

**ANSI/IEEE Std 802.11, 1999 Edition**

[Adopted by ISO/IEC and redesignated as  
ISO/IEC 8802-11:1999(E)]

**IEEE Standard for Information technology—  
Telecommunications and information exchange between systems—  
Local and metropolitan area networks—  
Specific requirements**

# **Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications**

**Adopted by the ISO/IEC and redesignated as  
ISO/IEC 8802-11:1999(E)**

Sponsor

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

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

Copyright © 1999 by the Institute of Electrical and Electronics Engineers, Inc.  
All rights reserved. Published 1999. Printed in the United States of America.

ISBN 0-7381-1658-0

*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.*

20 August 1999

SH94740

## ANSI/IEEE Std 802.11, 1999 Edition

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 all 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.

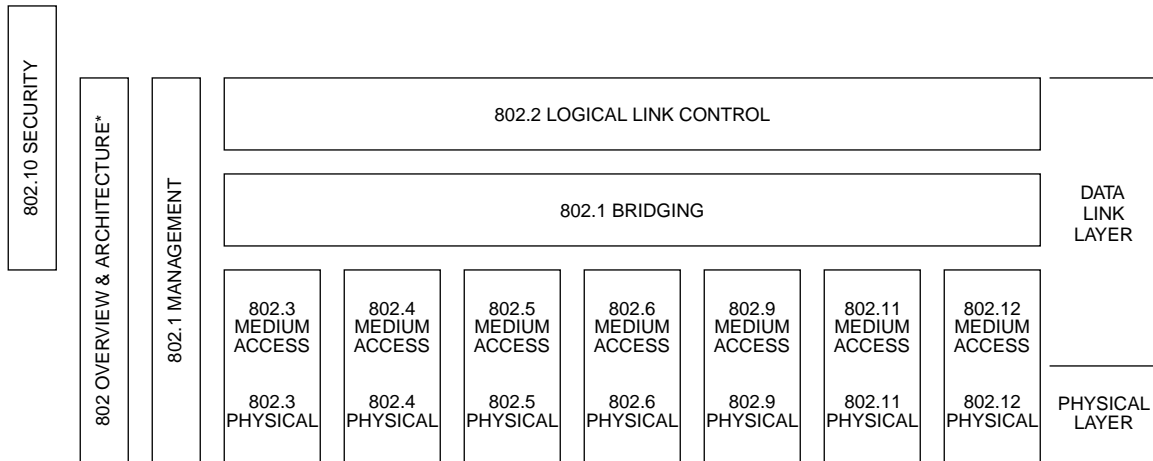
The patent holder has, however, filed a statement of assurance that it will grant a license under these rights without compensation or under reasonable rates and nondiscriminatory, reasonable terms and conditions to all applicants desiring to obtain such a license. The IEEE makes no representation as to the reasonableness of rates and/or terms and conditions of the license agreement offered by the patent holder. Contact information may be obtained from the IEEE Standards Department.

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

# Introduction to ANSI/IEEE Std 802.11, 1999 Edition

(This introduction is not a part of ANSI/IEEE Std 802.11, 1999 Edition or of ISO/IEC 8802-11: 1999, but is included for information purpose 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 (ISO) Open Systems Interconnection (OSI) Basic Reference Model (ISO/IEC 7498-1: 1994). The access standards define seven 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.
- ANSI/IEEE Std 802.1B and 802.1k [ISO/IEC 15802-2] *LAN/MAN Management*. Defines an OSI management-compatible architecture, and services and protocol elements for use in a LAN/MAN environment for performing remote management.
- ANSI/IEEE Std 802.1D [ISO/IEC 15802-3] *Media Access Control (MAC) Bridges*. 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.
- IEEE Std 802.1F *Common Definitions and Procedures for IEEE 802 Management Information*
- ANSI/IEEE Std 802.1G [ISO/IEC 15802-5] *Remote Media Access Control (MAC) Bridging*. Specifies extensions for the interconnection, using non-LAN communication technologies, of geographically separated IEEE 802 LANs below the level of the logical link control protocol.
- 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 [ISO/IEC 8802-5] *Token Ring Access Method and Physical Layer Specifications*
- ANSI/IEEE Std 802.6 [ISO/IEC 8802-6] *Distributed Queue Dual Bus Access Method and Physical Layer Specifications*
- ANSI/IEEE Std 802.9 [ISO/IEC 8802-9] *Integrated Services (IS) LAN Interface at the Medium Access Control (MAC) and Physical (PHY) Layers*
- ANSI/IEEE Std 802.10 *Interoperable LAN/MAN Security*
- IEEE Std 802.11 [ISO/IEC DIS 8802-11] *Wireless LAN Medium Access Control (MAC) and Physical Layer Specifications*
- ANSI/IEEE Std 802.12 [ISO/IEC DIS 8802-12] *Demand Priority Access Method, Physical Layer and Repeater Specifications*

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*

## 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.

## ANSI/IEEE Std 802.11, 1999 Edition [ISO/IEC 8802-11: 1999]

This standard is a revision of IEEE Std 802.11-1997. The Management Information Base according to OSI rules has been removed, many redundant management items have been removed, and Annex D has been completed with the Management Information Base according to SNMP. Minor changes have been made throughout the document.

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 Speci-



Major contributions to the 1999 edition were received from the following individuals:

Henri Moelard

Richard Ozer

Arnoud Zwemmer

The following members of the balloting committee voted on the 1999 version of this standard:

Kit Athul	A. Kamerman	Ronald C. Petersen
Thomas W. Bailey	Dean M. Kawaguchi	John R. Pickens
Peter K. Campbell	Edward R. Kelly	Alberto Profumo
James T. Carlo	Gary C. Kessler	Vikram Punj
David E. Carlson	Yongbum Kim	James A. Renfro
Brian J. Casey	Stephen Barton Kruger	Gary S. Robinson
Naftali Chayat	Joseph Kubler	Edouard Y. Rocher
Robert S. Crowder	Lanse M. Leach	James W. Romlein
Wim Diepstraten	Jai Yong Lee	Floyd E. Ross
Thomas J. Dineen	Randolph S. Little	Michael Rothenberg
Christos Douligieris	Ronald Mahany	Christoph Ruland
Paul S. Eastman	Peter Martini	Anil K. Sanwalka
Philip H. Enslow	Richard McBride	James E. Schuessler
Changxin Fan	Bennett Meyer	Rich Seifert
John W. Fendrich	Gene E. Milligan	Leo Sintonen
Michael A. Fischer	David S. Millman	Patricia Thaler
George R. Fishel	Hiroshi Miyano	Mike Trompower
Harvey A. Freeman	Warren Monroe	Mark-Rene Uchida
Robert J. Gagliano	John E. Montague	Emmanuel Van Lil
Patrick S. Gonia	Wayne D. Moyers	Sarosh N. Vesuna
Julio Gonzalez-Sanz	Shimon Muller	James Vorhies
Chris G. Guy	Ken Naganuma	Barry M. Vornbrock
Victor Hayes	Paul Nikolich	Qian-li Yang
Donald N. Heirman	Robert O'Hara	Oren Yuen
Henry Hoyt	Donal O'Mahony	Chris Zegelin
Raj Jain	Roger Pandanda	Jonathan M. Zweig

At the time the draft of the 1997 version 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

F. 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 to the 1997 version 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 for the 1997 version of this standard:

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. Kameron  
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-SA Standards Board approved this standard on 18 March 1999, it had the following membership:

**Richard J. Holleman**, *Chair*

**Donald N. Heirman**, *Vice Chair*

**Judith Gorman**, *Secretary*

Satish K. Aggarwal  
Dennis Bodson  
Mark D. Bowman  
James T. Carlo  
Gary R. Engmann  
Harold E. Epstein  
Jay Forster\*  
Ruben D. Garzon

James H. Gurney  
Lowell G. Johnson  
Robert J. Kennelly  
E. G. "Al" Kiener  
Joseph L. Koepfinger\*  
L. Bruce McClung  
Daleep C. Mohla  
Robert F. Munzner

Louis-François Pau  
Ronald C. Petersen  
Gerald H. Peterson  
John B. Posey  
Gary S. Robinson  
Akio Tojo  
Hans E. Weinrich  
Donald W. Zipse

\*Member Emeritus

Also included is the following nonvoting IEEE-SA Standards Board liaison:

