

This is an **Archive IEEE Standard**. It has been withdrawn or superseded by a later version of the standard.

ARCHIVE STANDARDS MAY HAVE VALUE AS HISTORICAL DOCUMENTS, BUT THEY ARE NOT VALID OR APPROVED IEEE STANDARDS. THE IEEE SHALL NOT BE LIABLE FOR ANY DAMAGES RESULTING FROM THE SUBSCRIBER'S OR USERS' PRACTICE OF THIS UNAPPROVED, ARCHIVE IEEE STANDARD.

For more information about this or other current, revised or withdrawn standards, please consult the IEEE Standards Status report on-line at <http://standards.ieee.org/db/status/>.

**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**

Sponsor

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

Approved 26 June 1997

IEEE Standards Board

Abstract: The medium access control (MAC) and physical characteristics for wireless local area networks (LANs) are specified in this standard, part of a series of standards for local and metropolitan area networks. The medium access control unit in this standard is designed to support physical layer units as they may be adopted dependent on the availability of spectrum. This standard contains three physical layer units: two radio units, both operating in the 2400–2500 MHz band, and one baseband infrared unit. One radio unit employs the frequency-hopping spread spectrum technique, and the other employs the direct sequence spread spectrum technique.

Keywords: ad hoc network, infrared, LAN, local area network, mobility, radio frequency, wireless

The Institute of Electrical and Electronics Engineers, Inc.
345 East 47th Street, New York, NY 10017-2394, USA

Copyright © 1997 by the Institute of Electrical and Electronics Engineers, Inc.
All rights reserved. Published 1997. Printed in the United States of America.

ISBN 1-55937-935-9

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 Technical Committees of the IEEE Societies and the Standards Coordinating Committees of the IEEE Standards Board. Members of the committees serve voluntarily and without compensation. They are not necessarily members of the Institute. The standards developed within IEEE represent a consensus of the broad expertise on the subject within the Institute as well as those activities outside of IEEE that have expressed an interest in participating in the development of the standard.

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

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.

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 all 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 technical 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 on standards and requests for interpretations should be addressed to:

Secretary, IEEE Standards Board
445 Hoes Lane
P.O. Box 1331
Piscataway, NJ 08855-1331
USA

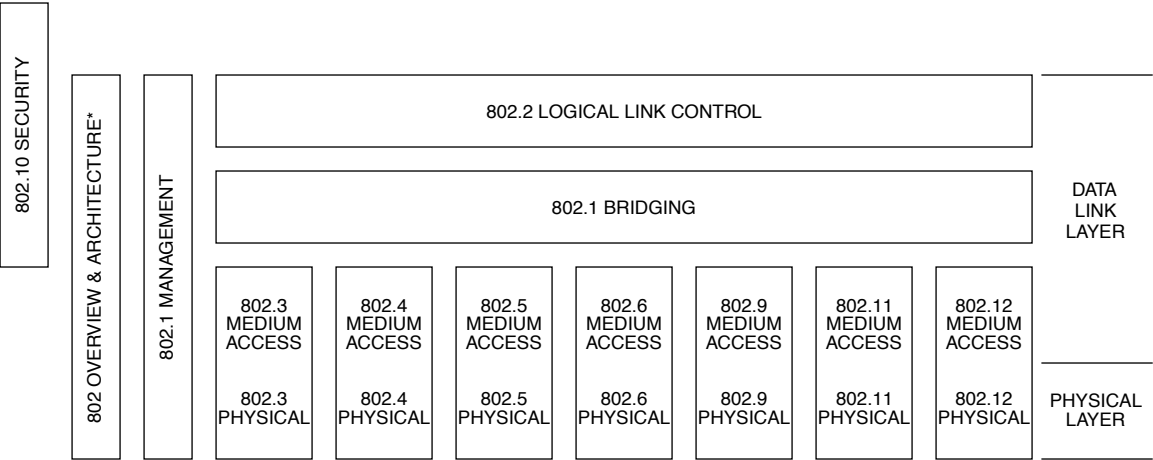
Note: Attention is called to the possibility that implementation of this standard may require use of subject matter covered by patent rights. By publication of this standard, no position is taken with respect to the existence or validity of any patent rights in connection therewith. The IEEE shall not 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.

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; (508) 750-8400. Permission to photocopy portions of any individual standard for educational classroom use can also be obtained through the Copyright Clearance Center.

Introduction

(This introduction is not part of IEEE Std 802.11-1997, but is included for information only.)

This standard 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 numbers.)



* Formerly IEEE Std 802.1A.

This family of standards deals with the physical and data link layers as defined by the International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) Open Systems Interconnection Basic Reference Model (ISO/IEC 7498-1: 1994). The access standards define several types of medium access technologies and associated physical media, each appropriate for particular applications or system objectives. Other types are under investigation.

The standards defining the access technologies are as follows:

- IEEE Std 802 *Overview and Architecture.* This standard provides an overview to the family of IEEE 802 Standards. This document forms part of the 802.1 scope of work.
- ANSI/IEEE Std 802.1B and 802.1k [ISO/IEC 15802-2] *LAN/MAN Management.* Defines an Open Systems Interconnection (OSI) management-compatible architecture, and services and protocol elements for use in a LAN/MAN environment for performing remote management.
- ANSI/IEEE Std 802.1D [ISO/IEC 10038] *MAC Bridging.* Specifies an architecture and protocol for the interconnection of IEEE 802 LANs below the MAC service boundary.
- ANSI/IEEE Std 802.1E [ISO/IEC 15802-4] *System Load Protocol.* Specifies a set of services and protocol for those aspects of management concerned with the loading of systems on IEEE 802 LANs.
- ANSI/IEEE Std 802.2 [ISO/IEC 8802-2] *Logical Link Control*
- ANSI/IEEE Std 802.3 [ISO/IEC 8802-3] *CSMA/CD Access Method and Physical Layer Specifications*
- ANSI/IEEE Std 802.4 [ISO/IEC 8802-4] *Token Passing Bus Access Method and Physical Layer Specifications*

- ANSI/IEEE Std 802.5 *Token Ring Access Method and Physical Layer Specifications*
[ISO/IEC 8802-5]
- ANSI/IEEE Std 802.6 *Distributed Queue Dual Bus Access Method and Physical Layer Specifications*
[ISO/IEC 8802-6]
- ANSI/IEEE Std 802.9 *Integrated Services (IS) LAN Interface at the Medium Access Control (MAC) and Physical (PHY) Layers*
[ISO/IEC 8802-9]
- ANSI/IEEE Std 802.10 *Interoperable LAN/MAN Security*
- IEEE Std 802.11 *Wireless LAN Medium Access Control (MAC) and Physical Layer Specifications*
[ISO/IEC DIS 8802-11]
- ANSI/IEEE Std 802.12 *Demand Priority Access Method, Physical Layer and Repeater Specifications*
[ISO/IEC DIS 8802-12]

In addition to the family of standards, the following is a recommended practice for a common Physical Layer technology:

- IEEE Std 802.7 *IEEE Recommended Practice for Broadband Local Area Networks*

The following additional working group has authorized standards projects under development:

- IEEE 802.14 *Standard Protocol for Cable-TV Based Broadband Communication Network*

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

Conformance test methodology

An additional standards series, identified by the number 1802, has been established to identify the conformance test methodology documents for the 802 family of standards. Thus the conformance test documents for 802.3 are numbered 1802.3.

IEEE Std 802.11-1997

This standard defines the protocol and compatible interconnection of data communication equipment via the “air,” radio or infrared, in a local area network (LAN) using the carrier sense multiple access protocol with collision avoidance (CSMA/CA) medium sharing mechanism. The medium access control (MAC) supports operation under control of an access point as well as between independent stations. The protocol includes authentication, association, and reassociation services, an optional encryption/decryption procedure, power management to reduce power consumption in mobile stations, and a point coordination function for time-bounded transfer of data. The standard includes the definition of the management information base (MIB) using Abstract Syntax Notation 1 (ASN.1) and specifies the MAC protocol in a formal way, using the Specification and Description Language (SDL).

The infrared implementation of the PHY supports 1 Mbit/s data rate with an optional 2 Mbit/s extension. The radio implementations of the PHY specify either a frequency-hopping spread spectrum (FHSS) supporting 1 Mbit/s and an optional 2 Mbit/s data rate or a direct sequence spread spectrum (DSSS) supporting both 1 and 2 Mbit/s data rates.

This standard contains state-of-the-art material. The area covered by this standard is undergoing evolution. Revisions are anticipated to this standard within the next few years to clarify existing material, to correct possible errors, and to incorporate new related material. Information on the current revision state of this and other IEEE 802 standards may be obtained from

Secretary, IEEE Standards Board
445 Hoes Lane
P.O. Box 1331
Piscataway, NJ 08855-1331 USA

Participants

At the time the draft of this standard was sent to sponsor ballot, the IEEE 802.11 working group had the following voting members:

Victor Hayes, *Chair* **Stuart J. Kerry** and **Chris Zegelin**, *Vice Chairs*
Bob O'Hara and **Greg Ennis**, *Chief Technical Editors*
George Fishel and **Carolyn L. Heide**, *Secretaries*

David Bagby, *MAC Group Chair* **C. Thomas Baumgartner**, *Infrared Chair and Editor*
Jan Boer, *Direct Sequence Chair* **Michael Fischer**, *State Diagram Editor*
Dean M. Kawaguchi, *PHY Group and FH Chair* **Mike Trompower**, *Direct Sequence Editor*

Jeff Abramowitz
Keith B. Amundsen
Phil Belanger
Manuel J. Betancor*
John Biddick
Simon Black
Alessandro M. Bolea
Pablo Brenner
Peter E. Chadwick
Naftali Chayat
Jonathon Y. Cheah
Hae Wook Choi
Wim Diepstraten
Robert J. Egan
Darwin Engwer
John Fakatselis
Matthew Fischer
Keith S. Furuya
Rich Gardner
Ian Gifford

Howard J. Hall
Bill Huhn
Donald C. Johnson
Mikio Kiyono
Joseph J. Kubler
Arthur Lashbrook
Francisco J. Lopez-Hernandez
Ronald Mahany
Bob Marshall
Jim McDonald
Akira Miura
Wayne D. Moyers
Ravi P. Nalamati
Mitsuji Okada
Al Petrick
Miri Ratner
James A. Renfro
William Roberts
Jon Walter Rosdahl

Michael Rothenberg
Chandos A. Rypinski
Anil K. Sanwalka
Roy Sebring
Glen Sherwood
Thomas Siep
Nathan Silberman
Don Sloan
Greg Smith
Marvin L. Sojka
Dave Strohschein
Bert Sullam
Mack Sullivan
Tom Tsoulogiannis
Jeanine Valadez
Sarosh Vesuna
Richard E. White
Donna A. Woznicki
Timothy M. Zimmerman
Johnny Zweig

Major contributions were received from the following individuals:

Robert Achatz
Ken Biba
Paul Eastman
Ed Geiger
Larry van der Jagt

Richard Lee
Kerry Lynn
Michael Masleid
John McKown
K. S. Natarajan
Jim Neally

Richard Ozer
Thomas Phinney
Leon S. Scaldeferri*
Jim Schuessler
François Y. Simon

*Deceased

The following persons were on the balloting committee:

Bernhard Albert
Jon M. Allingham
Jack S. Andresen
Kit Athul
Anthony L. Barnes
Robert T. Bell
Manuel J. Betancor
Simon Black
Alan L. Bridges
Graham Campbell
James T. Carlo
David E. Carlson
Peter E. Chadwick
Naftali Chayat
Alan J. Chwick
Ken Clements
Robert S. Crowder
Rifaat Dayem
Wim Diepstraten
Edward A. Dunlop
Sourav K. Dutta
Paul S. Eastman
Peter Ecclesine
Gregory Elkmann
John E. Emrich
Philip H. Enslow
Changxin Fan
Michael A. Fischer
Harvey A. Freeman
Robert J. Gagliano
Patrick S. Gonia
N. Douglas Grant
Govert M. Griffioen
Joseph L. Hammond
Victor Hayes
Kenneth C. Heck
Jan Hoogendoorn
Russell D. Housley
Walter K. Hurwitz

Richard J. Iliff
Tomoaki Ishifuji
Carlos Islas-Perez
Raj Jain
A. Kamerman
Peter M. Kelly
Yongbum Kim
Mikio Kiyono
Thaddeus Kobylarz
Stephen B. Kruger
Joseph J. Kubler
David J. Law
Jai Yong Lee
Jungtae Lee
Daniel E. Lewis
Randolph S. Little
Ming T. Liu
Joseph C. J. Loo
Donald C. Loughry
Robert D. Love
Ronald Mahany
Jim L. Mangin
Peter Martini
P. Takis Mathiopoulos
Steve Messenger
Bennett Meyer
Ann Miller
David S. Millman
Hiroshi Miyano
Stig Frode Mjolsnes
W. Melody Moh
John E. Montague
Wayne D. Moyers
Paul Nikolich
Ellis S. Nolley
Robert O'Hara
Donal O'Mahony
Roger Pandanda
Lalit Mohan Patnaik
Lucy W. Person

