

# EXHIBIT 1

UNITED STATES DISTRICT COURT

for the

District of Columbia

Nokia Corporation
Plaintiff
v.
Apple, Inc.
Defendant
Civil Action No. 09-cv-791-GMS
(If the action is pending in another district, state where:
District of Delaware)

SUBPOENA TO TESTIFY AT A DEPOSITION IN A CIVIL ACTION

To: The Institute of Electrical and Electronics Engineers, Inc. ("IEEE"), c/o Chris Brantley, Registered Agent, 2001 L St., N.W., Suite 700, Washington, D.C., 20036

Testimony: YOU ARE COMMANDED to appear at the time, date, and place set forth below to testify at a deposition to be taken in this civil action. If you are an organization that is not a party in this case, you must designate one or more officers, directors, or managing agents, or designate other persons who consent to testify on your behalf about the following matters, or those set forth in an attachment:

SEE ATTACHMENT A / SCHEDULE B

Table with 2 columns: Place (WilmerHale LLP, 1875 Pennsylvania Ave., NW, Washington, D.C., 20006) and Date and Time (06/24/2011 9:00 am)

The deposition will be recorded by this method: Videographer and stenographer

Production: You, or your representatives, must also bring with you to the deposition the following documents, electronically stored information, or objects, and permit their inspection, copying, testing, or sampling of the material:

SEE ATTACHMENT A / SCHEDULE A

The provisions of Fed. R. Civ. P. 45(c), relating to your protection as a person subject to a subpoena, and Rule 45 (d) and (e), relating to your duty to respond to this subpoena and the potential consequences of not doing so, are attached.

Date: 05/23/2011

CLERK OF COURT

Signature of Clerk or Deputy Clerk OR Attorney's Signature (Mina Tallon)

The name, address, e-mail, and telephone number of the attorney representing (name of party) Apple, Inc., who issues or requests this subpoena, are:

Nina Tallon, Esq., Wilmer Cutler Pickering Hale and Dorr LLP, 1875 Pennsylvania Avenue, NW, Washington, DC 20006
Nina.Tallon@wilmerhale.com, (202) 663-6000

Civil Action No. 09-cv-791-GMS

**PROOF OF SERVICE**

*(This section should not be filed with the court unless required by Fed. R. Civ. P. 45.)*

This subpoena for *(name of individual and title, if any)* \_\_\_\_\_  
was received by me on *(date)* \_\_\_\_\_.

I served the subpoena by delivering a copy to the named individual as follows: \_\_\_\_\_

\_\_\_\_\_ on *(date)* \_\_\_\_\_; or

I returned the subpoena unexecuted because: \_\_\_\_\_

Unless the subpoena was issued on behalf of the United States, or one of its officers or agents, I have also  
tendered to the witness fees for one day's attendance, and the mileage allowed by law, in the amount of  
\$ \_\_\_\_\_.

My fees are \$ \_\_\_\_\_ for travel and \$ \_\_\_\_\_ for services, for a total of \$ 0.00.

I declare under penalty of perjury that this information is true.

Date: \_\_\_\_\_

\_\_\_\_\_  
*Server's signature*

\_\_\_\_\_  
*Printed name and title*

\_\_\_\_\_  
*Server's address*

Additional information regarding attempted service, etc:

**Federal Rule of Civil Procedure 45 (c), (d), and (e) (Effective 12/1/07)**

**(c) Protecting a Person Subject to a Subpoena.**

**(1) *Avoiding Undue Burden or Expense; Sanctions.*** A party or attorney responsible for issuing and serving a subpoena must take reasonable steps to avoid imposing undue burden or expense on a person subject to the subpoena. The issuing court must enforce this duty and impose an appropriate sanction — which may include lost earnings and reasonable attorney’s fees — on a party or attorney who fails to comply.