Robert E. Hebner

Valerie E. Zelenty  
*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 .....	59
8.1	Authentication services .....	59
8.1.1	Open System authentication .....	59
8.1.2	Shared Key authentication .....	60
8.2	The Wired Equivalent Privacy (WEP) algorithm .....	61
8.2.1	Introduction.....	61
8.2.2	Properties of the WEP algorithm .....	62
8.2.3	WEP theory of operation .....	62
8.2.4	WEP algorithm specification .....	64
8.2.5	WEP Frame Body expansion .....	64
8.3	Security-Related MIB attributes .....	65
8.3.1	Authentication-Related MIB attributes.....	65
8.3.2	Privacy-Related MIB attributes .....	65
9.	MAC sublayer functional description.....	70
9.1	MAC architecture.....	70
9.1.1	Distributed coordination function (DCF).....	70
9.1.2	Point coordination function (PCF).....	70
9.1.3	Coexistence of DCF and PCF .....	71
9.1.4	Fragmentation/defragmentation overview .....	71
9.1.5	MAC data service .....	72
9.2	DCF.....	72
9.2.1	Carrier-sense mechanism .....	73
9.2.2	MAC-Level acknowledgments .....	73
9.2.3	Interframe space (IFS) .....	74
9.2.4	Random backoff time.....	75
9.2.5	DCF access procedure.....	76
9.2.6	Directed MPDU transfer procedure .....	82
9.2.7	Broadcast and multicast MPDU transfer procedure .....	83
9.2.8	ACK procedure .....	83
9.2.9	Duplicate detection and recovery.....	83
9.2.10	DCF timing relations.....	84
9.3	PCF .....	86
9.3.1	CFP structure and timing .....	87
9.3.2	PCF access procedure .....	88
9.3.3	PCF transfer procedure .....	89
9.3.4	Contention-Free polling list.....	92
9.4	Fragmentation .....	93
9.5	Defragmentation .....	94
9.6	Multirate support.....	95
9.7	Frame exchange sequences .....	95

9.8	MSDU transmission restrictions .....	97
10.	Layer management .....	98
10.1	Overview of management model .....	98
10.2	Generic management primitives .....	98
10.3	MLME SAP interface .....	100
10.3.1	Power management .....	100
10.3.2	Scan .....	101
10.3.3	Synchronization .....	103
10.3.4	Authenticate .....	105
10.3.5	De-authenticate .....	107
10.3.6	Associate .....	109
10.3.7	Reassociate .....	111
10.3.8	Disassociate .....	113
10.3.9	Reset .....	114
10.3.10	Start .....	116
10.4	PLME SAP interface .....	118
10.4.1	PLME-RESET.request .....	118
10.4.2	PLME-CHARACTERISTICS.request .....	118
10.4.3	PLME-CHARACTERISTICS.confirm .....	119
10.4.4	PLME-DSSSTESTMODE.request .....	121
10.4.5	PLME-DSSSTESTOUTPUT.request .....	122
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
12.	Physical layer (PHY) service specification .....	138
12.1	Scope .....	138
12.2	PHY functions .....	138
12.3	Detailed PHY service specifications .....	138
12.3.1	Scope and field of application .....	138
12.3.2	Overview of the service .....	138
12.3.3	Overview of interactions .....	138
12.3.4	Basic service and options .....	139
12.3.5	PHY-SAP detailed service specification .....	140
13.	PHY management .....	147

14.	Frequency-Hopping spread spectrum (FHSS) PHY specification for the 2.4 GHz Industrial, Scientific, and Medical (ISM) band.....	148
14.1	Overview.....	148
14.1.1	Overview of FHSS PHY.....	148
14.1.2	FHSS PHY functions.....	148
14.1.3	Service specification method and notation.....	148
14.2	FHSS PHY-specific service parameter lists.....	149
14.2.1	Overview.....	149
14.2.2	TXVECTOR parameters.....	149
14.2.3	RXVECTOR parameters.....	150
14.3	FHSS PLCP sublayer.....	150
14.3.1	Overview.....	150
14.3.2	PLCP frame format.....	151
14.3.3	PLCP state machines.....	154
14.4	PLME SAP layer management.....	163
14.4.1	Overview.....	163
14.4.2	FH PHY specific MAC sublayer management entity (MLME) procedures.....	163
14.4.3	FH PHY layer management entity state machines.....	163
14.5	FHSS PMD sublayer services.....	166
14.5.1	Scope and field of application.....	166
14.5.2	Overview of services.....	166
14.5.3	Overview of interactions.....	166
14.5.4	Basic service and options.....	166
14.5.5	PMD_SAP detailed service specification.....	167
14.6	FHSS PMD sublayer, 1.0 Mbit/s.....	172
14.6.1	1 Mbit/s PMD operating specifications, general.....	172
14.6.2	Regulatory requirements.....	172
14.6.3	Operating frequency range.....	173
14.6.4	Number of operating channels.....	174
14.6.5	Operating channel center frequency.....	174
14.6.6	Occupied channel bandwidth.....	176
14.6.7	Minimum hop rate.....	176
14.6.8	Hop sequences.....	177
14.6.9	Unwanted emissions.....	179
14.6.10	Modulation.....	179
14.6.11	Channel data rate.....	180
14.6.12	Channel switching/settling time.....	180
14.6.13	Receive to transmit switch time.....	180
14.6.14	PMD transmit specifications.....	181
14.6.15	PMD receiver specifications.....	182
14.6.16	Operating temperature range.....	183
14.7	FHSS PMD sublayer, 2.0 Mbit/s.....	183
14.7.1	Overview.....	183
14.7.2	Four-Level GFSK modulation.....	184
14.7.3	Channel data rate.....	185
14.8	FHSS PHY management information base (MIB).....	186
14.8.1	Overview.....	186
14.8.2	FH PHY attributes.....	187
14.9	FH PHY characteristics.....	194
15.	Direct sequence spread spectrum (DSSS) PHY specification for the 2.4 GHz band designated for ISM applications.....	195

15.1	Overview.....	195
15.1.1	Scope.....	195
15.1.2	DSSS PHY functions.....	195
15.1.3	Service specification method and notation.....	196
15.2	DSSS PLCP sublayer.....	196
15.2.1	Overview.....	196
15.2.2	PLCP frame format.....	196
15.2.3	PLCP field definitions.....	196
15.2.4	PLCP/DSSS PHY data scrambler and descrambler.....	199
15.2.5	PLCP data modulation and modulation rate change.....	199
15.2.6	PLCP transmit procedure.....	199
15.2.7	PLCP receive procedure.....	200
15.3	DSSS physical layer management entity (PLME).....	203
15.3.1	PLME_SAP sublayer management primitives.....	203
15.3.2	DSSS PHY MIB.....	204
15.3.3	DS PHY characteristics.....	205
15.4	DSSS PMD sublayer.....	205
15.4.1	Scope and field of application.....	205
15.4.2	Overview of service.....	206
15.4.3	Overview of interactions.....	206
15.4.4	Basic service and options.....	206
15.4.5	PMD_SAP detailed service specification.....	208
15.4.6	PMD operating specifications, general.....	215
15.4.7	PMD transmit specifications.....	218
15.4.8	PMD receiver specifications.....	222
16.	Infrared (IR) PHY specification.....	224
16.1	Overview.....	224
16.1.1	Scope.....	225
16.1.2	IR PHY functions.....	225
16.1.3	Service specification method and notation.....	225
16.2	IR PLCP sublayer.....	226
16.2.1	Overview.....	226
16.2.2	PLCP frame format.....	226
16.2.3	PLCP modulation and rate change.....	226
16.2.4	PLCP field definitions.....	227
16.2.5	PLCP procedures.....	228
16.3	IR PMD sublayer.....	230
16.3.1	Overview.....	230
16.3.2	PMD operating specifications, general.....	230
16.3.3	PMD transmit specifications.....	233
16.3.4	PMD receiver specifications.....	236
16.3.5	Energy Detect, Carrier Sense, and CCA definitions.....	237
16.4	PHY attributes.....	239
Annex A	(normative) Protocol Implementation Conformance Statement (PICS) proforma.....	241
A.1	Introduction.....	241
A.2	Abbreviations and special symbols.....	241
A.2.1	Status symbols.....	241
A.2.2	General abbreviations.....	241
A.3	Instructions for completing the PICS proforma.....	242
A.3.1	General structure of the PICS proforma.....	242

A.3.2 Additional information.....	242
A.3.3 Exception information.....	243
A.3.4 Conditional status.....	243
A.4 PICS proforma—ISO/IEC 8802-11: 1999.....	244
A.4.1 Implementation identification .....	244
A.4.2 Protocol summary, ISO/IEC 8802-11: 1999.....	244
A.4.3 IUT configuration .....	245
A.4.4 MAC protocol .....	245
A.4.5 Frequency-Hopping PHY functions.....	250
A.4.6 Direct sequence PHY functions .....	252
A.4.7 Infrared baseband PHY functions .....	255
 Annex B (informative) Hopping sequences.....	 259
 Annex C (normative) Formal description of MAC operation .....	 272
C.1 Introduction to the MAC formal description .....	275
C.2 Data type and operator definitions for the MAC state machines.....	277
C.3 State Machines for MAC stations .....	324
C.4 State machines for MAC access point .....	400
 Annex D (normative) ASN.1 encoding of the MAC and PHY MIB.....	 469
 Annex E (informative) Bibliography .....	 512
E.1 General .....	512
E.2 Specification and description language (SDL) documentation .....	512

## 7. Frame formats

The format of the MAC frames is specified in this clause. All stations shall be able to properly construct frames for transmission and decode frames upon reception, as specified in this clause.

### 7.1 MAC frame formats

Each frame consists of the following basic components:

- a) A *MAC header*, which comprises frame control, duration, address, and sequence control information;
- b) A variable length *frame body*, which contains information specific to the frame *type*;
- c) A *frame check sequence* (FCS), which contains an IEEE 32-bit cyclic redundancy code (CRC).

#### 7.1.1 Conventions

The MAC protocol data units (MPDUs) or frames in the MAC sublayer are described as a sequence of fields in specific order. Each figure in Clause 7 depicts the fields/subfields as they appear in the MAC frame and in the order in which they are passed to the physical layer convergence protocol (PLCP), from left to right.