Thomas L. Phinney
Vikram Prabhu
Alberto Profumo
David L. Propp
Vikram Punj
Andris Putnins
Fernando Ramos
James W. Romlein
Floyd E. Ross
Michael Rothenberg
Christoph Ruland
Chandos A. Rypinski
Anil K. Sanwalka
Gregory D. Schumacher
Rich Seifert
Lee A. Sendelbach
Michael Serrone
Adarshpal S. Sethi
Donald A. Sheppard
Nathan Silberman
Joseph S. Skorupa
Michael A. Smith
Marvin L. Sojka
Efsthios D. Sykas
Geoffrey O. Thompson
Robert C. Tripi
Mike Trompower
David B. Turner
Mark-Rene Uchida
James Vorhies
Yun-Che Wang
Raymond P. Wenig
Earl J. Whitaker
David W. Wilson
Jerry A. Wyatt
Qian-Li Yang
Iwen Yao
Oren Yuen
Jonathan M. Zweig

When the IEEE Standards Board approved this standard on 26 June 1997, it had the following membership:

Donald C. Loughry, *Chair*

Richard J. Holleman, *Vice Chair*

Andrew G. Salem, *Secretary*

Clyde R. Camp
Stephen L. Diamond
Harold E. Epstein
Donald C. Fleckenstein
Jay Forster**
Thomas F. Garrity
Donald N. Heirman
Jim Isaak
Ben C. Johnson

Lowell Johnson
Robert Kennelly
E. G. "Al" Kiener
Joseph L. Koepfinger**
Stephen R. Lambert
Lawrence V. McCall
L. Bruce McClung
Marco W. Migliaro

Louis-François Pau
Gerald H. Peterson
John W. Pope
Jose R. Ramos
Ronald H. Reimer
Ingo Rüsç
John S. Ryan
Chee Kiow Tan
Howard L. Wolfman

**Member Emeritus

Also included are the following nonvoting IEEE Standards Board liaisons:

Satish K. Aggarwal
Alan H. Cookson

Kristin Dittmann
IEEE Standards Project Editor

Contents

1.	Overview.....	1
1.1	Scope	1
1.2	Purpose	1
2.	Normative references	2
3.	Definitions.....	3
4.	Abbreviations and acronyms.....	6
5.	General description	9
5.1	General description of the architecture	9
5.1.1	How wireless LAN systems are different	9
5.2	Components of the IEEE 802.11 architecture	10
5.2.1	The independent BSS as an ad hoc network	10
5.2.2	Distribution system concepts	11
5.2.3	Area concepts.....	12
5.2.4	Integration with wired LANs	14
5.3	Logical service interfaces	14
5.3.1	Station service (SS).....	15
5.3.2	Distribution system service (DSS).....	15
5.3.3	Multiple logical address spaces	16
5.4	Overview of the services	17
5.4.1	Distribution of messages within a DS	17
5.4.2	Services that support the distribution service	18
5.4.3	Access and confidentiality control services	19
5.5	Relationships between services	21
5.6	Differences between ESS and IBSS LANs	23
5.7	Message information contents that support the services	24
5.7.1	Data	25
5.7.2	Association	25
5.7.3	Reassociation	25
5.7.4	Disassociation	26
5.7.5	Privacy	26
5.7.6	Authentication	26
5.7.7	Deauthentication	27
5.8	Reference model.....	27
6.	MAC service definition.....	29
6.1	Overview of MAC services.....	29
6.1.1	Asynchronous data service	29
6.1.2	Security services	29
6.1.3	MSDU ordering	29
6.2	Detailed service specification.....	30
6.2.1	MAC data services	30
7.	Frame formats	34
7.1	MAC frame formats	34
7.1.1	Conventions	34
7.1.2	General frame format.....	34

7.1.3	Frame fields	35
7.2	Format of individual frame types	41
7.2.1	Control frames	41
7.2.2	Data frames	43
7.2.3	Management frames.....	45
7.3	Management frame body components	50
7.3.1	Fixed fields.....	50
7.3.2	Information elements	55
8.	Authentication and privacy	60
8.1	Authentication services	60
8.1.1	Open System authentication	60
8.1.2	Shared Key authentication	61
8.2	The Wired Equivalent Privacy (WEP) algorithm	62
8.2.1	Introduction.....	62
8.2.2	Properties of the WEP algorithm	63
8.2.3	WEP theory of operation	63
8.2.4	WEP algorithm specification	65
8.2.5	WEP MPDU expansion	65
8.3	Security-Related MIB attributes.....	66
8.3.1	Authentication-Related MIB attributes.....	66
8.3.2	Privacy-Related MIB attributes	66
9.	MAC sublayer functional description	71
9.1	MAC architecture	71
9.1.1	Distributed coordination function (DCF).....	71
9.1.2	Point coordination function (PCF).....	71
9.1.3	Coexistence of DCF and PCF	72
9.1.4	Fragmentation/defragmentation overview	72
9.1.5	MAC data service	73
9.2	DCF	73
9.2.1	Carrier sense mechanism	74
9.2.2	MAC-Level acknowledgments	74
9.2.3	Interframe space (IFS)	75
9.2.4	Random backoff time.....	76
9.2.5	DCF access procedure.....	77
9.2.6	Directed MPDU transfer procedure.....	83
9.2.7	Broadcast and multicast MPDU transfer procedure	84
9.2.8	ACK procedure	84
9.2.9	Duplicate detection and recovery.....	84
9.2.10	DCF timing relations.....	85
9.3	PCF.....	87
9.3.1	CFP structure and timing	88
9.3.2	PCF access procedure	89
9.3.3	PCF transfer procedure	90
9.3.4	Contention-Free polling list	93
9.4	Fragmentation.....	94
9.5	Defragmentation	95
9.6	Multirate support	96
9.7	Frame exchange sequences	97
9.8	MSDU transmission restrictions	98

10.	Layer management.....	100
10.1	Overview of management model	100
10.2	Generic management primitives.....	100
10.3	MLME SAP interface.....	102
10.3.1	Power management	102
10.3.2	Scan.....	103
10.3.3	Synchronization	105
10.3.4	Authenticate	107
10.3.5	De-authenticate	109
10.3.6	Associate	111
10.3.7	Reassociate.....	113
10.3.8	Disassociate.....	115
10.3.9	Reset.....	116
10.3.10	Start	118
10.4	PLME SAP interface	120
10.4.1	PLME-RESET.request.....	120
10.4.2	PLME-DSSSTESTMODE.request	120
10.4.3	PLME-DSSSTESTOUTPUT.request	121
11.	MAC sublayer management entity	123
11.1	Synchronization.....	123
11.1.1	Basic approach	123
11.1.2	Maintaining synchronization	123
11.1.3	Acquiring synchronization, scanning.....	125
11.1.4	Adjusting STA timers	127
11.1.5	Timing synchronization for frequency-hopping (FH) PHYs.....	128
11.2	Power management	128
11.2.1	Power management in an infrastructure network	128
11.2.2	Power management in an IBSS.....	133
11.3	Association and reassociation	136
11.3.1	STA association procedures.....	136
11.3.2	AP association procedures	136
11.3.3	STA reassociation procedures.....	136
11.3.4	AP reassociation procedures	137
11.4	Management information base (MIB) definitions.....	137
11.4.1	MIB summary	137
11.4.2	Managed object class templates.....	139
11.4.3	Attribute group templates	141
11.4.4	Attribute templates.....	142
11.4.5	Notification templates	151
12.	Physical layer (PHY) service specification.....	152
12.1	Scope	152
12.2	PHY functions	152
12.3	Detailed PHY service specifications	152
12.3.1	Scope and field of application.....	152
12.3.2	Overview of the service	152
12.3.3	Overview of interactions.....	152
12.3.4	Basic service and options.....	153
12.3.5	PHY-SAP detailed service specification	154

13.	PHY management	161
13.1	PHY MIB	161
13.1.1	PHY attributes.....	161
13.1.2	PHY object class.....	163
13.1.3	PHY attribute group templates.....	164
13.1.4	PHY attribute templates.....	166
14.	Frequency-Hopping spread spectrum (FHSS) PHY specification for the 2.4 GHz Industrial, Scientific, and Medical (ISM) band	179
14.1	Overview	179
14.1.1	Overview of FHSS PHY.....	179
14.1.2	FHSS PHY functions	179
14.1.3	Service specification method and notation	179
14.2	FHSS PHY specific service parameter lists	180
14.2.1	Overview.....	180
14.2.2	TXVECTOR parameters.....	180
14.2.3	RXVECTOR parameters	181
14.3	FHSS PLCP sublayer	181
14.3.1	Overview.....	181
14.3.2	PLCP frame format	182
14.3.3	PLCP state machines.....	185
14.4	PLME SAP layer management	194
14.4.1	Overview.....	194
14.4.2	FH PHY specific MAC sublayer management entity (MLME) procedures.....	194
14.4.3	FH PHY layer management entity state machines	194
14.5	FHSS PMD sublayer services	197
14.5.1	Scope and field of application.....	197
14.5.2	Overview of services.....	197
14.5.3	Overview of interactions.....	197
14.5.4	Basic service and options.....	197
14.5.5	PMD_SAP detailed service specification	199
14.6	FHSS PMD sublayer, 1.0 Mbit/s.....	203
14.6.1	1 Mbit/s PMD operating specifications, general.....	203
14.6.2	Regulatory requirements.....	203
14.6.3	Operating frequency range.....	204
14.6.4	Number of operating channels	205
14.6.5	Operating channel center frequency	205
14.6.6	Occupied channel bandwidth.....	207
14.6.7	Minimum hop rate.....	207
14.6.8	Hop sequences	208
14.6.9	Unwanted emissions	210
14.6.10	Modulation.....	210
14.6.11	Channel data rate.....	211
14.6.12	Channel switching/settling time.....	211
14.6.13	Receive to transmit switch time	211
14.6.14	PMD transmit specifications.....	212
14.6.15	PMD receiver specifications	213
14.6.16	Operating temperature range.....	214
14.7	FHSS PMD sublayer, 2.0 Mbit/s.....	214
14.7.1	Overview.....	214
14.7.2	Four-Level GFSK modulation	215
14.7.3	Channel data rate.....	216
14.8	FHSS PHY management information base (MIB).....	217

14.8.1	Overview.....	217
14.8.2	FH PHY attributes.....	218
15.	Direct sequence spread spectrum (DSSS) PHY specification for the 2.4 GHz band designated for ISM applications.....	228
15.1	Overview	228
15.1.1	Scope.....	228
15.1.2	DSSS PHY functions	228
15.1.3	Service specification method and notation	229
15.2	DSSS PLCP sublayer	229
15.2.1	Overview.....	229
15.2.2	PLCP frame format	229
15.2.3	PLCP field definitions.....	229
15.2.4	PLCP/DSSS PHY data scrambler and descrambler.....	232
15.2.5	PLCP data modulation and modulation rate change.....	232
15.2.6	PLCP transmit procedure	232
15.2.7	PLCP receive procedure	233
15.3	DSSS physical layer management entity (PLME)	236
15.3.1	PLME_SAP sublayer management primitives	236
15.3.2	DSSS PHY MIB	236
15.4	DSSS PMD sublayer	238
15.4.1	Scope and field of application.....	238
15.4.2	Overview of service.....	238
15.4.3	Overview of interactions.....	239
15.4.4	Basic service and options.....	239
15.4.5	PMD_SAP detailed service specification	241
15.4.6	PMD operating specifications, general	248
15.4.7	PMD transmit specifications.....	251
15.4.8	PMD receiver specifications	255
16.	Infrared (IR) PHY specification.....	257
16.1	Overview	257
16.1.1	Scope.....	258
16.1.2	IR PHY functions.....	258
16.1.3	Service specification method and notation	258
16.2	IR PLCP sublayer.....	259
16.2.1	Overview.....	259
16.2.2	PLCP frame format	259
16.2.3	PLCP modulation and rate change.....	259
16.2.4	PLCP field definitions.....	260
16.2.5	PLCP procedures	261
16.3	IR PMD sublayer.....	263
16.3.1	Overview.....	263
16.3.2	PMD operating specifications, general	263
16.3.3	PMD transmit specifications.....	266
16.3.4	PMD receiver specifications	269
16.3.5	Energy Detect, Carrier Sense, and CCA definitions.....	270
16.4	PHY attributes	271

