address of the STA that recently has successfully associated with the AP.

The Sequence Number is the value of the 802.11 Sequence Number field of the Association Request frame received from the associating STA. The sequence number is provided to aid the APME in other APs in the determination of whether the association represented by this IAPP-ADD.request is the most recent association for the STA identified by the MAC Address. The 802.11 sequence number may be an ambiguous indication of the most recent association. But, this information may be useful to an algorithm making a determination of the location of the most recent association of a STA.

The Timeout parameter is the value, in seconds that the IAPP-ADD.confirm primitive will be generated with a status of TIMEOUT, if both the ADD-notify packet (see 6.2) and the Layer 2 Update frame (see 6.3) have not been sent. The TIMEOUT status will not be generated by the IAPP-ADD.confirm only when both the ADD-notify packet and Layer 2 Update frame have been transmitted before the expiration of the period indicated by the Timeout parameter.

4.5.3 When generated

This service primitive should be generated by an APME when the local AP generates an 802.11 MLME-ASSOCIATE.indication.

4.5.4 Effect of receipt

Receipt of this service primitive should cause the following actions to occur:

- a) The IAPP entity sends a Layer 2 Update frame to the DS, addressed such that it will cause forwarding tables in layer 2 devices that receive the frame to be updated so that all future traffic received by those layer 2 devices is forwarded to the port on which the frame was received,
- b) The IAPP entity notifies the APs in the local multicast domain of the DS of the association between the AP and STA by sending an IAPP ADD-notify packet to the IAPP IP multicast address. The IAPP multicast address is 224.0.1.178. See RFC 1112:1989.
- c) The IAPP-ADD function also indicates that any cache entry for the STA must be cleared since a new association has occurred.

4.6 IAPP-ADD.confirm

4.6.1 Function

This service primitive is used to confirm that the actions initiated by an IAPP-ADD.request have been completed and inform an APME of the status of those actions.

4.6.2 Semantics of the service primitive

The IAPP-ADD.confirm primitive has the following semantics:

```
IAPP-ADD.confirm {  
    Status  
}
```

The Status parameter indicates the success or failure of the corresponding IAPP-ADD.request. The allowable values for this parameter are SUCCESSFUL, FAIL and TIMEOUT. SUCCESSFUL status indicates that the corresponding IAPP-ADD.request was able to send both the IAPP ADD-notify packet and Layer 2 Update frame before the timeout expired. FAIL indicates that for some reason, the IAPP ADD-notify packet and the Layer 2 Update frame could not be sent at all. TIMEOUT status indicates that one or both of the ADD-notify packet and Layer 2 Update frame were not sent before the timeout expired.

4.6.3 When generated

This service primitive is generated upon completion of the actions of the IAPP-ADD.request or expiration of the timeout specified in the corresponding IAPP-ADD.request primitive.

4.6.4 Effect of receipt

Upon receipt of this service primitive by an APME with Status=SUCCESSFUL, the APME should cause the DS Services to begin forwarding frames for the associated STA. Receipt of this primitive with Status=TIMEOUT should cause the APME to attempt to determine the cause of the failure to send the ADD-notify packet and Layer 2 Update frames and possibly invoke the IAPP-ADD.request again. When Status=FAIL, the STA's association should be denied or the STA disassociated.

4.7 IAPP-ADD.indication

4.7.1 Function

The IAPP-ADD.indication primitive is used to indicate to an APME that an association relationship has been established between a STA and another AP in the DS.

4.7.2 Semantics of the service primitive

The IAPP-ADD.indication primitive has the following semantics:

```
IAPP-ADD.indication {  
    MAC Address,  
    Sequence Number  
}
```

The MAC Address is the address of the STA received in the IAPP ADD-notify packet.

The Sequence Number is the value of the 802.11 Sequence Number field of the Association Request frame received from the associating STA as received by the local IAPP entity in the ADD-notify packet. The sequence number is provided to aid the APME in the determination of whether the association represented by this IAPP-ADD.indication is the most recent association for the STA identified by the MAC Address. The 802.11 sequence number is not an unambiguous indication of the most recent association. But, this information may be useful to an algorithm making this determination.

4.7.3 When generated

This service primitive is generated upon receipt of an IAPP ADD-notify packet from the DS.

4.7.4 Effect of receipt

Upon receipt of this service primitive the APME should determine if the STA indicated by the MAC Address is shown to be associated with the AP receiving the IAPP-ADD.indication, with a sequence number older than that in the IAPP ADD-notify packet. If so, this service primitive should cause the generation of an 802.11 MLME-DISASSOCIATE.request by the APME. See 4.7.2. If the sequence number received in the IAPP ADD-notify packet is older than that received from the STA when it associated with the AP receiving the IAPP ADD-notify packet, the APME should ignore the indicated association and issue an IAPP-ADD.request.

Implementers of STA MAC entities are advised of the importance of continuing the sequential assignment of sequence numbers for outgoing MPDUs and MMPDUs throughout STA operation, as required by 802.11. A discontinuity in the sequence numbering at the time of reassociation could cause roaming in an IAPP environment to be unreliable. The 802.11 sequence number may be an ambiguous indication of the most recent association. But, this information may be useful to an algorithm making a determination of the location of the most recent association of a STA.

4.8 IAPP-MOVE.request

4.8.1 Function

This primitive should be issued by the APME when it receives an MLME-REASSOCIATE.indication from the MLME indicating that an STA has reassociated with the AP. It will attempt to send an IAPP MOVE-notify packet to the AP with which the reassociating STA was previously associated to notify that AP of the STA's reassociation.

4.8.2 Semantics of the service primitive

The IAPP-MOVE.request primitive has the following semantics:

```
IAPP-MOVE.request {  
    MAC Address,  
    Sequence Number,  
    Old AP,  
    Context Block,  
    Timeout  
}
```

The MAC Address is the address of the STA that recently has successfully reassociated with the AP.

The Sequence Number is the value of the 802.11 Sequence Number field of the Reassociation Request frame received from the reassociating STA. The sequence number is provided to aid the APME in other APs in the determination of whether the association represented by this IAPP-MOVE.request is the most recent association for the STA identified by the MAC Address. The 802.11 sequence number is not an unambiguous indication of the most recent association. But, this information may be useful to an algorithm making this determination.

Old AP is the MAC address of the AP with which the reassociating STA was last associated. This value is obtained by the APME from the Current AP Address field of the 802.11 Reassociation Request frame.

The Context Block is the context to be sent to the Old AP. Otherwise, the Context Block is null. The Context Block is a container for information defined in 802.11 that is to be forwarded from one AP to another upon the reassociation of a STA.

The Timeout parameter value is the number of seconds expected for the IAPP MOVE-notify packet to be sent and the IAPP MOVE-response packet received. Failure to send the packet and receive a response in this time results in the IAPP-MOVE.confirm primitive being generated with a status of TIMEOUT.

4.8.3 When generated

This service primitive is generated by an APME when the MLME receives an 802.11 MLME-REASSOCIATE.indication from the local AP.

4.8.4 Effect of receipt

Receipt of this service primitive should cause the following actions to occur:

- a) The IAPP entity determines the DSM Layer 3 address of the AP identified by the old BSSID presented in the reassociation request and the security information needed to communicate with that AP using the methods described in Clause 5.