In figures, all bits within fields are numbered, from 0 to  $k$ , where the length of the field is  $k + 1$  bit. The octet boundaries within a field can be obtained by taking the bit numbers of the field modulo 8. Octets within numeric fields that are longer than a single octet are depicted in increasing order of significance, from lowest numbered bit to highest numbered bit. The octets in fields longer than a single octet are sent to the PLCP in order from the octet containing the lowest numbered bits to the octet containing the highest numbered bits.

Any field containing a CRC is an exception to this convention and is transmitted commencing with the coefficient of the highest-order term.

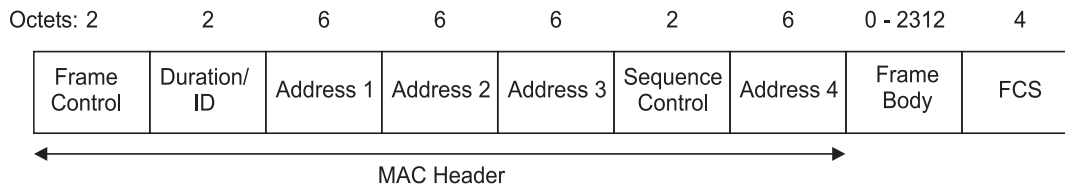
MAC addresses are assigned as ordered sequences of bits. The Individual/Group bit is always transferred first and is bit 0 of the first octet.

Values specified in decimal are coded in natural binary unless otherwise stated. The values in Table 1 are in binary, with the bit assignments shown in the table. Values in other tables are shown in decimal notation.

Reserved fields and subfields are set to 0 upon transmission and are ignored upon reception.

#### 7.1.2 General frame format

The MAC frame format comprises a set of fields that occur in a fixed order in all frames. Figure 12 depicts the general MAC frame format. The fields Address 2, Address 3, Sequence Control, Address 4, and Frame Body are only present in certain frame types. Each field is defined in 7.1.3. The format of each of the individual frame types is defined in 7.2.



**Figure 12—MAC frame format**

### 7.1.3 Frame fields

#### 7.1.3.1 Frame Control field

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

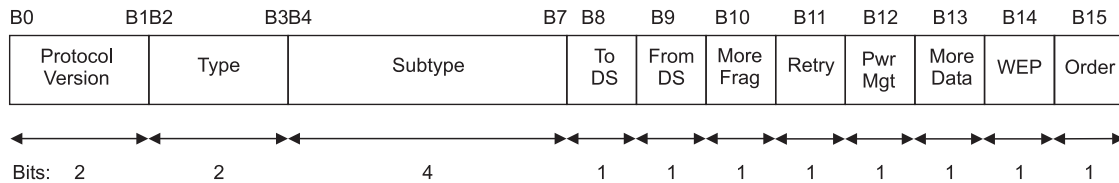


Figure 13—Frame Control field

##### 7.1.3.1.1 Protocol Version field

The Protocol Version field is 2 bits in length and is invariant in size and placement across all revisions of this standard. For this standard, the value of the protocol version is 0. All other values are reserved. The revision level will be incremented only when a fundamental incompatibility exists between a new revision and the prior edition of the standard. A device that receives a frame with a higher revision level than it supports will discard the frame without indication to the sending station or to LLC.

##### 7.1.3.1.2 Type and Subtype fields

The Type field is 2 bits in length, and the Subtype field is 4 bits in length. The Type and Subtype fields together identify the function of the frame. There are three frame types: control, data, and management. Each of the frame types have several defined subtypes. Table 1 defines the valid combinations of type and subtype.

##### 7.1.3.1.3 To DS field

The To DS field is 1 bit in length and is set to 1 in data type frames destined for the DS. This includes all data type frames sent by STAs associated with an AP. The To DS field is set to 0 in all other frames.

##### 7.1.3.1.4 From DS field

The From DS field is 1 bit in length and is set to 1 in data type frames exiting the DS. It is set to 0 in all other frames.

The permitted To/From DS bit combinations and their meanings are given in Table 2.

##### 7.1.3.1.5 More Fragments field

The More Fragments field is 1 bit in length and is set to 1 in all data or management type frames that have another fragment of the current MSDU or current MMPDU to follow. It is set to 0 in all other frames.

**Table 1—Valid type and subtype combinations**

Type value b3 b2	Type description	Subtype value b7 b6 b5 b4	Subtype description
00	Management	0000	Association request
00	Management	0001	Association response
00	Management	0010	Reassociation request
00	Management	0011	Reassociation response
00	Management	0100	Probe request
00	Management	0101	Probe response
00	Management	0110–0111	Reserved
00	Management	1000	Beacon
00	Management	1001	Announcement traffic indication message (ATIM)
00	Management	1010	Disassociation
00	Management	1011	Authentication
00	Management	1100	Deauthentication
00	Management	1101–1111	Reserved
01	Control	0000–1001	Reserved
01	Control	1010	Power Save (PS)-Poll
01	Control	1011	Request To Send (RTS)
01	Control	1100	Clear To Send (CTS)
01	Control	1101	Acknowledgment (ACK)
01	Control	1110	Contention-Free (CF)-End
01	Control	1111	CF-End + CF-Ack
10	Data	0000	Data
10	Data	0001	Data + CF-Ack
10	Data	0010	Data + CF-Poll
10	Data	0011	Data + CF-Ack + CF-Poll
10	Data	0100	Null function (no data)
10	Data	0101	CF-Ack (no data)
10	Data	0110	CF-Poll (no data)
10	Data	0111	CF-Ack + CF-Poll (no data)
10	Data	1000–1111	Reserved
11	Reserved	0000–1111	Reserved

**Table 2—To/From DS combinations in data type frames**

To/From DS values	Meaning
To DS = 0 From DS = 0	A data frame direct from one STA to another STA within the same IBSS, as well as all management and control type frames.
To DS = 1 From DS = 0	Data frame destined for the DS.
To DS = 0 From DS = 1	Data frame exiting the DS.
To DS = 1 From DS = 1	Wireless distribution system (WDS) frame being distributed from one AP to another AP.

#### 7.1.3.1.6 Retry field

The Retry field is 1 bit in length and is set to 1 in any data or management type frame that is a retransmission of an earlier frame. It is set to 0 in all other frames. A receiving station uses this indication to aid in the process of eliminating duplicate frames.

#### 7.1.3.1.7 Power Management field

The Power Management field is 1 bit in length and is used to indicate the power management mode of a STA. The value of this field remains constant in each frame from a particular STA within a frame exchange sequence defined in 9.7. The value indicates the mode in which the station will be after the successful completion of the frame exchange sequence.

A value of 1 indicates that the STA will be in power-save mode. A value of 0 indicates that the STA will be in active mode. This field is always set to 0 in frames transmitted by an AP.

#### 7.1.3.1.8 More Data field

The More Data field is 1 bit in length and is used to indicate to a STA in power-save mode that more MSDUs, or MMPDUs are buffered for that STA at the AP. The More Data field is valid in directed data or management type frames transmitted by an AP to an STA in power-save mode. A value of 1 indicates that at least one additional buffered MSDU, or MMPDU, is present for the same STA.

The More Data field may be set to 1 in directed data type frames transmitted by a contention-free (CF)-Pollable STA to the point coordinator (PC) in response to a CF-Poll to indicate that the STA has at least one additional buffered MSDU available for transmission in response to a subsequent CF-Poll.

The More Data field is set to 0 in all other directed frames.

The More Data field is set to 1 in broadcast/multicast frames transmitted by the AP, when additional broadcast/multicast MSDUs, or MMPDUs, remain to be transmitted by the AP during this beacon interval. The More Data field is set to 0 in broadcast/multicast frames transmitted by the AP when no more broadcast/multicast MSDUs, or MMPDUs, remain to be transmitted by the AP during this beacon interval and in all broadcast/multicast frames transmitted by non-AP stations.

#### 7.1.3.1.9 WEP field

The WEP field is 1 bit in length. It is set to 1 if the Frame Body field contains information that has been processed by the WEP algorithm. The WEP field is only set to 1 within frames of type Data and frames of

type Management, subtype Authentication. The WEP field is set to 0 in all other frames. When the WEP bit is set to 1, the Frame Body field is expanded as defined in 8.2.5.

### 7.1.3.1.10 Order field

The Order field is 1 bit in length and is set to 1 in any data type frame that contains an MSDU, or fragment thereof, which is being transferred using the StrictlyOrdered service class. This field is set to 0 in all other frames.

### 7.1.3.2 Duration/ID field

The Duration/ID field is 16 bits in length. The contents of this field are as follows:

- a) In control type frames of subtype Power Save (PS)-Poll, the Duration/ID field carries the association identity (AID) of the station that transmitted the frame in the 14 least significant bits (lsb), with the 2 most significant bits (msb) both set to 1. The value of the AID is in the range 1–2007.
- b) In all other frames, the Duration/ID field contains a duration value as defined for each frame type in 7.2. For frames transmitted during the contention-free period (CFP), the duration field is set to 32 768.

Whenever the contents of the Duration/ID field are less than 32 768, the duration value is used to update the network allocation vector (NAV) according to the procedures defined in Clause 9.