ANNEXES

Annex A	(normative) Protocol Implementation Conformance Statement (PICS) proforma	273
Annex B	(informative) Hopping sequences	291
Annex C	(normative) Formal description of MAC operation.....	305
Annex D	(normative) ASN.1 encoding of the MAC and PHY MIB	443
Annex E	(informative) Bibliography	445

Contents

1. Overview.....	1
1.1 Scope	1
1.2 Purpose	1
2. Normative references	2
3. Definitions.....	3
4. Abbreviations and acronyms.....	6
5. General description	9
5.1 General description of the architecture	9
5.1.1 How wireless LAN systems are different	9
5.2 Components of the IEEE 802.11 architecture	10
5.2.1 The independent BSS as an ad hoc network	10
5.2.2 Distribution system concepts	11
5.2.3 Area concepts.....	12
5.2.4 Integration with wired LANs.....	14
5.3 Logical service interfaces	14
5.3.1 Station service (SS).....	15
5.3.2 Distribution system service (DSS).....	15
5.3.3 Multiple logical address spaces	16
5.4 Overview of the services	17
5.4.1 Distribution of messages within a DS.....	17
5.4.2 Services that support the distribution service	18
5.4.3 Access and confidentiality control services.....	19
5.5 Relationships between services	21
5.6 Differences between ESS and IBSS LANs	23
5.7 Message information contents that support the services	24
5.7.1 Data	25
5.7.2 Association.....	25
5.7.3 Reassociation	25
5.7.4 Disassociation	26
5.7.5 Privacy	26
5.7.6 Authentication.....	26
5.7.7 Deauthentication	27
5.8 Reference model.....	27
6. MAC service definition.....	29
6.1 Overview of MAC services.....	29
6.1.1 Asynchronous data service	29
6.1.2 Security services	29
6.1.3 MSDU ordering	29
6.2 Detailed service specification.....	30
6.2.1 MAC data services	30
7. Frame formats	34
7.1 MAC frame formats	34

7.1.1	Conventions	34
7.1.2	General frame format	34
7.1.3	Frame fields	35
7.2	Format of individual frame types	41
7.2.1	Control frames	41
7.2.2	Data frames	43
7.2.3	Management frames	45
7.3	Management frame body components	50
7.3.1	Fixed fields	50
7.3.2	Information elements	55
8.	Authentication and privacy	60
8.1	Authentication services	60
8.1.1	Open System authentication	60
8.1.2	Shared Key authentication	61
8.2	The Wired Equivalent Privacy (WEP) algorithm	62
8.2.1	Introduction	62
8.2.2	Properties of the WEP algorithm	63
8.2.3	WEP theory of operation	63
8.2.4	WEP algorithm specification	65
8.2.5	WEP MPDU expansion	65
8.3	Security-Related MIB attributes	66
8.3.1	Authentication-Related MIB attributes	66
8.3.2	Privacy-Related MIB attributes	66
9.	MAC sublayer functional description	71
9.1	MAC architecture	71
9.1.1	Distributed coordination function (DCF)	71
9.1.2	Point coordination function (PCF)	71
9.1.3	Coexistence of DCF and PCF	72
9.1.4	Fragmentation/defragmentation overview	72
9.1.5	MAC data service	73
9.2	DCF	73
9.2.1	Carrier sense mechanism	74
9.2.2	MAC-Level acknowledgments	74
9.2.3	Interframe space (IFS)	75
9.2.4	Random backoff time	76
9.2.5	DCF access procedure	77
9.2.6	Directed MPDU transfer procedure	83
9.2.7	Broadcast and multicast MPDU transfer procedure	84
9.2.8	ACK procedure	84
9.2.9	Duplicate detection and recovery	84
9.2.10	DCF timing relations	85
9.3	PCF	87
9.3.1	CFP structure and timing	88
9.3.2	PCF access procedure	89
9.3.3	PCF transfer procedure	90
9.3.4	Contention-Free polling list	93
9.4	Fragmentation	94
9.5	Defragmentation	95
9.6	Multirate support	96
9.7	Frame exchange sequences	97

9.8	MSDU transmission restrictions	98
10.	Layer management.....	100
10.1	Overview of management model	100
10.2	Generic management primitives.....	100
10.3	MLME SAP interface.....	102
10.3.1	Power management	102
10.3.2	Scan.....	103
10.3.3	Synchronization	105
10.3.4	Authenticate	107
10.3.5	De-authenticate	109
10.3.6	Associate	111
10.3.7	Reassociate.....	113
10.3.8	Disassociate.....	115
10.3.9	Reset.....	116
10.3.10	Start	118
10.4	PLME SAP interface	120
10.4.1	PLME-RESET.request.....	120
10.4.2	PLME-DSSSTESTMODE.request	120
10.4.3	PLME-DSSSTESTOUTPUT.request	121
11.	MAC sublayer management entity	123
11.1	Synchronization.....	123
11.1.1	Basic approach	123
11.1.2	Maintaining synchronization	123
11.1.3	Acquiring synchronization, scanning.....	125
11.1.4	Adjusting STA timers	127
11.1.5	Timing synchronization for frequency-hopping (FH) PHYs.....	128
11.2	Power management	128
11.2.1	Power management in an infrastructure network	128
11.2.2	Power management in an IBSS.....	133
11.3	Association and reassociation	136
11.3.1	STA association procedures.....	136
11.3.2	AP association procedures	136
11.3.3	STA reassociation procedures.....	136
11.3.4	AP reassociation procedures	137
11.4	Management information base (MIB) definitions.....	137
11.4.1	MIB summary	137
11.4.2	Managed object class templates.....	139
11.4.3	Attribute group templates	141
11.4.4	Attribute templates.....	142
11.4.5	Notification templates	151
12.	Physical layer (PHY) service specification.....	152
12.1	Scope	152
12.2	PHY functions	152
12.3	Detailed PHY service specifications	152
12.3.1	Scope and field of application.....	152
12.3.2	Overview of the service	152
12.3.3	Overview of interactions.....	152
12.3.4	Basic service and options.....	153

12.3.5	PHY-SAP detailed service specification	154
13.	PHY management	161
13.1	PHY MIB	161
13.1.1	PHY attributes.....	161
13.1.2	PHY object class.....	163
13.1.3	PHY attribute group templates.....	164
13.1.4	PHY attribute templates.....	166
14.	Frequency-Hopping spread spectrum (FHSS) PHY specification for the 2.4 GHz Industrial, Scientific, and Medical (ISM) band179	
14.1	Overview	179
14.1.1	Overview of FHSS PHY	179
14.1.2	FHSS PHY functions	179
14.1.3	Service specification method and notation	179
14.2	FHSS PHY specific service parameter lists	180
14.2.1	Overview.....	180
14.2.2	TXVECTOR parameters.....	180
14.2.3	RXVECTOR parameters	181
14.3	FHSS PLCP sublayer	181
14.3.1	Overview.....	181
14.3.2	PLCP frame format	182
14.3.3	PLCP state machines.....	185
14.4	PLME SAP layer management	194
14.4.1	Overview.....	194
14.4.2	FH PHY specific MAC sublayer management entity (MLME) procedures.....	194
14.4.3	FH PHY layer management entity state machines	194
14.5	FHSS PMD sublayer services	197
14.5.1	Scope and field of application.....	197
14.5.2	Overview of services.....	197
14.5.3	Overview of interactions.....	197
14.5.4	Basic service and options.....	197
14.5.5	PMD_SAP detailed service specification	199
14.6	FHSS PMD sublayer, 1.0 Mbit/s.....	203
14.6.1	1 Mbit/s PMD operating specifications, general.....	203
14.6.2	Regulatory requirements.....	203
14.6.3	Operating frequency range.....	204
14.6.4	Number of operating channels	205
14.6.5	Operating channel center frequency	205
14.6.6	Occupied channel bandwidth.....	207
14.6.7	Minimum hop rate.....	207
14.6.8	Hop sequences	208
14.6.9	Unwanted emissions	210
14.6.10	Modulation	210
14.6.11	Channel data rate.....	211
14.6.12	Channel switching/settling time.....	211
14.6.13	Receive to transmit switch time	211
14.6.14	PMD transmit specifications.....	212
14.6.15	PMD receiver specifications	213
14.6.16	Operating temperature range.....	214
14.7	FHSS PMD sublayer, 2.0 Mbit/s.....	214
14.7.1	Overview.....	214

14.7.2	Four-Level GFSK modulation	215
14.7.3	Channel data rate.....	216
14.8	FHSS PHY management information base (MIB).....	217
14.8.1	Overview.....	217
14.8.2	FH PHY attributes.....	218
15.	Direct sequence spread spectrum (DSSS) PHY specification for the 2.4 GHz band designated for ISM applications	228
15.1	Overview	228
15.1.1	Scope.....	228
15.1.2	DSSS PHY functions	228
15.1.3	Service specification method and notation	229
15.2	DSSS PLCP sublayer	229
15.2.1	Overview.....	229
15.2.2	PLCP frame format	229
15.2.3	PLCP field definitions.....	229
15.2.4	PLCP/DSSS PHY data scrambler and descrambler.....	232
15.2.5	PLCP data modulation and modulation rate change	232
15.2.6	PLCP transmit procedure	232
15.2.7	PLCP receive procedure	233
15.3	DSSS physical layer management entity (PLME)	236
15.3.1	PLME_SAP sublayer management primitives	236
15.3.2	DSSS PHY MIB	236
15.4	DSSS PMD sublayer	238
15.4.1	Scope and field of application.....	238
15.4.2	Overview of service	238
15.4.3	Overview of interactions.....	239
15.4.4	Basic service and options.....	239
15.4.5	PMD_SAP detailed service specification	241
15.4.6	PMD operating specifications, general	248
15.4.7	PMD transmit specifications.....	251
15.4.8	PMD receiver specifications	255
16.	Infrared (IR) PHY specification.....	257
16.1	Overview	257
16.1.1	Scope.....	258
16.1.2	IR PHY functions.....	258
16.1.3	Service specification method and notation	258
16.2	IR PLCP sublayer.....	259
16.2.1	Overview.....	259
16.2.2	PLCP frame format	259
16.2.3	PLCP modulation and rate change.....	259
16.2.4	PLCP field definitions.....	260
16.2.5	PLCP procedures	261
16.3	IR PMD sublayer.....	263
16.3.1	Overview.....	263
16.3.2	PMD operating specifications, general	263
16.3.3	PMD transmit specifications.....	266
16.3.4	PMD receiver specifications	269
16.3.5	Energy Detect, Carrier Sense, and CCA definitions.....	270
16.4	PHY attributes	271
Annex A		273

Annex B	291
Annex C	305
Annex D	443
Annex E	445

**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

1. Overview

1.1 Scope

The scope of this standard is to develop a medium access control (MAC) and physical layer (PHY) specification for wireless connectivity for fixed, portable, and moving stations within a local area.

1.2 Purpose

The purpose of this standard is to provide wireless connectivity to automatic machinery, equipment, or stations that require rapid deployment, which may be portable or hand-held, or which may be mounted on moving vehicles within a local area. This standard also offers regulatory bodies a means of standardizing access to one or more frequency bands for the purpose of local area communication.

Specifically, this standard

- Describes the functions and services required by an IEEE 802.11 compliant device to operate within ad hoc and infrastructure networks as well as the aspects of station mobility (transition) within those networks.
- Defines the MAC procedures to support the asynchronous MAC service data unit (MSDU) delivery services.
- Defines several PHY signaling techniques and interface functions that are controlled by the IEEE 802.11 MAC.
- Permits the operation of an IEEE 802.11 conformant device within a wireless local area network (LAN) that may coexist with multiple overlapping IEEE 802.11 wireless LANs.
- Describes the requirements and procedures to provide privacy of user information being transferred over the wireless medium (WM) and authentication of IEEE 802.11 conformant devices.

2. Normative references

The following standards contain provisions which, through references in this text, constitute provisions of this standard. At the time of publication, the editions indicated were valid. All standards are subject to revision, and parties to agreements based on this standard are encouraged to investigate the possibility of applying the most recent editions of the standards listed below.

IEEE Std 802-1990, IEEE Standards for Local and Metropolitan Area Networks: Overview and Architecture (ANSI).¹

IEEE Std C95.1-1991, IEEE Standard Safety Levels with Respect to Human Exposure to Radio Frequency Electromagnetic Fields, 3 kHz to 300 GHz (ANSI).

ISO/IEC 7498-1: 1994, Information technology—Open Systems Interconnection—Basic Reference Model: The Basic Model.²

ISO/IEC 8802-2: 1994, Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements—Part 2: Logical link control.