The encoding of the Duration/ID field is given in Table 3.

**Table 3—Duration/ID field encoding**

Bit 15	Bit 14	Bits 13–0	Usage
0		0–32 767	Duration
1	0	0	Fixed value within frames transmitted during the CFP
1	0	1–16 383	Reserved
1	1	0	Reserved
1	1	1–2 007	AID in PS-Poll frames
1	1	2 008–16 383	Reserved

### 7.1.3.3 Address fields

There are four address fields in the MAC frame format. These fields are used to indicate the BSSID, source address, destination address, transmitting station address, and receiving station address. The usage of the four address fields in each frame type is indicated by the abbreviations BSSID, DA, SA, RA, and TA, indicating basic service set identifier (BSSID), Destination Address, Source Address, Receiver Address, and Transmitter Address, respectively. Certain frames may not contain some of the address fields.

Certain address field usage is specified by the relative position of the address field (1–4) within the MAC header, independent of the type of address present in that field. For example, receiver address matching is always performed on the contents of the Address 1 field in received frames, and the receiver address of CTS and ACK frames is always obtained from the Address 2 field in the corresponding RTS frame, or from the frame being acknowledged.

### 7.1.3.3.1 Address representation

Each Address field contains a 48-bit address as defined in 5.2 of IEEE Std 802-1990.

### 7.1.3.3.2 Address designation

A MAC sublayer address is one of the following two types:

- a) *Individual address.* The address associated with a particular station on the network.
- b) *Group address.* A multidestination address, associated with one or more stations on a given network. The two kinds of group addresses are as follows:
  - 1) *Multicast-group address.* An address associated by higher-level convention with a group of logically related stations.
  - 2) *Broadcast address.* A distinguished, predefined multicast address that always denotes the set of all stations on a given LAN. All 1s in the Destination Address field are interpreted to be the broadcast address. This group is predefined for each communication medium to consist of all stations actively connected to that medium; it is used to broadcast to all the active stations on that medium. All stations are able to recognize the broadcast address. It is not necessary that a station be capable of generating the broadcast address.

The address space is also partitioned into locally administered and universal (globally administered) addresses. The nature of a body and the procedures by which it administers these universal (globally administered) addresses is beyond the scope of this standard. See IEEE Std 802-1990 for more information.

### 7.1.3.3.3 BSSID field

The BSSID field is a 48-bit field of the same format as an IEEE 802 MAC address. This field uniquely identifies each BSS. The value of this field, in an infrastructure BSS, is the MAC address currently in use by the STA in the AP of the BSS.

The value of this field in an IBSS is a locally administered IEEE MAC address formed from a 46-bit random number generated according to the procedure defined in 11.1.3. The individual/group bit of the address is set to 0. The universal/local bit of the address is set to 1. This mechanism is used to provide a high probability of selecting a unique BSSID.

The value of all 1s is used to indicate the broadcast BSSID. A broadcast BSSID may only be used in the BSSID field of management frames of subtype probe request.

### 7.1.3.3.4 Destination Address (DA) field

The DA field contains an IEEE MAC individual or group address that identifies the MAC entity or entities intended as the final recipient(s) of the MSDU (or fragment thereof) contained in the frame body field.

### 7.1.3.3.5 Source Address (SA) field

The SA field contains an IEEE MAC individual address that identifies the MAC entity from which the transfer of the MSDU (or fragment thereof) contained in the frame body field was initiated. The individual/group bit is always transmitted as a zero in the source address.

### 7.1.3.3.6 Receiver Address (RA) field

The RA field contains an IEEE MAC individual or group address that identifies the intended immediate recipient STA(s), on the WM, for the information contained in the frame body field.

### 7.1.3.3.7 Transmitter Address (TA) field

The TA field contains an IEEE MAC individual address that identifies the STA that has transmitted, onto the WM, the MPDU contained in the frame body field. The Individual/Group bit is always transmitted as a zero in the transmitter address.

### 7.1.3.4 Sequence Control field

The Sequence Control field is 16 bits in length and consists of two subfields, the Sequence Number and the Fragment Number. The format of the Sequence Control field is illustrated in Figure 14.

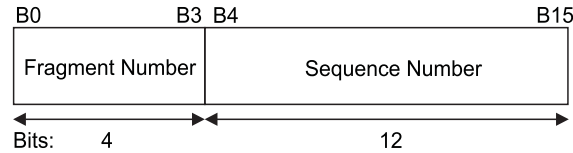


Figure 14—Sequence Control field

#### 7.1.3.4.1 Sequence Number field

The Sequence Number field is a 12-bit field indicating the sequence number of an MSDU or MMPDU. Each MSDU or MMPDU transmitted by a STA is assigned a sequence number. Sequence numbers are assigned from a single modulo 4096 counter, starting at 0 and incrementing by 1 for each MSDU or MMPDU. Each fragment of an MSDU or MMPDU contains the assigned sequence number. The sequence number remains constant in all retransmissions of an MSDU, MMPDU, or fragment thereof.

#### 7.1.3.4.2 Fragment Number field

The Fragment Number field is a 4-bit field indicating the number of each fragment of an MSDU or MMPDU. The fragment number is set to zero in the first or only fragment of an MSDU or MMPDU and is incremented by one for each successive fragment of that MSDU or MMPDU. The fragment number remains constant in all retransmissions of the fragment.

### 7.1.3.5 Frame Body field

The Frame Body is a variable length field that contains information specific to individual frame types and subtypes. The minimum frame body is 0 octets. The maximum length frame body is defined by the maximum length (MSDU + ICV + IV), where ICV and IV are the WEP fields defined in 8.2.5.

### 7.1.3.6 FCS field

The FCS field is a 32-bit field containing a 32-bit CRC. The FCS is calculated over all the fields of the MAC header and the Frame Body field. These are referred to as the *calculation fields*.

The FCS is calculated using the following standard generator polynomial of degree 32:

$$G(x) = x^{32} + x^{26} + x^{23} + x^{22} + x^{16} + x^{12} + x^{11} + x^{10} + x^8 + x^7 + x^5 + x^4 + x^2 + x + 1$$

The FCS is the 1's complement of the sum (modulo 2) of the following:

- a) The remainder of  $x^k \times (x^{31} + x^{30} + x^{29} + \dots + x^2 + x + 1)$  divided (modulo 2) by  $G(x)$ , where  $k$  is the number of bits in the calculation fields, and

- b) The remainder after multiplication of the contents (treated as a polynomial) of the calculation fields by  $x^{32}$  and then division by  $G(x)$ .

The FCS field is transmitted commencing with the coefficient of the highest-order term.

As a typical implementation, at the transmitter, the initial remainder of the division is preset to all 1's and is then modified by division of the calculation fields by the generator polynomial  $G(x)$ . The 1's complement of this remainder is transmitted, with the highest-order bit first, as the FCS field.

At the receiver, the initial remainder is preset to all 1's and the serial incoming bits of the calculation fields and FCS, when divided by  $G(x)$ , results in the absence of transmission errors, in a unique nonzero remainder value. The unique remainder value is the polynomial:

$$x^{31} + x^{30} + x^{26} + x^{25} + x^{24} + x^{18} + x^{15} + x^{14} + x^{12} + x^{11} + x^{10} + x^8 + x^6 + x^5 + x^4 + x^3 + x + 1$$

## 7.2 Format of individual frame types

### 7.2.1 Control frames

In the following descriptions, "immediately previous" frame means a frame whose reception concluded within the prior short interframe space (SIFS) interval.

The subfields within the Frame Control field of control frames are set as illustrated in Figure 15.

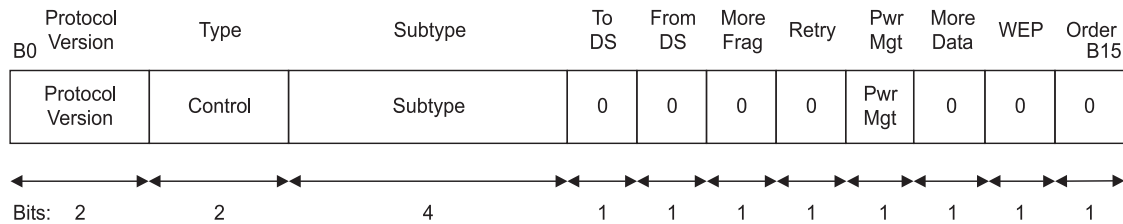


Figure 15—Frame Control field subfield values within control frames

#### 7.2.1.1 Request To Send (RTS) frame format

The frame format for the RTS frame is as defined in Figure 16.

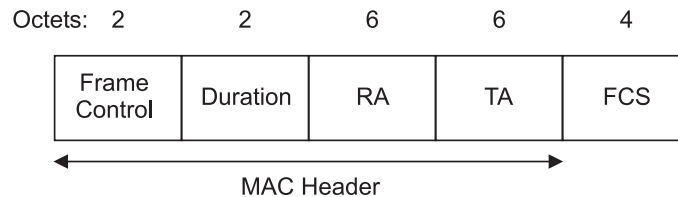


Figure 16—RTS frame

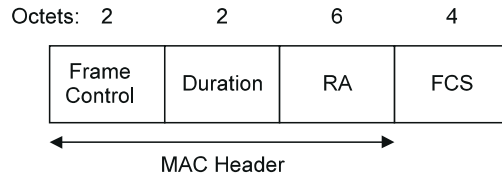
The RA of the RTS frame is the address of the STA, on the WM, that is the intended immediate recipient of the pending directed data or management frame.

The TA is the address of the STA transmitting the RTS frame.

The duration value is the time, in microseconds, required to transmit the pending data or management frame, plus one CTS frame, plus one ACK frame, plus three SIFS intervals. If the calculated duration includes a fractional microsecond, that value is rounded up to the next higher integer.

### 7.2.1.2 Clear To Send (CTS) frame format

The frame format for the CTS frame is as defined in Figure 17.



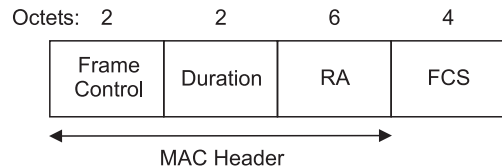
**Figure 17—CTS frame**

The RA of the CTS frame is copied from the TA field of the immediately previous RTS frame to which the CTS is a response.

The duration value is the value obtained from the Duration field of the immediately previous RTS frame, minus the time, in microseconds, required to transmit the CTS frame and its SIFS interval. If the calculated duration includes a fractional microsecond, that value is rounded up to the next higher integer.

### 7.2.1.3 Acknowledgment (ACK) frame format

The frame format for the ACK frame is as defined in Figure 18.



**Figure 18—ACK frame**

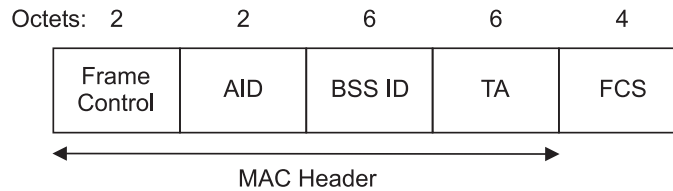
The RA of the ACK frame is copied from the Address 2 field of the immediately previous directed data, management, or PS-Poll control frame.

If the More Fragment bit was set to 0 in the Frame Control field of the immediately previous directed data or management frame, the duration value is set to 0. If the More Fragment bit was set to 1 in the Frame Control field of the immediately previous directed data or management frame, the duration value is the value obtained from the Duration field of the immediately previous data or management frame, minus the time, in microseconds, required to transmit the ACK frame and its SIFS interval. If the calculated duration includes a fractional microsecond, that value is rounded up to the next higher integer.

### 7.2.1.4 Power-Save Poll (PS-Poll) frame format

The frame format for the PS-Poll frame is as defined in Figure 19.

The BSSID is the address of the STA contained in the AP. The TA is the address of the STA transmitting the frame. The AID is the value assigned to the STA transmitting the frame by the AP in the association response frame that established that STA's current association.

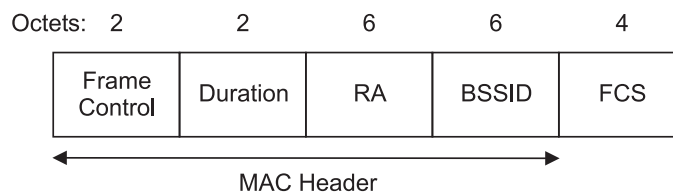


**Figure 19—PS-Poll frame**

The AID value always has its two most significant bits each set to 1. All STAs, upon receipt of a PS-Poll frame, update their NAV settings as appropriate under the coordination function rules using a duration value equal to the time, in microseconds, required to transmit one ACK frame plus one SIFS interval.

**7.2.1.5 CF-End frame format**

The frame format for the CF-End frame is as defined in Figure 20.



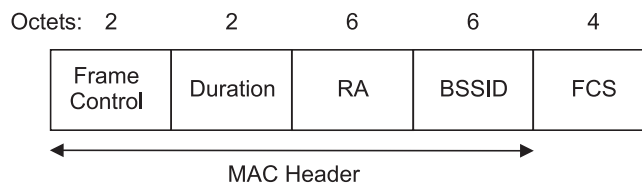
**Figure 20—CF-End frame**

The BSSID is the address of the STA contained in the AP. The RA is the broadcast group address.

The Duration field is set to 0.

**7.2.1.6 CF-End + CF-Ack frame format**

The frame format for the contention-free-end acknowledge (CF-End + CF-Ack) frame is as defined in Figure 21.



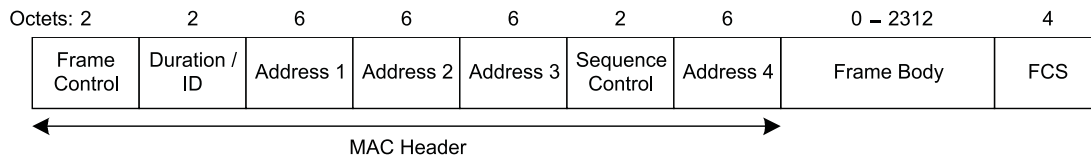
**Figure 21—CF-End + CF-Ack Frame**

The BSSID is the address of the STA contained in the AP. The RA is the broadcast group address.

The Duration field is set to 0.

**7.2.2 Data frames**

The frame format for a Data frame is independent of subtype and is as defined in Figure 22.



**Figure 22—Data frame**

The content of the Address fields of the data frame is dependent upon the values of the To DS and From DS bits and is defined in Table 4. Where the content of a field is shown as not applicable (N/A), the field is omitted. Note that Address 1 always holds the receiver address of the intended receiver (or, in the case of multi-cast frames, receivers), and that Address 2 always holds the address of the station that is transmitting the frame.

**Table 4 —Address field contents**

To DS	From DS	Address 1	Address 2	Address 3	Address 4
0	0	DA	SA	BSSID	N/A
0	1	DA	BSSID	SA	N/A
1	0	BSSID	SA	DA	N/A
1	1	RA	TA	DA	SA

A station uses the contents of the Address 1 field to perform address matching for receive decisions. In cases where the Address 1 field contains a group address, the BSSID also is validated to ensure that the broadcast or multicast originated in the same BSS.

A station uses the contents of the Address 2 field to direct the acknowledgment if an acknowledgment is necessary.

The DA is the destination of the MSDU (or fragment thereof) in the frame body field.

The SA is the address of the MAC entity that initiated the MSDU (or fragment thereof) in the frame body field.

The RA is the address of the STA contained in the AP in the wireless distribution system that is the next immediate intended recipient of the frame.

The TA is the address of the STA contained in the AP in the wireless distribution system that is transmitting the frame.

The BSSID of the Data frame is determined as follows:

- a) If the station is an AP or is associated with an AP, the BSSID is the address currently in use by the STA contained in the AP.
- b) If the station is a member of an IBSS, the BSSID is the BSSID of the IBSS.

The frame body consists of the MSDU or a fragment thereof, and a WEP IV and ICV (if and only if the WEP subfield in the frame control field is set to 1). The frame body is null (0 octets in length) in data frames of Subtype Null function (no data), CF-Ack (no data), CF-Poll (no data), and CF-Ack+CF-Poll (no data).

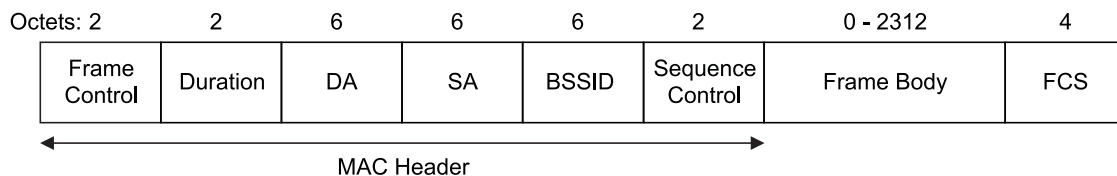
Within all data type frames sent during the CFP, the Duration field is set to the value 32 768. Within all data type frames sent during the contention period, the Duration field is set according to the following rules:

- If the Address 1 field contains a group address, the duration value is set to 0.
- If the More Fragments bit is set to 0 in the Frame Control field of a frame and the Address 1 field contains an individual address, the duration value is set to the time, in microseconds, required to transmit one ACK frame, plus one SIFS interval.
- If the More Fragments bit is set to 1 in the Frame Control field of a frame, and the Address 1 field contains an individual address, the duration value is set to the time, in microseconds, required to transmit the next fragment of this data frame, plus two ACK frames, plus three SIFS intervals.

The duration value calculation for the data frame is based on the rules in 9.6 that determine the data rate at which the control frames in the frame exchange sequence are transmitted. If the calculated duration includes a fractional microsecond, that value is rounded up to the next higher integer. All stations process Duration field values less than or equal to 32 767 from valid data frames to update their NAV settings as appropriate under the coordination function rules.

### 7.2.3 Management frames

The frame format for a Management frame is independent of frame subtype and is as defined in Figure 23.



**Figure 23—Management frame format**

A STA uses the contents of the Address 1 field to perform the address matching for receive decisions. In the case where the Address 1 field contains a group address and the frame type is other than Beacon, the BSSID also is validated to ensure that the broadcast or multicast originated in the same BSS. If the frame type is Beacon, other address matching rules apply, as specified in 11.1.2.3.