ISO/IEC 8824-1: 1995, Information technology—Abstract Syntax Notation One (ASN.1): Specification of basic notation.

ISO/IEC 8824-1: 1995/Amd.1: 1996, Information technology—Abstract Syntax Notation One (ASN.1): Specification of basic notation, Amendment 1: Rules of extensibility.

ISO/IEC 8824-2: 1995, Information technology—Abstract Syntax Notation One (ASN.1): Information object specification.

ISO/IEC 8824-2: 1995/Amd.1: 1996, Information technology—Abstract Syntax Notation One (ASN.1): Information object specification, Amendment 1: Rules of extensibility.

ISO/IEC 8824-3: 1995, Information technology—Abstract Syntax Notation One (ASN.1): Constraint specification.

ISO/IEC 8824-4: 1995, Information technology—Abstract Syntax Notation One (ASN.1): Parameterization of ASN.1 specifications.

ISO/IEC 8825-1: 1995, Information technology—ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER).

ISO/IEC 8825-2: 1996, Information technology—ASN.1 encoding rules: Specification of Packed Encoding Rules (PER).

ISO/IEC 10039: 1991, Information technology—Open systems interconnection—Local area networks—Medium Access Control (MAC) service definition.

¹IEEE publications are available from the Institute of Electrical and Electronics Engineers, 445 Hoes Lane, P.O. Box 1331, Piscataway, NJ 08855-1331, USA.

²ISO publications are available from the ISO Central Secretariat, Case Postale 56, 1 rue de Varembe, CH-1211, Genève 20, Switzerland/Suisse. ISO publications are also available in the United States from the Sales Department, American National Standards Institute, 11 West 42nd Street, 13th Floor, New York, NY 10036, USA.

ISO/IEC 15802-1: 1995, Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Common specifications—Part 1: Medium Access Control (MAC) service definition.

ITU Radio Regulations, volumes 1–4.³

ITU-T Recommendation X.210 (11/93), Information technology—Open systems interconnection—Basic Reference Model: Conventions for the definition of OSI services (*common text with ISO/IEC*).

ITU-T Recommendation Z.100 (03/93), CCITT specification and description language (SDL).

ITU-T Recommendation Z.105 (03/95), SDL combined with ASN.1 (SDL/ASN.1).

3. Definitions

3.1 access control: The prevention of unauthorized usage of resources.

3.2 access point (AP): Any entity that has station functionality and provides access to the distribution services, via the wireless medium (WM) for associated stations.

3.3 ad hoc network: A network composed solely of stations within mutual communication range of each other via the wireless medium (WM). An ad hoc network is typically created in a spontaneous manner. The principal distinguishing characteristic of an ad hoc network is its limited temporal and spatial extent. These limitations allow the act of creating and dissolving the ad hoc network to be sufficiently straightforward and convenient so as to be achievable by nontechnical users of the network facilities; i.e., no specialized “technical skills” are required and little or no investment of time or additional resources is required beyond the stations that are to participate in the ad hoc network. The term *ad hoc* is often used as slang to refer to an independent basic service set (IBSS).

3.4 association: The service used to establish access point/station (AP/STA) mapping and enable STA invocation of the distribution system services (DSSs).

3.5 authentication: The service used to establish the identity of one station as a member of the set of stations authorized to associate with another station.

3.6 basic service area (BSA): The conceptual area within which members of a basic service set (BSS) may communicate.

3.7 basic service set (BSS): A set of stations controlled by a single coordination function (CF).

3.8 basic service set (BSS) basic rate set: The set of data transfer rates that all the stations in a BSS will be capable of using to receive frames from the wireless medium (WM). The BSS basic rate set data rates are preset for all stations in the BSS.

3.9 broadcast: The broadcast address is a unique multicast address that specifies all stations.

3.10 channel: An instance of medium use for the purpose of passing protocol data units (PDUs) that may be used simultaneously, in the same volume of space, with other instances of medium use (on other channels) by other instances of the same physical layer (PHY), with an acceptably low frame error ratio due to mutual

³ITU publications are available from the International Telecommunications Union, Sales Section, Place des Nations, CH-1211, Genève 20, Switzerland/Suisse. They are also available in the United States from the U.S. Department of Commerce, Technology Administration, National Technical Information Service (NTIS), Springfield, VA 22161, USA.

interference. Some PHYs provide only one channel, whereas others provide multiple channels. Examples of channel types are as shown in the following table:

Single channel	n-channel
Narrowband radio-frequency (RF) channel	Frequency division multiplexed channels
Baseband infrared	Direct sequence spread spectrum (DSSS) with code division multiple access

3.11 clear channel assessment (CCA) function: That logical function in the physical layer (PHY) that determines the current state of use of the wireless medium (WM).

3.12 confidentiality: The property of information that is not made available or disclosed to unauthorized individuals, entities, or processes.

3.13 coordination function: The logical function that determines when a station operating within a basic service set (BSS) is permitted to transmit and may be able to receive protocol data units (PDUs) via the wireless medium (WM). The coordination function within a BSS may have one point coordination function (PCF) and will have one distributed coordination function (DCF).

3.14 coordination function (CF)-Pollable: A station able (1) to respond to a CF Poll with a data frame, if such a frame is queued and able to be generated, and (2) to interpret acknowledgments in frames sent to or from the point coordinator.

3.15 deauthentication: The service that voids an existing authentication relationship.

3.16 directed address: *See:* unicast frame.

3.17 disassociation: The service that removes an existing association.

3.18 distributed coordination function (DCF): A class of coordination function where the same coordination function logic is active in every station in the basic service set (BSS) whenever the network is in operation.

3.19 distribution: The service that, by using association information, delivers medium access control (MAC) service data units (MSDUs) within the distribution system (DS).

3.20 distribution system (DS): A system used to interconnect a set of basic service sets (BSSs) and integrated local area networks (LANs) to create an extended service set (ESS).

3.21 distribution system medium (DSM): The medium or set of media used by a distribution system (DS) for communications between access points (APs) and portals of an extended service set (ESS).

3.22 distribution system service (DSS): The set of services provided by the distribution system (DS) that enable the medium access control (MAC) to transport MAC service data units (MSDUs) between stations that are not in direct communication with each other over a single instance of the wireless medium (WM). These services include transport of MSDUs between the access points (APs) of basic service sets (BSSs) within an extended service set (ESS), transport of MSDUs between portals and BSSs within an ESS, and transport of MSDUs between stations in the same BSS in cases where the MSDU has a multicast or broadcast destination address or where the destination is an individual address, but the station sending the MSDU chooses to involve DSS. DSSs are provided between pairs of IEEE 802.11 MACs.

3.23 extended rate set (ERS): The set of data transfer rates supported by a station (if any) beyond the extended service set (ESS) basic rate set. This set may include data transfer rates that will be defined in future physical layer (PHY) standards.

3.24 extended service area (ESA): The conceptual area within which members of an extended service set (ESS) may communicate. An ESA is larger than or equal to a basic service area (BSA) and may involve several basic service sets (BSSs) in overlapping, disjointed, or both configurations.

3.25 extended service set (ESS): A set of one or more interconnected basic service sets (BSSs) and integrated local area networks (LANs) that appear as a single BSS to the logical link control layer at any station associated with one of those BSSs.

3.26 Gaussian frequency shift keying (GFSK): A modulation scheme where the data is first filtered by a Gaussian filter in the baseband and then modulated with a simple frequency modulation.

3.27 independent basic service set (IBSS): A BSS that forms a self-contained network, and in which no access to a distribution system (DS) is available.

3.28 infrastructure: The infrastructure includes the distribution system medium (DSM), access point (AP), and portal entities. It is also the logical location of distribution and integration service functions of an extended service set (ESS). An infrastructure contains one or more APs and zero or more portals in addition to the distribution system (DS).

3.29 integration: The service that enables delivery of medium access control (MAC) service data units (MSDUs) between the distribution system (DS) and an existing, non-IEEE 802.11 local area network (via a portal).

3.30 medium access control (MAC) management protocol data unit (MMPDU): The unit of data exchanged between two peer MAC entities to implement the MAC management protocol.

3.31 medium access control (MAC) protocol data unit (MPDU): The unit of data exchanged between two peer MAC entities using the services of the physical layer (PHY).

3.32 medium access control (MAC) service data unit (MSDU): Information that is delivered as a unit between MAC service access points (SAPs).

3.33 minimally conformant network: An IEEE 802.11 network in which two stations in a single basic service area (BSA) are conformant with IEEE 802.11.

3.34 mobile station: A type of station that uses network communications while in motion.

3.35 multicast: A medium access control (MAC) address that has the group bit set. A multicast medium access control (MAC) service data unit (MSDU) is one with a multicast destination address. A multicast MPDU or control frame is one with a multicast receiver address.

3.36 network allocation vector (NAV): An indicator, maintained by each station, of time periods when transmission onto the wireless medium (WM) will not be initiated by the station whether or not the station's clear channel assessment (CCA) function senses the WM is busy.

3.37 point coordination function (PCF): A class of possible coordination functions where the coordination function logic is active in only one station in a basic service set (BSS) at any given time that the network is in operation.

3.38 portable station: A type of station that may be moved from location to location, but only uses network communications while at a fixed location.

3.39 portal: The logical point at which medium access control (MAC) service data units (MSDUs) from a non-IEEE 802.11 local area network (LAN) enter the distribution system (DS) of an extended service set (ESS).

3.40 privacy: The service used to prevent the content of messages from being read by other than the intended recipients.

3.41 reassociation: The service that enables an established association [between access point (AP) and station (STA)] to be transferred from one AP to another (or the same) AP.

3.42 station (STA): Any device that contains an IEEE 802.11 conformant medium access control (MAC) and physical layer (PHY) interface to the wireless medium (WM).

3.43 station basic rate: A data transfer rate belonging to the extended service set (ESS) basic rate set that is used by a station for specific transmissions. The station basic rate may change dynamically as frequently as each medium access control (MAC) protocol data unit (MPDU) transmission attempt, based on local considerations at that station.

3.44 station service (SS): The set of services that support transport of medium access control (MAC) service data units (MSDUs) between stations within a basic service set (BSS).

3.45 time unit (TU): A measurement of time equal to 1024 μ s.

3.46 unauthorized disclosure: The process of making information available to unauthorized individuals, entities, or processes.

3.47 unauthorized resource use: Use of resource not consistent with the defined security policy.

3.48 unicast frame: A frame that is addressed to a single recipient, not a broadcast or multicast frame. *Syn:* directed address.

3.49 wired equivalent privacy (WEP): The optional cryptographic confidentiality algorithm specified by IEEE 802.11 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.

3.50 wireless medium (WM): The medium used to implement the transfer of protocol data units (PDUs) between peer physical layer (PHY) entities of a wireless local area network (LAN).

4. Abbreviations and acronyms

ACK	acknowledgment
AID	association identifier
AP	access point
ATIM	announcement traffic indication message
BSA	basic service area
BSS	basic service set
BSSID	basic service set identification
CCA	clear channel assessment
CF	contention free
CFP	contention-free period

CID	connection identifier
CP	contention period
CRC	cyclic redundancy code
CS	carrier sense
CTS	clear to send
CW	contention window
DA	destination address
DBPSK	differential binary phase shift keying
DCE	data communication equipment
DCF	distributed coordination function
DCLA	direct current level adjustment
DIFS	distributed (coordination function) interframe space
DLL	data link layer
Dp	desensitization
DQPSK	differential quadrature phase shift keying
DS	distribution system
DSAP	destination service access point
DSM	distribution system medium
DSS	distribution system service
DSSS	direct sequence spread spectrum
DTIM	delivery traffic indication message
ED	energy detection
EIFS	extended interframe space
EIRP	equivalent isotropically radiated power
ERS	extended rate set
ESA	extended service area
ESS	extended service set
FC	frame control
FCS	frame check sequence
FER	frame error ratio
FH	frequency hopping
FHSS	frequency-hopping spread spectrum
GFSK	Gaussian frequency shift keying
IBSS	independent basic service set
ICV	integrity check value
IDU	interface data unit
IFS	interframe space
IMp	intermodulation protection
IR	infrared (PHY)
ISM	industrial, scientific, and medical
IV	initialization vector
LLC	logical link control
LME	layer management entity
LRC	long retry count
lsb	least significant bit
MAC	medium access control
MDF	management-defined field
MIB	management information base
MLME	MAC sublayer management entity
MMPDU	MAC management protocol data unit
MPDU	MAC protocol data unit
msb	most significant bit
MSDU	MAC service data unit
NAV	network allocation vector

PC	point coordinator
PCF	point coordination function
PDU	protocol data unit
PHY	physical (layer)
PHY-SAP	physical layer service access point
PIFS	point (coordination function) interframe space
PLCP	physical layer convergence protocol
PLME	physical layer management entity
PMD	physical medium dependent
PMD-SAP	physical medium dependent service access point
PN	pseudonoise (PN code sequence)
PPDU	PLCP protocol data unit
ppm	parts per million
PPM	pulse position modulation
PRNG	pseudorandom number generator
PS	power save (mode)
PSDU	PLCP SDU
RA	receiver address
RF	radio frequency
RSSI	received signal strength indication
RTS	request to send
RX	receive or receiver
SA	source address
SAP	service access point
SDU	service data unit
SFD	start frame delimiter
SIFS	short interframe space
SLRC	station long retry count
SME	station management entity
SMT	station management
SQ	signal quality (PN code correlation strength)
SRC	short retry count
SS	station service
SSAP	source service access point
SSID	service set identifier
SSRC	station short retry count
STA	station
TA	transmitter address
TBTT	target beacon transmission time
TIM	traffic indication map
TSF	timing synchronization function
TU	time unit
TX	transmit or transmitter
TXE	transmit enable
WAN	wide area network
WDM	wireless distribution media
WDS	wireless distribution system
WEP	wired equivalent privacy
WM	wireless medium

5. General description

5.1 General description of the architecture

This subclause presents the concepts and terminology used within IEEE Std 802.11-1997 (referred to throughout the text as IEEE 802.11). Specific terms are defined in Clause 3. Illustrations convey key IEEE 802.11 concepts and the interrelationships of the architectural components. IEEE 802.11 uses an architecture to describe functional components of an IEEE 802.11 LAN. The architectural descriptions are not intended to represent any specific physical implementation of IEEE 802.11.