The address fields for management frames do not vary by frame subtype.

The BSSID of the management frame is determined as follows:

- a) If the station is an AP or is associated with an AP, the BSSID is the address currently in use by the STA contained in the AP.
- b) If the station is a member of an IBSS, the BSSID is the BSSID of the IBSS.
- c) In Management frames of subtype Probe Request, the BSSID is either a specific BSSID, or the broadcast BSSID as defined in the procedures specified in Clause 10.

The DA is the destination of the frame.

The SA is the address of the station transmitting the frame.

Within all management type frames sent during the CFP, the Duration field is set to the value 32 768. Within all management type frames sent during the contention period, the Duration field is set according to the following rules:

- If the DA field contains a group address, the duration value is set to 0.
- If the More Fragments bit is set to 0 in the Frame Control field of a frame and the DA contains an individual address, the duration value is set to the time, in microseconds, required to transmit one ACK frame, plus one SIFS interval.
- If the More Fragments bit is set to 1 in the Frame Control field of a frame, and the DA contains an individual address, the duration value is the time, in microseconds, required to transmit the next fragment of this management frame, plus two ACK frames, plus three SIFS intervals.

The duration value calculation for the management frame is based on the rules in 9.6 that determine the data rate at which the control frames in the frame exchange sequence are transmitted. If the calculated duration includes a fractional microsecond, that value is rounded up to the next higher integer. All stations process Duration field values less than or equal to 32 767 from valid management frames to update their NAV settings as appropriate under the coordination function rules.

The frame body consists of the fixed fields and information elements defined for each management frame subtype. All fixed fields and information elements are mandatory unless stated otherwise, and they can appear only in the specified order. Stations encountering an element type they do not understand ignore that element. Element type codes not explicitly defined in this standard are reserved, and do not appear in any frames.

### 7.2.3.1 Beacon frame format

The frame body of a management frame of subtype Beacon contains the information shown in Table 5.

**Table 5—Beacon frame body**

Order	Information	Notes
1	Timestamp	
2	Beacon interval	
3	Capability information	
4	SSID	
5	Supported rates	
6	FH Parameter Set	The FH Parameter Set information element is present within Beacon frames generated by STAs using frequency-hopping PHYs.
7	DS Parameter Set	The DS Parameter Set information element is present within Beacon frames generated by STAs using direct sequence PHYs.
8	CF Parameter Set	The CF Parameter Set information element is only present within Beacon frames generated by APs supporting a PCF.
9	IBSS Parameter Set	The IBSS Parameter Set information element is only present within Beacon frames generated by STAs in an IBSS.
10	TIM	The TIM information element is only present within Beacon frames generated by APs.

### 7.2.3.2 IBSS Announcement Traffic Indication Message (ATIM) frame format

The frame body of a management frame of subtype ATIM is null.

### 7.2.3.3 Disassociation frame format

The frame body of a management frame of subtype Disassociation contains the information shown in Table 6.

**Table 6—Disassociation frame body**

Order	Information
1	Reason code

### 7.2.3.4 Association Request frame format

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

**Table 7 —Association Request frame body**

Order	Information
1	Capability information
2	Listen interval
3	SSID
4	Supported rates

### 7.2.3.5 Association Response frame format

The frame body of a management frame of subtype Association Response contains the information shown in Table 8.

**Table 8—Association Response frame body**

Order	Information
1	Capability information
2	Status code
3	Association ID (AID)
4	Supported rates

### 7.2.3.6 Reassociation Request frame format

The frame body of a management frame of subtype Reassociation Request contains the information shown in Table 9.

**Table 9—Reassociation Request frame body**

Order	Information
1	Capability information
2	Listen interval
3	Current AP address
4	SSID
5	Supported rates

**7.2.3.7 Reassociation Response frame format**

The frame body of a management frame of subtype Reassociation Response contains the information shown in Table 10.

**Table 10—Reassociation Response frame body**

Order	Information
1	Capability information
2	Status code
3	Association ID (AID)
4	Supported rates

**7.2.3.8 Probe Request frame format**

The frame body of a management frame of subtype Probe Request contains the information shown in Table 11.

**Table 11—Probe Request frame body**

Order	Information
1	SSID
2	Supported rates

**7.2.3.9 Probe Response frame format**

The frame body of a management frame of subtype Probe Response contains the information shown in Table 12.

**Table 12—Probe Response frame body**

Order	Information	Notes
1	Timestamp	
2	Beacon interval	
3	Capability information	
4	SSID	
5	Supported rates	
6	FH Parameter Set	The FH Parameter Set information element is present within Probe Response frames generated by STAs using frequency-hopping PHYs.
7	DS Parameter Set	The DS Parameter Set information element is present within Probe Response frames generated by STAs using direct sequence PHYs.
8	CF Parameter Set	The CF Parameter Set information element is only present within Probe Response frames generated by APs supporting a PCF.
9	IBSS Parameter Set	The IBSS Parameter Set information element is only present within Probe Response frames generated by STAs in an IBSS.

**7.2.3.10 Authentication frame format**

The frame body of a management frame of subtype Authentication contains the information shown in Table 13.

**Table 13—Authentication frame body**

Order	Information	Notes
1	Authentication algorithm number	
2	Authentication transaction sequence number	
3	Status code	The status code information is reserved and set to 0 in certain Authentication frames as defined in Table 14.
4	Challenge text	The challenge text information is only present in certain Authentication frames as defined in Table 14.

**Table 14—Presence of challenge text information**

Authentication algorithm	Authentication transaction sequence no.	Status code	Challenge text
Open System	1	Reserved	Not present
Open System	2	Status	Not present
Shared Key	1	Reserved	Not present
Shared Key	2	Status	Present
Shared Key	3	Reserved	Present
Shared Key	4	Status	Not present

### 7.2.3.11 Deauthentication

The frame body of a management frame of subtype Deauthentication contains the information shown in Table 15.

**Table 15—Deauthentication frame body**

Order	Information
1	Reason code

## 7.3 Management frame body components

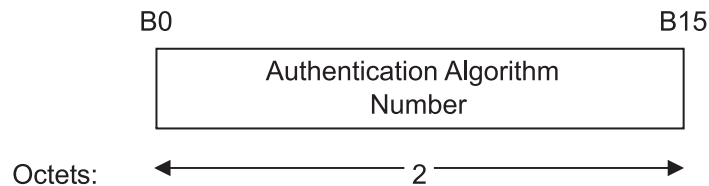
Within management frames, fixed-length mandatory frame body components are defined as fixed fields; variable length mandatory and all optional frame body components are defined as information elements.

### 7.3.1 Fixed fields

#### 7.3.1.1 Authentication Algorithm Number field

The Authentication Algorithm Number field indicates a single authentication algorithm. The length of the Authentication Algorithm Number field is 2 octets. The Authentication Algorithm Number field is illustrated in Figure 24. The following values are defined for authentication algorithm number:

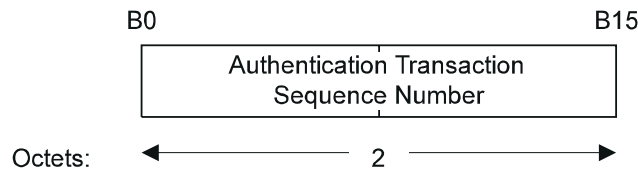
- Authentication algorithm number = 0: Open System
- Authentication algorithm number = 1: Shared Key
- All other values of authentication number are reserved.



**Figure 24—Authentication Algorithm Number fixed field**

#### 7.3.1.2 Authentication Transaction Sequence Number field

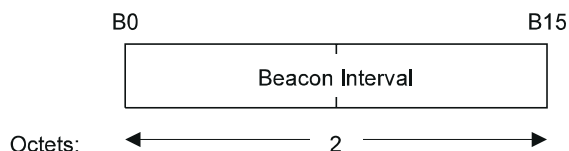
The Authentication Transaction Sequence Number field indicates the current state of progress through a multistep transaction. The length of the Authentication Transaction Sequence Number field is 2 octets. The Authentication Transaction Sequence Number field is illustrated in Figure 25.



**Figure 25—Authentication Transaction Sequence Number fixed field**

### 7.3.1.3 Beacon Interval field

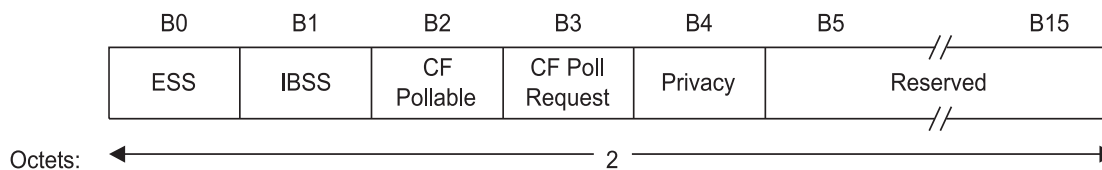
The Beacon Interval field represents the number of time units (TUs) between target beacon transmission times (TBTTs). The length of the Beacon Interval field is 2 octets. The Beacon Interval field is illustrated in Figure 26.



**Figure 26—Beacon Interval fixed field**

### 7.3.1.4 Capability Information field

The Capability Information field contains a number of subfields that are used to indicate requested or advertised capabilities. The length of the Capability Information field is 2 octets. The Capability Information field consists of the following subfields: ESS, IBSS, CF-Pollable, CF-Poll Request, and Privacy. The remaining part of the Capability Information field is reserved. The format of the Capability Information field is as illustrated in Figure 27.



**Figure 27—Capability Information fixed field**

Each Capability Information subfield is interpreted only in the management frame subtypes for which the transmission rules are defined.

APs set the ESS subfield to 1 and the IBSS subfield to 0 within transmitted Beacon or Probe Response management frames. STAs within an IBSS set the ESS subfield to 0 and the IBSS subfield to 1 in transmitted Beacon or Probe Response management frames.

STAs set the CF-Pollable and CF-Poll Request subfields in Association and Reassociation Request management frames according to Table 16.

**Table 16—STA usage of CF-Pollable and CF-Poll Request**

CF-Pollable	CF-Poll request	Meaning
0	0	STA is not CF-Pollable
0	1	STA is CF-Pollable, not requesting to be placed on the CF-Polling list
1	0	STA is CF-Pollable, requesting to be placed on the CF-Polling list
1	1	STA is CF-Pollable, requesting never to be polled

APs set the CF-Pollable and CF-Poll Request subfields in Beacon, Probe Response, Association Response, and Reassociation Response management frames according to Table 17. An AP sets the CF-Pollable and CF-Poll Request subfield values in Association Response and Reassociation Response management frames equal to the values in the last Beacon or Probe Response frame that it transmitted.

**Table 17—AP usage of CF-Pollable and CF-Poll Request**

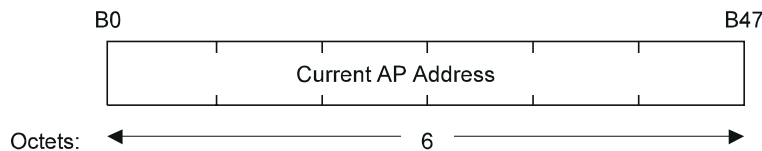
CF-Pollable	CF-Poll Request	Meaning
0	0	No point coordinator at AP
0	1	Point coordinator at AP for delivery only (no polling)
1	0	Point coordinator at AP for delivery and polling
1	1	Reserved

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

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

**7.3.1.5 Current AP Address field**

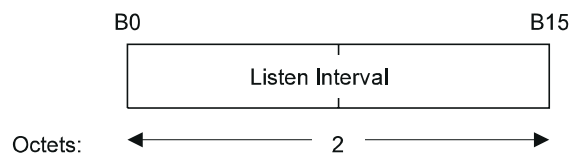
The Current AP Address field is the MAC address of the AP with which the station is currently associated. The length of the Current AP Address field is 6 octets. The Current AP Address field is illustrated in Figure 28.



**Figure 28—Current AP Address fixed field**

**7.3.1.6 Listen Interval field**

The Listen Interval field is used to indicate to the AP how often an STA wakes to listen to Beacon management frames. The value of this parameter is the STA’s Listen Interval parameter of the MLME-Associate.request primitive and is expressed in units of Beacon Interval. The length of the Listen Interval field is 2 octets. The Listen Interval field is illustrated in Figure 29.

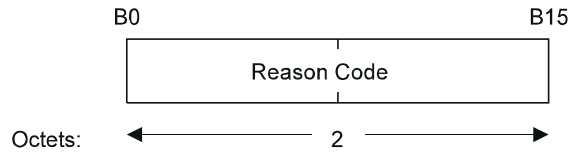


**Figure 29—Listen Interval fixed field**

An AP may use the Listen Interval information in determining the lifetime of frames that it buffers for an STA.

### 7.3.1.7 Reason Code field

This Reason Code field is used to indicate the reason that an unsolicited notification management frame of type Disassociation or Deauthentication was generated. The length of the Reason Code field is 2 octets. The Reason Code field is illustrated in Figure 30.



**Figure 30—Reason Code fixed field**

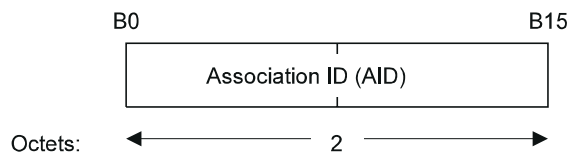
The reason codes are defined in Table 18.

**Table 18—Reason codes**

Reason code	Meaning
0	Reserved
1	Unspecified reason
2	Previous authentication no longer valid
3	Deauthenticated because sending station is leaving (or has left) IBSS or ESS
4	Disassociated due to inactivity
5	Disassociated because AP is unable to handle all currently associated stations
6	Class 2 frame received from nonauthenticated station
7	Class 3 frame received from nonassociated station
8	Disassociated because sending station is leaving (or has left) BSS
9	Station requesting (re)association is not authenticated with responding station
10–65 535	Reserved

### 7.3.1.8 Association ID (AID) field

The AID field is a value assigned by an AP during association that represents the 16-bit ID of a STA. The length of the AID field is 2 octets. The AID field is illustrated in Figure 31.

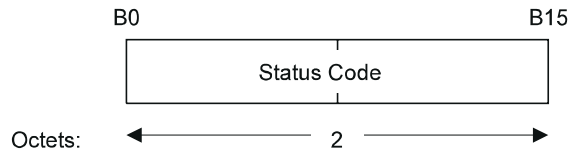


**Figure 31—AID fixed field**

The value assigned as the Association ID is in the range 1–2007 and is placed in the 14 least significant bits of the AID field, with the two most significant bits of the AID field each set to 1 (see 7.1.3.2).

### 7.3.1.9 Status Code field

The Status Code field is used in a response management frame to indicate the success or failure of a requested operation. The length of the Status Code field is 2 octets. The Status Code field is illustrated in Figure 32.



**Figure 32—Status Code fixed field**

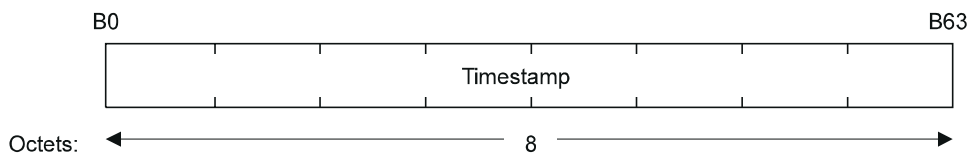
If an operation is successful, then the status code is set to 0. If an operation results in failure, the status code indicates a failure cause. The failure cause codes are defined in Table 19.

**Table 19—Status codes**

Status code	Meaning
0	Successful
1	Unspecified failure
2–9	Reserved
10	Cannot support all requested capabilities in the Capability Information field
11	Reassociation denied due to inability to confirm that association exists
12	Association denied due to reason outside the scope of this standard
13	Responding station does not support the specified authentication algorithm
14	Received an Authentication frame with authentication transaction sequence number out of expected sequence
15	Authentication rejected because of challenge failure
16	Authentication rejected due to timeout waiting for next frame in sequence
17	Association denied because AP is unable to handle additional associated stations
18	Association denied due to requesting station not supporting all of the data rates in the BSSBasicRateSet parameter
19–65 535	Reserved

### 7.3.1.10 Timestamp field

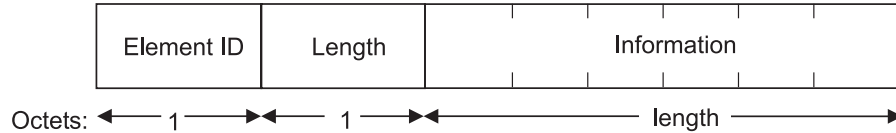
This field represents the value of the TSFTIMER (see 11.1) of a frame’s source. The length of the Timestamp field is 8 octets. The Timestamp field is illustrated in Figure 33.



**Figure 33—Timestamp fixed field**

### 7.3.2 Information elements

Elements are defined to have a common general format consisting of a 1 octet Element ID field, a 1 octet length field, and a variable-length element-specific information field. Each element is assigned a unique Element ID as defined in this standard. The Length field specifies the number of octets in the Information field. See Figure 34.



**Figure 34—Element format**

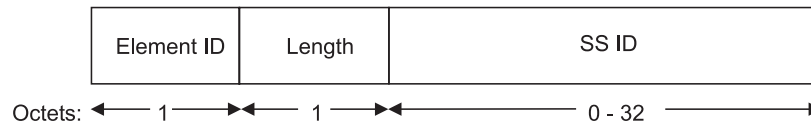
The set of valid elements is defined in Table 20.

**Table 20—Element IDs**

Information element	Element ID
SSID	0
Supported rates	1
FH Parameter Set	2
DS Parameter Set	3
CF Parameter Set	4
TIM	5
IBSS Parameter Set	6
Reserved	7–15
Challenge text	16
Reserved for challenge text extension	17–31
Reserved	32–255

#### 7.3.2.1 Service Set Identity (SSID) element

The SSID element indicates the identity of an ESS or IBSS. See Figure 35.