5.1.1 How wireless LAN systems are different

Wireless networks have fundamental characteristics that make them significantly different from traditional wired LANs.

5.1.1.1 Destination address does not equal destination location

In wired LANs, an address is equivalent to a physical location. This is implicitly assumed in the design of wired LANs. In IEEE 802.11, the addressable unit is a station (STA). The STA is a message destination, but not (in general) a fixed location.

5.1.1.2 The media impact the design

The physical layers used in IEEE 802.11 are fundamentally different from wired media. Thus IEEE 802.11 PHYs

- a) Use a medium that has neither absolute nor readily observable boundaries outside of which stations with conformant PHY transceivers are known to be unable to receive network frames.
- b) Are unprotected from outside signals.
- c) Communicate over a medium significantly less reliable than wired PHYs.
- d) Have dynamic topologies.
- e) Lack full connectivity, and therefore the assumption normally made that every STA can hear every other STA is invalid (that is, STAs may be “hidden” from each other).
- f) Have time-varying and asymmetric propagation properties.

Because of limitations on wireless PHY ranges, wireless LANs intended to cover reasonable geographic distances may be built from basic coverage building blocks.

5.1.1.3 The impact of handling mobile stations

One of the requirements of IEEE 802.11 is to handle *mobile* as well as *portable* stations. A *portable* station is one that is moved from location to location, but is only used while at a fixed location. *Mobile* stations actually access the LAN while in motion.

For technical reasons, it is not sufficient to handle only portable stations. Propagation effects blur the distinction between portable and mobile stations; stationary stations often appear to be mobile due to propagation effects.

Another aspect of mobile stations is that they may often be battery powered. Hence power management is an important consideration. For example, it cannot be presumed that a station's receiver will always be powered on.

5.1.1.4 Interaction with other IEEE 802 layers

IEEE 802.11 is required to appear to higher layers [logical link control (LLC)] as a current style 802 LAN. This requires that the IEEE 802.11 network handle station mobility within the MAC sublayer. To meet reliability assumptions (that LLC makes about lower layers), it is necessary for IEEE 802.11 to incorporate functionality that is untraditional for MAC sublayers.

5.2 Components of the IEEE 802.11 architecture

The IEEE 802.11 architecture consists of several components that interact to provide a wireless LAN that supports station mobility transparently to upper layers.

The *basic service set* (BSS) is the basic building block of an IEEE 802.11 LAN. Figure 1 shows two BSSs, each of which has two stations that are members of the BSS.

It is useful to think of the ovals used to depict a BSS as the coverage area within which the member stations of the BSS may remain in communication. (The concept of area, while not precise, is often good enough.) If a station moves out of its BSS, it can no longer directly communicate with other members of the BSS.

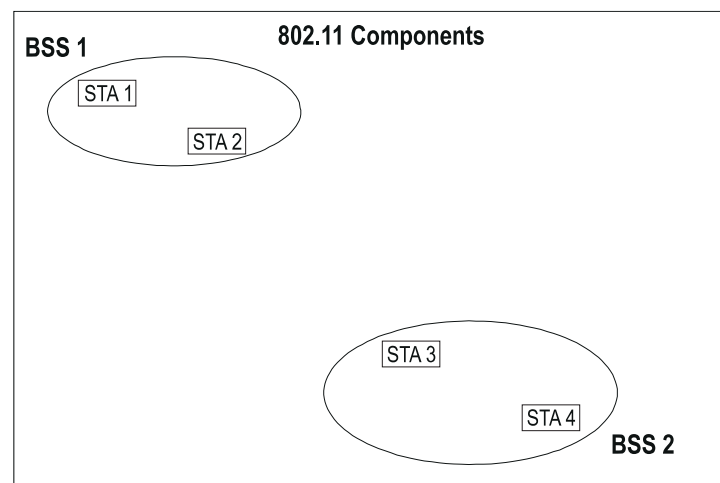


Figure 1—Basic service sets

5.2.1 The independent BSS as an ad hoc network

The independent BSS (IBSS) is the most basic type of IEEE 802.11 LAN. A minimum IEEE 802.11 LAN may consist of only two stations.

Figure 1 shows two IBSSs. This mode of operation is possible when IEEE 802.11 stations are able to communicate directly. Because this type of IEEE 802.11 LAN is often formed without pre-planning, for only as long as the LAN is needed, this type of operation is often referred to as an *ad hoc network*.

5.2.1.1 STA to BSS association is dynamic

The association between a STA and a BSS is dynamic (STAs turn on, turn off, come within range, and go out of range). To become a member of an infrastructure BSS, a station shall become “associated.” These associations are dynamic and involve the use of the distribution system service (DSS), which is described later.

5.2.2 Distribution system concepts

PHY limitations determine the direct station-to-station distance that may be supported. For some networks this distance is sufficient; for other networks, increased coverage is required.

Instead of existing independently, a BSS may also form a component of an extended form of network that is built with multiple BSSs. The architectural component used to interconnect BSSs is the *distribution system* (DS).

IEEE 802.11 logically separates the wireless medium (WM) from the distribution system medium (DSM). Each logical medium is used for different purposes, by a different component of the architecture. The IEEE 802.11 definitions neither preclude, nor demand, that the multiple media be either the same or different.

Recognizing that the multiple media are *logically* different is key to understanding the flexibility of the architecture. The IEEE 802.11 LAN architecture is specified independently of the physical characteristics of any specific implementation.

The DS enables mobile device support by providing the logical services necessary to handle address to destination mapping and seamless integration of multiple BSSs.

An *access point* (AP) is a STA that provides access to the DS by providing DS services in addition to acting as a STA.

Figure 2 adds the DS and AP components to the IEEE 802.11 architecture picture.

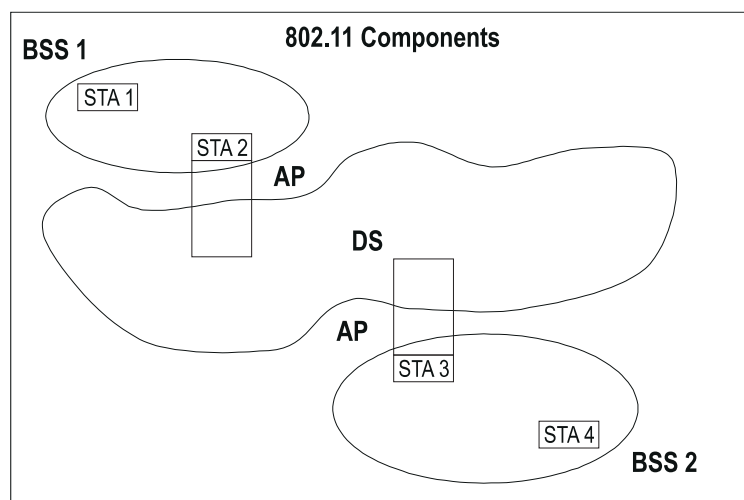


Figure 2—Distribution systems and access points

Data move between a BSS and the DS via an AP. Note that all APs are also STAs; thus they are addressable entities. The addresses used by an AP for communication on the WM and on the DSM are not necessarily the same.

5.2.2.1 Extended service set (ESS): The large coverage network

The DS and BSSs allow IEEE 802.11 to create a wireless network of arbitrary size and complexity. IEEE 802.11 refers to this type of network as the *extended service set* (ESS) network.

The key concept is that the ESS network appears the same to an LLC layer as an IBSS network. Stations within an ESS may communicate and mobile stations may move from one BSS to another (within the same ESS) transparently to LLC.

Nothing is assumed by IEEE 802.11 about the relative physical locations of the BSSs in Figure 3.

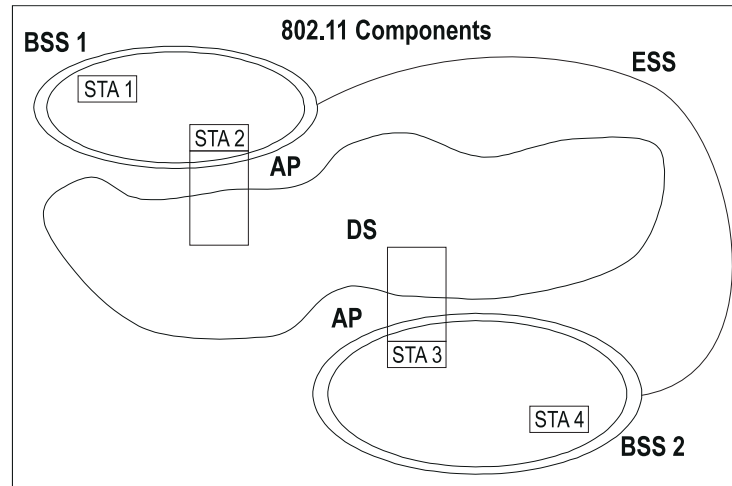


Figure 3—Extended service set

All of the following are possible:

- The BSSs may partially overlap. This is commonly used to arrange contiguous coverage within a physical volume.
- The BSSs could be physically disjointed. Logically there is no limit to the distance between BSSs.
- The BSSs may be physically collocated. This may be done to provide redundancy.
- One (or more) IBSS or ESS networks may be physically present in the same space as one (or more) ESS networks. This may arise for a number of reasons. Two of the most common are when an ad hoc network is operating in a location that also has an ESS network, and when physically overlapping IEEE 802.11 networks have been set up by different organizations.

5.2.3 Area concepts

For wireless PHYs, well-defined coverage areas simply do not exist. Propagation characteristics are dynamic and unpredictable. Small changes in position or direction may result in dramatic differences in signal strength. Similar effects occur whether a station is stationary or mobile (as moving objects may impact station-to-station propagation).

Figure 4 shows a signal strength map for a simple square room with a standard metal desk and an open doorway. Figure 4 is a static snapshot; the propagation patterns change dynamically as stations and objects in the environment move. In Figure 4 the dark (solid) blocks in the lower left are a metal desk and there is a doorway at the top right of the figure. The figure indicates relative differences in field strength with different intensities and indicates the variability of field strength even in a static environment.

While the architecture diagrams show sharp boundaries for BSSs, this is an artifact of the pictorial representation, not a physical reality. Since dynamic three-dimensional field strength pictures are difficult to draw, well-defined shapes are used by IEEE 802.11 architectural diagrams to represent the coverage of a BSS.