**Figure 35—SSID element format**

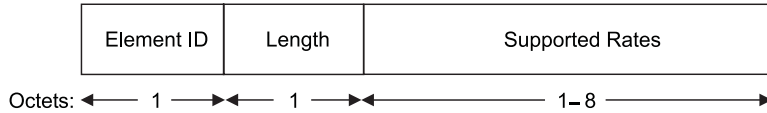
The length of the SSID information field is between 0 and 32 octets. A 0 length information field indicates the broadcast SSID.

#### 7.3.2.2 Supported Rates element

The Supported Rates element specifies the rates in the Operational Rate Set as described in the MLME\_Join.request and MLME\_Start.request primitives. The information field is encoded as 1 to 8 octets where each octet describes a single supported rate in units of 500 kbit/s.

Within Beacon, Probe Response, Association Response, and Reassociation Response management frames, each supported rate belonging to the BSSBasicRateSet, as defined in 10.3.10.1, is encoded as an octet with the msb (bit 7) set to 1 (e.g., a 1 Mbit/s rate belonging to the BSSBasicRateSet is encoded as X'82'). Rates not belonging to the BSSBasicRateSet are encoded with the msb set to 0 (e.g., a 2 Mbit/s rate not belonging to the BSSBasicRateSet is encoded as X'04'). The msb of each Supported Rate octet in other management frame types is ignored by receiving STAs.

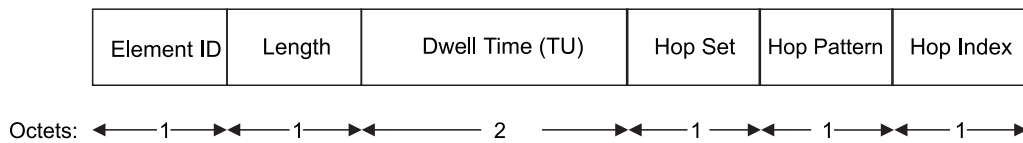
BSSBasicRateSet information in Beacon and Probe Response management frames is used by STAs in order to avoid associating with a BSS if they do not support all the data rates in the BSSBasicRateSet. See Figure 36.



**Figure 36—Supported rates element format**

### 7.3.2.3 FH Parameter Set element

The FH Parameter Set element contains the set of parameters necessary to allow synchronization for STAs using a frequency-hopping (FH) PHY. The information field contains Dwell Time, Hop Set, Hop Pattern, and Hop Index parameters. The total length of the information field is 5 octets. See Figure 37.



**Figure 37—FH Parameter Set element format**

The Dwell Time field is 2 octets in length and contains the dwell time in TU.

The Hop Set field identifies the current set (dot11CurrentSet) of hop patterns and is a single octet.

The Hop Pattern field identifies the current pattern (dot11CurrentPattern) within a set of hop patterns and is a single octet.

The Hop Index field selects the current index (dot11CurrentIndex) within a pattern and is a single octet.

The description of the attributes used in this subclause can be found in 14.8.2.1.

### 7.3.2.4 DS Parameter Set element

The DS Parameter Set element contains information to allow channel number identification for STAs using a direct sequence spread spectrum (DSSS) PHY. The information field contains a single parameter containing the dot11CurrentChannelNumber (see 15.4.6.2 for values). The length of the dot11CurrentChannelNumber parameter is 1 octet. See Figure 38.

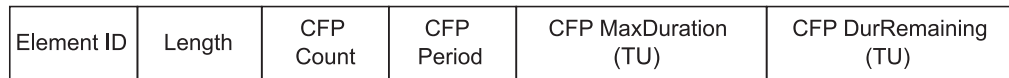
### 7.3.2.5 CF Parameter Set element

The CF Parameter Set element contains the set of parameters necessary to support the PCF. The information field contains the CFPCount, CFPPeriod, CFPMaxDuration, and CFPDurRemaining fields. The total length of the information field is 6 octets. See Figure 39.



Octets: ← 1 → ← 1 → ← 1 →

**Figure 38—DS Parameter Set element format**



Octets: ← 1 → ← 1 → ← 1 → ← 1 → ← 2 → ← 2 →

**Figure 39—CF Parameter Set element format**

CFPCount indicates how many DTIMs (including the current frame) appear before the next CFP start. A CFPCount of 0 indicates that the current DTIM marks the start of the CFP.

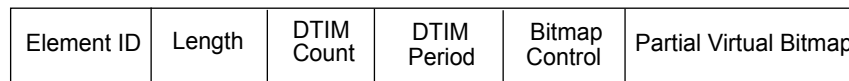
CFPPeriod indicates the number of DTIM intervals between the start of CFPs. The value is an integral number of DTIM intervals.

CFPMaxDuration indicates the maximum duration, in TU, of the CFP that may be generated by this PCF. This value is used by STAs to set their NAV at the TBTT of beacons that begin CFPs.

CFPDurRemaining indicates the maximum time, in TU, remaining in the present CFP, and is set to zero in CFP Parameter elements of beacons transmitted during the contention period. The value of CFPDurRemaining is referenced to the immediately previous TBTT. This value is used by all STAs to update their NAVs during CFPs.

### 7.3.2.6 TIM

The TIM element contains four fields: DTIM Count, DTIM Period, Bitmap Control, and Partial Virtual Bitmap. See Figure 40.



Octets: ← 1 → ← 1 → ← 1 → ← 1 → ← 1 → ← 1-251 →

**Figure 40—TIM element format**

The Length field for this element indicates the length of the information field, which is constrained as described below.

The DTIM Count field indicates how many beacons (including the current frame) appear before the next DTIM. A DTIM Count of 0 indicates that the current TIM is a DTIM. The DTIM count field is a single octet.

The DTIM Period field indicates the number of Beacon intervals between successive DTIMs. If all TIMs are DTIMs, the DTIM Period field has the value 1. The DTIM Period value 0 is reserved. The DTIM period field is a single octet.

The Bitmap Control field is a single octet. Bit 0 of the field contains the Traffic Indicator bit associated with Association ID 0. This bit is set to 1 in TIM elements with a value of 0 in the DTIM Count field when one or

more broadcast or multicast frames are buffered at the AP. The remaining 7 bits of the field form the Bitmap Offset.

The traffic-indication virtual bitmap, maintained by the AP that generates a TIM, consists of 2008 bits, and is organized into 251 octets such that bit number  $N$  ( $0 \leq N \leq 2007$ ) in the bitmap corresponds to bit number  $(N \bmod 8)$  in octet number  $\lfloor N/8 \rfloor$  where the low-order bit of each octet is bit number 0, and the high order bit is bit number 7. Each bit in the traffic-indication virtual bitmap corresponds to traffic buffered for a specific station within the BSS that the AP is prepared to deliver at the time the beacon frame is transmitted. Bit number  $N$  is 0 if there are no directed frames buffered for the station whose Association ID is  $N$ . If any directed frames for that station are buffered and the AP is prepared to deliver them, bit number  $N$  in the traffic-indication virtual bitmap is 1. A PC may decline to set bits in the TIM for CF-Pollable stations it does not intend to poll (see 11.2.1.5).

The Partial Virtual Bitmap field consists of octets numbered  $N1$  through  $N2$  of the traffic indication virtual bitmap, where  $N1$  is the largest even number such that bits numbered 1 through  $(N1 \times 8) - 1$  in the bitmap are all 0 and  $N2$  is the smallest number such that bits numbered  $(N2 + 1) \times 8$  through 2007 in the bitmap are all 0. In this case, the Bitmap Offset subfield value contains the number  $\lfloor N1/2 \rfloor$ , and the Length field will be set to  $(N2 - N1) + 4$ .

In the event that all bits other than bit 0 in the virtual bitmap are 0, the Partial Virtual Bitmap field is encoded as a single octet equal to 0, and the Bitmap Offset subfield is 0.

### 7.3.2.7 IBSS Parameter Set element

The IBSS Parameter Set element contains the set of parameters necessary to support an IBSS. The information field contains the ATIM Window parameter. See Figure 41.

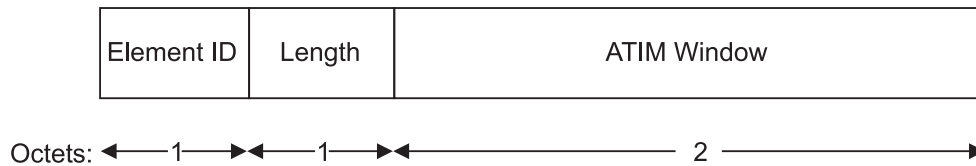


Figure 41—IBSS Parameter Set element format

The ATIM Window field is 2 octets in length and contains the ATIM Window length in TU.

### 7.3.2.8 Challenge Text element

The Challenge Text element contains the challenge text within Authentication exchanges. The element information field length is dependent upon the authentication algorithm and the transaction sequence number as specified in 8.1. See Figure 42.

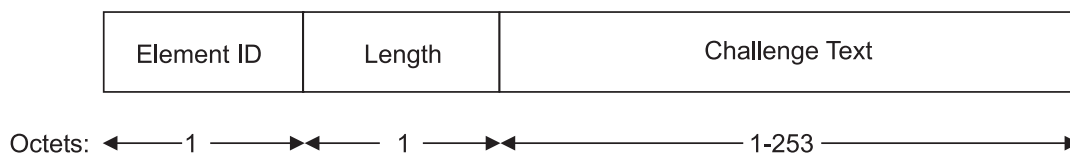


Figure 42—Challenge Text element format