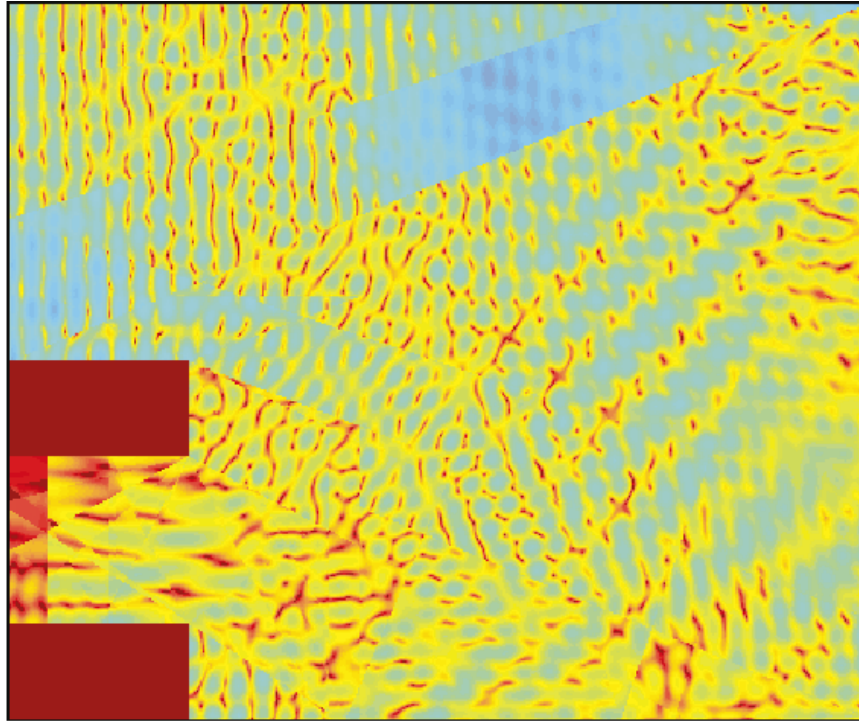


Figure 4—A representative signal intensity map

Further description difficulties arise when attempting to describe collocated coverage areas. Consider Figure 5, in which STA 6 could belong to BSS 2 or BSS 3.

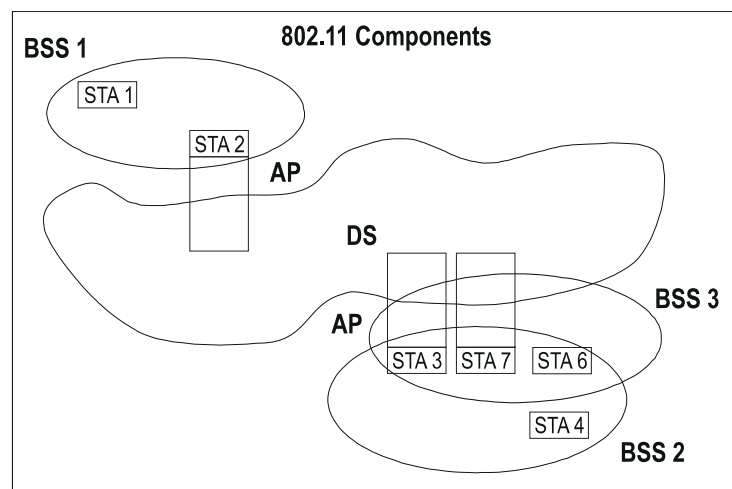


Figure 5—Collocated coverage areas

While the concept of sets of stations is correct, it is often convenient to talk about areas. For many topics the concept of area is sufficient. *Volume* is a more precise term than area, though still not technically correct. For historical reasons and convenience, this standard uses the common term *area*.

5.2.4 Integration with wired LANs

To integrate the IEEE 802.11 architecture with a traditional wired LAN, a final *logical* architectural component is introduced—a *portal*.

A portal is the logical point at which MSDUs from an integrated non-IEEE 802.11 LAN enter the IEEE 802.11 DS. For example, a portal is shown in Figure 6 connecting to a wired 802 LAN.

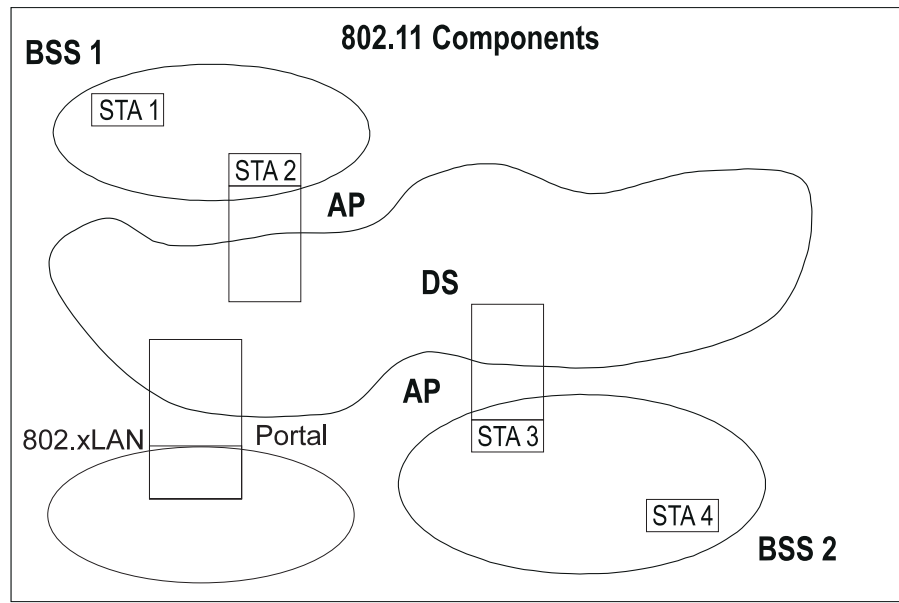


Figure 6—Connecting to other IEEE 802 LANs

All data from non-IEEE 802.11 LANs enter the 802.11 architecture via a portal. The portal provides logical integration between the IEEE 802.11 architecture and existing wired LANs. It is possible for one device to offer both the functions of an AP and a portal; this could be the case when a DS is implemented from 802 LAN components.

In IEEE 802.11, the ESS architecture (APs and the DS) provides traffic segmentation and range extension. Logical connections between IEEE 802.11 and other LANs are via the portal. Portals connect between the DSM and the LAN medium that is to be integrated.

5.3 Logical service interfaces

The IEEE 802.11 architecture allows for the possibility that the DS may not be identical to an existing wired LAN. A DS may be created from many different technologies including current 802 wired LANs. IEEE 802.11 does not constrain the DS to be either data link or network layer based. Nor does IEEE 802.11 constrain a DS to be either centralized or distributed in nature.

IEEE 802.11 explicitly does not specify the details of DS implementations. Instead, IEEE 802.11 specifies *services*. The services are associated with different components of the architecture. There are two categories of IEEE 802.11 service—the station service (SS) and the distribution system service (DSS). Both categories of service are used by the IEEE 802.11 MAC sublayer.

The complete set of IEEE 802.11 architectural services are as follows:

- a) Authentication
- b) Association
- c) Deauthentication
- d) Disassociation
- e) Distribution
- f) Integration
- g) Privacy
- h) Reassociation
- i) MSDU delivery

This set of services is divided into two groups: those that are part of every station, and those that are part of a DS.

5.3.1 Station service (SS)

The service provided by stations is known as the *station service*.

The SS is present in every IEEE 802.11 station (including APs, as APs include station functionality). The SS is specified for use by MAC sublayer entities. All conformant stations provide SS.

The SS is as follows:

- a) Authentication
- b) Deauthentication
- c) Privacy
- d) MSDU delivery

5.3.2 Distribution system service (DSS)

The service provided by the DS is known as the *distribution system service*.

These services are represented in the IEEE 802.11 architecture by arrows within the APs, indicating that the services are used to cross media and address space logical boundaries. This is the convenient place to show the services in the picture. The physical embodiment of various services may or may not be within a physical AP.

The DSSs are provided by the DS. They are accessed via a STA that also provides DSSs. A STA that is providing access to DSS is an AP.

The DSSs are as follows:

- a) Association
- b) Disassociation
- c) Distribution
- d) Integration
- e) Reassociation

DSSs are specified for use by MAC sublayer entities.

Figure 7 combines the components from previous figures with both types of services to show the complete IEEE 802.11 architecture.

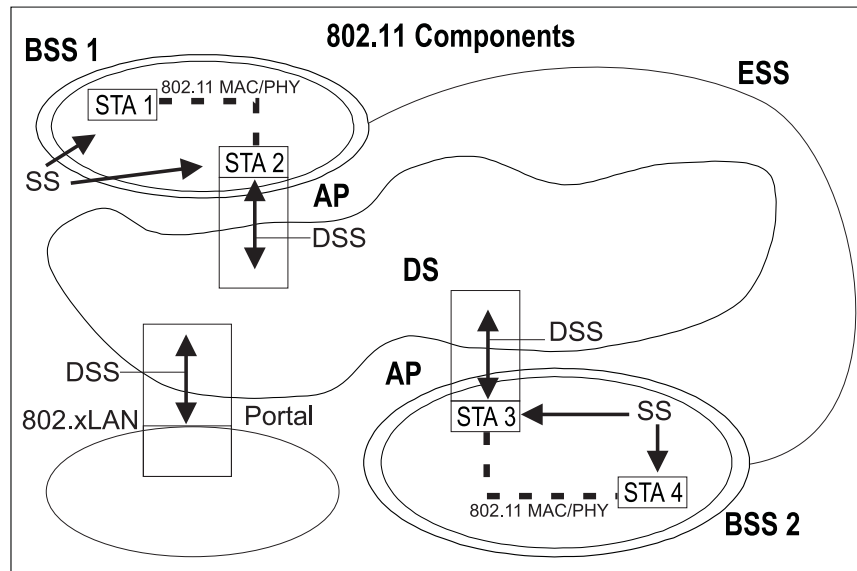


Figure 7—Complete IEEE 802.11 architecture

5.3.3 Multiple logical address spaces

Just as the IEEE 802.11 architecture allows for the possibility that the WM, DSM, and an integrated wired LAN may all be different physical media, it also allows for the possibility that each of these components may be operating within different address spaces. IEEE 802.11 only uses and specifies the use of the WM address space.

Each IEEE 802.11 PHY operates in a single medium—the WM. The IEEE 802.11 MAC operates in a single address space. MAC addresses are used on the WM in the IEEE 802.11 architecture. Therefore, it is unnecessary for the standard to explicitly specify that its addresses are “WM addresses.” This is assumed throughout the IEEE 802.11 standard.

IEEE 802.11 has chosen to use the IEEE 802 48-bit address space (see 7.1.3.3.1). Thus IEEE 802.11 addresses are compatible with the address space used by the 802 LAN family.

The IEEE 802.11 choice of address space implies that for many instantiations of the IEEE 802.11 architecture, the wired LAN MAC address space and the IEEE 802.11 MAC address space may be the same. In those situations where a DS that uses MAC level 802 addressing is appropriate, all three of the logical address spaces used within a system could be identical. While this is a common case, it is not the only combination allowed by the architecture. The IEEE 802.11 architecture allows for all three logical address spaces to be distinct.

A multiple address space example is one where the DS implementation uses network layer addressing. In this case, the WM address space and the DS address space would be different.

The ability of the architecture to handle multiple logical media and address spaces is key to the ability of IEEE 802.11 to be independent of the DS implementation and to interface cleanly with network layer mobility approaches. The implementation of the DS is unspecified and is beyond the scope of this standard.

5.4 Overview of the services

There are nine services specified by IEEE 802.11. Six of the services are used to support MSDU delivery between STAs. Three of the services are used to control IEEE 802.11 LAN access and confidentiality.

This subclause presents the services, an overview of how each service is used, and a description of how the service relates to other services and the IEEE 802.11 architecture. The services are presented in an order designed to help build an understanding of the operation of an IEEE 802.11 ESS network. As a result, the SSSs and DSSs are intermixed in order (rather than being grouped by category).

Each of the services is supported by one or more MAC frame types. Some of the services are supported by MAC management messages and some by MAC data messages. All of the messages gain access to the WM via the IEEE 802.11 MAC sublayer medium access method specified in Clause 9 of this standard.

The IEEE 802.11 MAC sublayer uses three types of messages—*data*, *management*, and *control* (see Clause 7). The data messages are handled via the MAC data service path.

MAC management messages are used to support the IEEE 802.11 services and are handled via the MAC management service data path.

MAC control messages are used to support the delivery of IEEE 802.11 data and management messages.

The examples here assume an ESS network environment. The differences between the ESS and the IBSS network environments are discussed separately in 5.6.

5.4.1 Distribution of messages within a DS

5.4.1.1 Distribution

This is the primary service used by IEEE 802.11 stations. It is conceptually invoked by every data message to or from an IEEE 802.11 STA operating in an ESS (when the frame is sent via the DS). Distribution is a DSS.

Refer to the ESS network in Figure 7 and consider a data message being sent from STA 1 to STA 4. The message is sent from STA 1 and received by STA 2 (the “input” AP). The AP gives the message to the distribution service of the DS.

It is the job of the distribution service to deliver the message within the DS in such a way that it arrives at the appropriate DS destination for the intended recipient.

In this example, the message is distributed to STA 3 (the “output” AP) and STA 3 accesses the WM to send the message to STA 4 (the intended destination).

How the message is distributed within the DS is not specified by IEEE 802.11. All IEEE 802.11 is required to do is to provide the DS with enough information for the DS to be able to determine the “output” point that corresponds to the desired recipient. The necessary information is provided to the DS by the three association related services (association, reassociation, and disassociation).

The previous example was a case where the AP that invoked the distribution service was different from the AP that received the distributed message. If the message had been intended for a station that was a member of the same BSS as the sending station, then the “input” and “output” APs for the message would have been the same.

In either example, the distribution service was logically invoked. Whether the message actually had to traverse the physical DSM or not is a DS implementation matter and is not specified by IEEE 802.11.

While IEEE 802.11 does not specify DS implementations, it does recognize and support the use of the WM as the DSM. This is specifically supported by the IEEE 802.11 frame formats. (Refer to Clause 7 for details.)

5.4.1.2 Integration

If the distribution service determines that the intended recipient of a message is a member of an integrated LAN, the “output” point of the DS would be a portal instead of an AP.

Messages that are distributed to a portal cause the DS to invoke the Integration function (conceptually after the distribution service). The Integration function is responsible for accomplishing whatever is needed to deliver a message from the DSM to the integrated LAN media (including any required media or address space translations). Integration is a DSS.

Messages received from an integrated LAN (via a portal) by the DS for an IEEE 802.11 STA will invoke the Integration function before the message is distributed by the distribution service.

The details of an Integration function are dependent on a specific DS implementation and are outside the scope of this standard.

5.4.2 Services that support the distribution service

The primary purpose of a MAC sublayer is to transfer MSDUs between MAC sublayer entities. The information required for the distribution service to operate is provided by the association services. Before a data message can be handled by the distribution service, a STA shall be “associated.”

To understand the concept of association, it is necessary first to understand the concept of *mobility*.

5.4.2.1 Mobility types

There are three transition types of significance to this standard that describe the mobility of stations within a network:

- a) **No-transition:** In this type, two subclasses that are usually indistinguishable are identified:
 - 1) Static—no motion.
 - 2) Local movement—movement within the PHY range of the communicating STAs [i.e., movement within a basic service area (BSA)].
- b) **BSS-transition:** This type is defined as a station movement from one BSS in one ESS to another BSS within the same ESS.
- c) **ESS-transition:** This type is defined as station movement from a BSS in one ESS to a BSS in a different ESS. This case is supported only in the sense that the STA may move. Maintenance of upper-layer connections cannot be guaranteed by IEEE 802.11; in fact, disruption of service is likely to occur.

The different association services support the different categories of mobility.

5.4.2.2 Association

To deliver a message within a DS, the distribution service needs to know which AP to access for the given IEEE 802.11 STA. This information is provided to the DS by the concept of *association*. Association is necessary, but not sufficient, to support BSS-transition mobility. Association is sufficient to support “no-transition” mobility. Association is a DSS.

Before a STA is allowed to send a data message via an AP, it shall first become associated with the AP. The act of becoming associated invokes the association service, which provides the STA to AP mapping to the DS. The DS uses this information to accomplish its message distribution service. How the information provided by the association service is stored and managed within the DS is not specified by this standard.

At any given instant, a STA may be associated with no more than one AP. This ensures that the DS may determine a unique answer to the question, “which AP is serving STA X?” Once an association is completed, a STA may make full use of a DS (via the AP) to communicate. Association is always initiated by the mobile STA, not the AP.

An AP may be associated with many STAs at one time.

A STA learns what APs are present and then requests to establish an association by invoking the association service. For the details of how a station learns about what APs are present, see 11.1.3 on scanning.

5.4.2.3 Reassociation

Association is sufficient for no-transition message delivery between IEEE 802.11 stations. Additional functionality is needed to support BSS-transition mobility. The additional required functionality is provided by the reassociation service. Reassociation is a DSS.

The reassociation service is invoked to “move” a current association from one AP to another. This keeps the DS informed of the current mapping between AP and STA as the station moves from BSS to BSS within an ESS. Reassociation also enables changing association attributes of an established association while the STA remains associated with the same AP. Reassociation is always initiated by the mobile STA.

5.4.2.4 Disassociation

The disassociation service is invoked whenever an existing association is to be terminated. Disassociation is a DSS.

In an ESS, this tells the DS to void existing association information. Attempts to send messages via the DS to a disassociated STA will be unsuccessful.

The disassociation service may be invoked by either party to an association (non-AP STA or AP). Disassociation is a notification, not a request. Disassociation cannot be refused by either party to the association.

APs may need to disassociate STAs to enable the AP to be removed from a network for service or for other reasons.

STAs shall attempt to disassociate whenever they leave a network. However, the MAC protocol does not depend on STAs invoking the disassociation service. (MAC management is designed to accommodate loss of an associated STA.)

5.4.3 Access and confidentiality control services

Two services are required for IEEE 802.11 to provide functionality equivalent to that which is inherent to wired LANs. The design of wired LANs assumes the physical attributes of wire. In particular, wired LAN design assumes the physically closed and controlled nature of wired media. The physically open medium nature of an IEEE 802.11 LAN violates those assumptions.

Two services are provided to bring the IEEE 802.11 functionality in line with wired LAN assumptions; authentication and privacy. *Authentication* is used instead of the wired media physical connection. *Privacy* is used to provide the confidential aspects of closed wired media.

5.4.3.1 Authentication

In wired LANs, physical security can be used to prevent unauthorized access. This is impractical in wireless LANs since they have a medium without precise bounds.

IEEE 802.11 provides the ability to control LAN access via the authentication service. This service is used by all stations to establish their identity to stations with which they will communicate. This is true for both ESS and IBSS networks. If a mutually acceptable level of authentication has not been established between two stations, an association shall not be established. Authentication is an SS.

IEEE 802.11 supports several authentication processes. The IEEE 802.11 authentication mechanism also allows expansion of the supported authentication schemes. IEEE 802.11 does not mandate the use of any particular authentication scheme.

IEEE 802.11 provides link level authentication between IEEE 802.11 stations. IEEE 802.11 does not provide either end-to-end (message origin to message destination) or user-to-user authentication. IEEE 802.11 authentication is used simply to bring the wireless link up to the assumed physical standards of a wired link. (This use of authentication is independent of any authentication process that may be used in higher levels of a network protocol stack.) If authentication other than that described here is desired, it is recommended that IEEE Std 802.10-1992 [B3]⁴ be implemented.

If desired, an IEEE 802.11 network may be operated using Open System authentication (see 8.1.1). This may violate implicit assumptions made by higher network layers. In an Open System, any station may become authenticated.

IEEE 802.11 also supports Shared Key authentication. Use of this authentication mechanism requires implementation of the WEP option (see 8.2). In a Shared Key authentication system, identity is demonstrated by knowledge of a shared, secret, WEP encryption key.

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

IEEE 802.11 requires mutually acceptable, successful, authentication.

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

5.4.3.1.1 Preauthentication

Because the authentication process could be time-consuming (depending on the authentication protocol in use), the authentication service can be invoked independently of the association service.

Preauthentication is typically done by a STA while it is already associated with an AP (with which it previously authenticated). IEEE 802.11 does not require that STAs preauthenticate with APs. However, authentication is required before an association can be established.

If the authentication is left until reassociation time, this may impact the speed with which a STA can reassociate between APs, limiting BSS-transition mobility performance. The use of preauthentication takes the authentication service overhead out of the time-critical reassociation process.

⁴The numbers in brackets correspond to those of the bibliography in Annex E.

5.4.3.2 Deauthentication

The deauthentication service is invoked whenever an existing authentication is to be terminated. Deauthentication is an SS.

In an ESS, since 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.

5.4.3.3 Privacy

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

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

IEEE 802.11 specifies an optional privacy algorithm [wired equivalent privacy (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.

The default privacy state for all IEEE 802.11 STAs is “in the clear.” If the privacy service is not invoked, all messages shall be sent unencrypted. If this default is not acceptable to one party or the other, data frames shall not be successfully communicated between the LLC entities. Unencrypted data frames received at a station configured for mandatory privacy, as well as encrypted data frames using a key not available at the receiving station, are discarded without an indication to LLC (or without indication to distribution services in the case of “To DS” frames received at an AP). These frames are acknowledged on the WM [if received without frame check sequence (FCS) error] to avoid wasting WM bandwidth on retries.

5.5 Relationships between services

A STA keeps two state variables for each STA with which direct communication via the WM is needed:

- *Authentication state*: The values are unauthenticated and authenticated.
- *Association state*: The values are unassociated and associated.

These two variables create three local states for each remote STA:

- *State 1*: Initial start state, unauthenticated, unassociated.
- *State 2*: Authenticated, not associated.
- *State 3*: Authenticated and associated.

The relationships between these station state variables and the services are given by Figure 8.

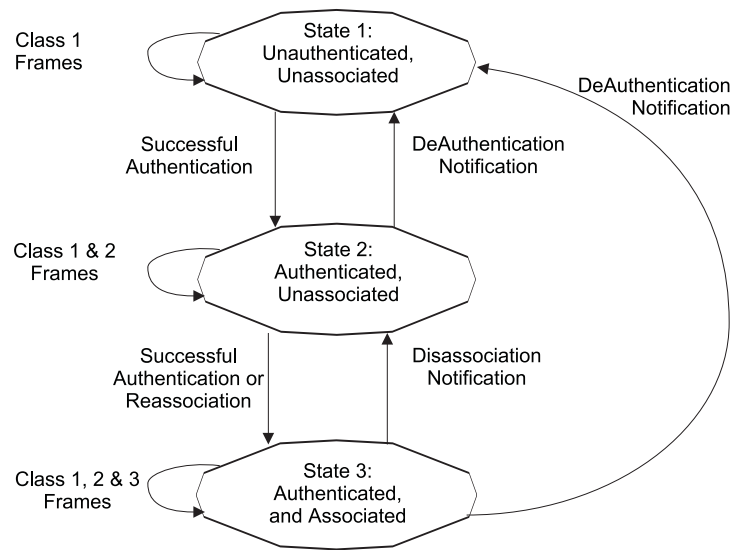


Figure 8—Relationship between state variables and services

The current state existing between the source and destination station determines the IEEE 802.11 frame types that may be exchanged between that pair of STAs (see Clause 7). The state of the sending STA given by Figure 8 is with respect to the intended receiving STA. The allowed frame types are grouped into classes and the classes correspond to the station state. In State 1, only Class 1 frames are allowed. In State 2, either Class 1 or Class 2 frames are allowed. In State 3, all frames are allowed (Classes 1, 2, and 3). The frame classes are defined as follows:

- a) Class 1 frames (permitted from within States 1, 2, and 3):
 - 1) Control frames
 - i) Request to send (RTS)
 - ii) Clear to send (CTS)
 - iii) Acknowledgment (ACK)
 - iv) Contention-Free (CF)-End+ACK
 - v) CF-End
 - 2) Management frames
 - i) Probe request/response
 - ii) Beacon
 - iii) Authentication: Successful authentication enables a station to exchange Class 2 frames. Unsuccessful authentication leaves the STA in State 1.
 - iv) Deauthentication: Deauthentication notification when in State 2 or State 3 changes the STA's state to State 1. The STA shall become authenticated again prior to sending Class 2 frames.
 - v) Announcement traffic indication message (ATIM)
 - 3) Data frames
 - i) Data: Data frames with frame control (FC) control bits "To DS" and "From DS" both false.
- b) Class 2 frames (if and only if authenticated; allowed from within State 2 and State 3 only):
 - 1) Management frames:
 - i) Association request/response
 - Successful association enables Class 3 frames.
 - Unsuccessful association leaves STA in State 2.
 - ii) Reassociation request/response

- Successful reassociation enables Class 3 frames.
 - Unsuccessful reassociation leaves the STA in State 2 (with respect to the STA that was sent the reassociation message). Reassociation frames shall only be sent if the sending STA is already associated in the same ESS.
- iii) Disassociation
- Disassociation notification when in State 3 changes a Station's state to State 2. This station shall become associated again if it wishes to utilize the DS.

If STA A receives a Class 2 frame with a unicast address in the Address 1 field from STA B that is not authenticated with STA A, STA A shall send a deauthentication frame to STA B.

(The use of the word "receive" in this subclause refers to a frame that meets all of the filtering criteria specified in Clause 9.)

- c) Class 3 frames (if and only if associated; allowed only from within State 3):
- 1) Data frames
 - Data subtypes: Data frames allowed. That is, either the "To DS" or "From DS" FC control bits may be set to true to utilize DSSs.
 - 2) Management frames
 - Deauthentication: Deauthentication notification when in State 3 implies disassociation as well, changing the STA's state from 3 to 1. The station shall become authenticated again prior to another association.
 - 3) Control frames
 - PS-Poll

If STA A receives a Class 3 frame with a unicast address in the Address 1 field from STA B that is authenticated but not associated with STA A, STA A shall send a disassociation frame to STA B.

If STA A receives a Class 3 frame with a unicast address in the Address 1 field from STA B that is not authenticated with STA A, STA A shall send a deauthentication frame to STA B.

(The use of the word "receive" in this subclause refers to a frame that meets all of the filtering criteria specified in Clauses 8 and 9.)

5.6 Differences between ESS and IBSS LANs

In 5.2.1 the concept of the IBSS LAN was introduced. It was noted that an IBSS is often used to support an ad hoc network. In an IBSS network, a STA communicates directly with one or more other STAs.

Consider the full IEEE 802.11 architecture as shown in Figure 9.

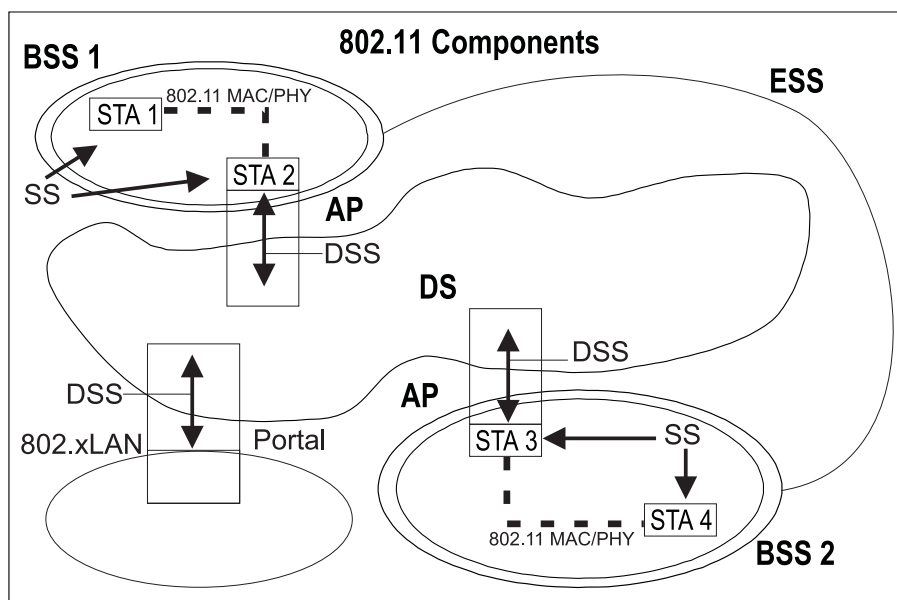


Figure 9—IEEE 802.11 architecture (again)

An IBSS consists of STAs that are directly connected. Thus there is (by definition) only one BSS. Further, since there is no physical DS, there cannot be a portal, an integrated wired LAN, or the DSSs. The logical picture reduces to Figure 10.

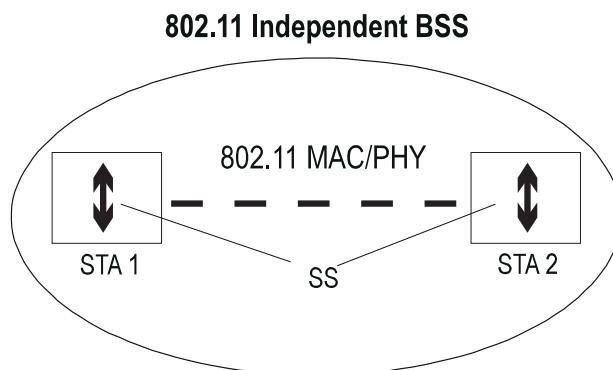


Figure 10—Logical architecture of an IBSS

Only the minimum two stations are shown in Figure 10. An IBSS may have an arbitrary number of members. In an IBSS, only Class 1 and Class 2 frames are allowed, since there is no DS in an IBSS.

The services that apply to an IBSS are the SSs.

5.7 Message information contents that support the services

Each service is supported by one or more IEEE 802.11 messages. Information items are given by name; for corresponding values, see Clause 7.

5.7.1 Data

For a STA to send data to another STA, it sends a data message, as shown below:

Data messages

- Message type: Data
- Message subtype: Data
- Information items:
 - IEEE source address of message
 - IEEE destination address of message
 - BSS ID
- Direction of message: From STA to STA

5.7.2 Association

For a STA to associate, the association service causes the following messages to occur:

Association request

- Message type: Management
- Message subtype: Association request
- Information items:
 - IEEE address of the STA initiating the association
 - IEEE address of the AP with which the initiating station will associate
 - ESS ID
- Direction of message: From STA to AP

Association response

- Message type: Management
- Message subtype: Association response
- Information items:
 - Result of the requested association. This is an item with values “successful” and “unsuccessful.”
 - If the association is successful, the response shall include the association identifier (AID).
- Direction of message: From AP to STA

5.7.3 Reassociation

For a STA to reassociate, the reassociation service causes the following message to occur:

Reassociation request

- Message type: Management
- Message subtype: Reassociation request
- Information items:
 - IEEE address of the STA initiating the reassociation
 - IEEE address of the AP with which the initiating station will reassociate
 - IEEE address of the AP with which the initiating station is currently associated
 - ESSID
- Direction of message:
 - From STA to AP (The AP with which the STA is requesting reassociation)

The address of the current AP is included for efficiency. The inclusion of the current AP address facilitates MAC reassociation to be independent of the DS implementation.

Reassociation response

- Message type: Management
- Message subtype: Reassociation response
- Information items:
 - Result of the requested reassociation. This is an item with values “successful” and “unsuccessful.”
 - If the reassociation is successful, the response shall include the AID.
- Direction of message: From AP to STA

5.7.4 Disassociation

For a STA to terminate an active association, the disassociation service causes the following message to occur:

Disassociation

- Message type: Management
- Message subtype: Disassociation
- Information items:
 - IEEE address of the station that is being disassociated. This shall be the broadcast address in the case of an AP disassociating with all associated stations.
 - IEEE address of the AP with which the station is currently associated.
- Direction of message: From STA to STA (e.g., STA to AP or AP to STA)

5.7.5 Privacy

For a STA to invoke the WEP privacy algorithm (as controlled by the related MIB attributes, see Clause 11), the privacy service causes MPDU encryption and sets the WEP frame header bit appropriately (see Clause 7).

5.7.6 Authentication

For a STA to authenticate with another STA, the authentication service causes one or more authentication management frames to be exchanged. The exact sequence of frames and their content is dependent on the authentication scheme invoked. For all authentication schemes, the authentication algorithm is identified within the management frame body.

In an IBSS environment, either station may be the initiating STA (STA 1). In an ESS environment, STA 1 is the mobile STA, and STA 2 is the AP.

Authentication (first frame of sequence)

- Message type: Management
- Message subtype: Authentication
- Information items:
 - Authentication algorithm identification
 - Station identity assertion
 - Authentication transaction sequence number
 - Authentication algorithm dependent information
- Direction of message: First frame in the transaction sequence is always from STA 1 to STA 2.

The first frame in an authentication sequence shall always be unencrypted.

Authentication (intermediate sequence frames)

- Message type: Management
- Message subtype: Authentication
- Information items:
 - Authentication algorithm identification
 - Authentication transaction sequence number
 - Authentication algorithm dependent information
- Direction of message:
 - Even transaction sequence numbers: From STA 2 to STA 1
 - Odd transaction sequence numbers: From STA 1 to STA 2

Authentication (final frame of sequence)

- Message type: Management
- Message subtype: Authentication
- Information items:
 - Authentication algorithm identification
 - Authentication transaction sequence number
 - Authentication algorithm dependent information
 - The result of the requested authentication. This is an item with values “successful” and “unsuccessful.”
- Direction of message: STA 2 to STA 1

5.7.7 Deauthentication

For a STA to invalidate an active authentication, the following message is sent:

Deauthentication

- Message type: Management
- Message subtype: Deauthentication
- Information items:
 - IEEE address of the STA that is being deauthenticated
 - IEEE address of the STA with which the STA is currently authenticated
 - This shall be the broadcast address in the case of a STA deauthenticating all STAs currently authenticated.
- Direction of message: From STA to STA

5.8 Reference model

The standard presents the architectural view, emphasizing the separation of the system into two major parts: the MAC of the data link layer and the PHY. These layers are intended to correspond closely to the lowest

layers of the ISO/IEC basic reference model of Open Systems Interconnection (OSI) (ISO/IEC 7498-1: 1994⁵). The layers and sublayers described in this standard are shown in Figure 11.

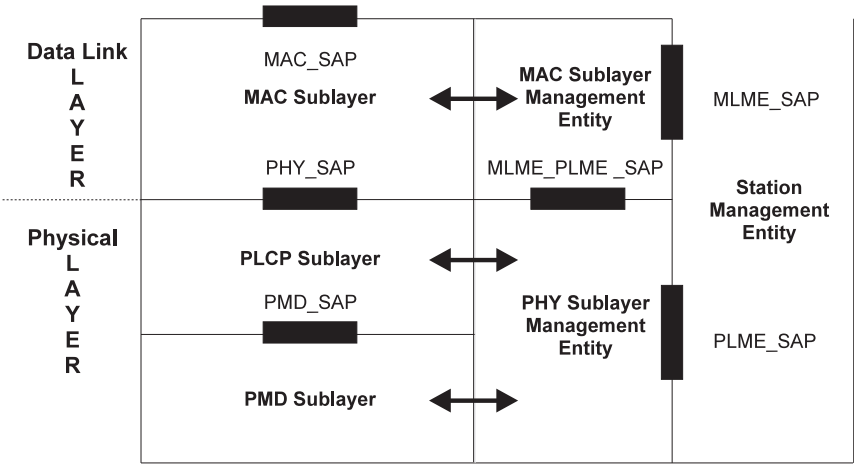


Figure 11 — Portion of the ISO/IEC basic reference model covered in this standard

⁵Information on normative references can be found in Clause 2.

6. MAC service definition

6.1 Overview of MAC services

6.1.1 Asynchronous data service

This service provides peer LLC entities with the ability to exchange MAC service data units (MSDUs). To support this service, the local MAC uses the underlying PHY-level services to transport an MSDU to a peer MAC entity, where it will be delivered to the peer LLC. Such asynchronous MSDU transport is performed on a best-effort connectionless basis. There are no guarantees that the submitted MSDU will be delivered successfully. Broadcast and multicast transport is part of the asynchronous data service provided by the MAC. Due to the characteristics of the WM, broadcast and multicast MSDUs may experience a lower quality of service, compared to that of unicast MSDUs. All STAs will support the asynchronous data service. Because operation of certain functions of the MAC may cause reordering of some MSDUs, as discussed in more detail below, there are two service classes within the asynchronous data service. By selecting the desired service class, each LLC entity initiating the transfer of MSDUs is able to control whether MAC entities are or are not allowed to reorder those MSDUs.

6.1.2 Security services

Security services in IEEE 802.11 are provided by the authentication service and the wired equivalent privacy (WEP) mechanism. The scope of the security services provided is limited to station-to-station data exchange. The privacy service offered by an IEEE 802.11 WEP implementation is the encryption of the MSDU. For the purposes of this standard, WEP is viewed as a logical service located within the MAC sublayer as shown in the reference model, Figure 11. Actual implementations of the WEP service are transparent to the LLC or other layers above the MAC sublayer.

The security services provided by the WEP in IEEE 802.11 are as follows:

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

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

The MAC sublayer security services provided by WEP rely on information from non-Layer 2 management or system entities. Management entities communicate information to WEP through a set of MIB attributes.

6.1.3 MSDU ordering

The services provided by the MAC sublayer permit, and may in certain cases require, the reordering of MSDUs. The MAC does not intentionally reorder MSDUs except as may be necessary to improve the likelihood of successful delivery based on the current operational (“power management”) mode of the designated recipient station(s). The sole effect of this reordering (if any), for the set of MSDUs received at the MAC service interface of any single station, is a change in the delivery order of broadcast and multicast MSDUs, relative to directed MSDUs, originating from a single source station address. If a higher-layer protocol using the asynchronous data service cannot tolerate this possible reordering, the optional StrictlyOrdered service class should be used. MSDUs transferred between any pair of stations using the StrictlyOrdered service class are not subject to the relative reordering that is possible when the ReorderableMulticast service class is used. However, the desire to receive MSDUs sent using the StrictlyOrdered service class at a station precludes simultaneous use of the MAC power management facilities at that station.