**(2) *Command to Produce Materials or Permit Inspection.***

**(A) *Appearance Not Required.*** A person commanded to produce documents, electronically stored information, or tangible things, or to permit the inspection of premises, need not appear in person at the place of production or inspection unless also commanded to appear for a deposition, hearing, or trial.

**(B) *Objections.*** A person commanded to produce documents or tangible things or to permit inspection may serve on the party or attorney designated in the subpoena a written objection to inspecting, copying, testing or sampling any or all of the materials or to inspecting the premises — or to producing electronically stored information in the form or forms requested. The objection must be served before the earlier of the time specified for compliance or 14 days after the subpoena is served. If an objection is made, the following rules apply:

**(i)** At any time, on notice to the commanded person, the serving party may move the issuing court for an order compelling production or inspection.

**(ii)** These acts may be required only as directed in the order, and the order must protect a person who is neither a party nor a party’s officer from significant expense resulting from compliance.

**(3) *Quashing or Modifying a Subpoena.***

**(A) *When Required.*** On timely motion, the issuing court must quash or modify a subpoena that:

**(i)** fails to allow a reasonable time to comply;

**(ii)** requires a person who is neither a party nor a party’s officer to travel more than 100 miles from where that person resides, is employed, or regularly transacts business in person — except that, subject to Rule 45(c)(3)(B)(iii), the person may be commanded to attend a trial by traveling from any such place within the state where the trial is held;

**(iii)** requires disclosure of privileged or other protected matter, if no exception or waiver applies; or

**(iv)** subjects a person to undue burden.

**(B) *When Permitted.*** To protect a person subject to or affected by a subpoena, the issuing court may, on motion, quash or modify the subpoena if it requires:

**(i)** disclosing a trade secret or other confidential research, development, or commercial information;

**(ii)** disclosing an unretained expert’s opinion or information that does not describe specific occurrences in dispute and results from the expert’s study that was not requested by a party; or

**(iii)** a person who is neither a party nor a party’s officer to incur substantial expense to travel more than 100 miles to attend trial.

**(C) *Specifying Conditions as an Alternative.*** In the circumstances described in Rule 45(c)(3)(B), the court may, instead of quashing or modifying a subpoena, order appearance or production under specified conditions if the serving party:

**(i)** shows a substantial need for the testimony or material that cannot be otherwise met without undue hardship; and

**(ii)** ensures that the subpoenaed person will be reasonably compensated.

**(d) Duties in Responding to a Subpoena.**

**(1) *Producing Documents or Electronically Stored Information.*** These procedures apply to producing documents or electronically stored information:

**(A) *Documents.*** A person responding to a subpoena to produce documents must produce them as they are kept in the ordinary course of business or must organize and label them to correspond to the categories in the demand.

**(B) *Form for Producing Electronically Stored Information Not Specified.*** If a subpoena does not specify a form for producing electronically stored information, the person responding must produce it in a form or forms in which it is ordinarily maintained or in a reasonably usable form or forms.

**(C) *Electronically Stored Information Produced in Only One Form.*** The person responding need not produce the same electronically stored information in more than one form.

**(D) *Inaccessible Electronically Stored Information.*** The person responding need not provide discovery of electronically stored information from sources that the person identifies as not reasonably accessible because of undue burden or cost. On motion to compel discovery or for a protective order, the person responding must show that the information is not reasonably accessible because of undue burden or cost. If that showing is made, the court may nonetheless order discovery from such sources if the requesting party shows good cause, considering the limitations of Rule 26(b)(2)(C). The court may specify conditions for the discovery.

**(2) *Claiming Privilege or Protection.***

**(A) *Information Withheld.*** A person withholding subpoenaed information under a claim that it is privileged or subject to protection as trial-preparation material must:

**(i)** expressly make the claim; and

**(ii)** describe the nature of the withheld documents, communications, or tangible things in a manner that, without revealing information itself privileged or protected, will enable the parties to assess the claim.

**(B) *Information Produced.*** If information produced in response to a subpoena is subject to a claim of privilege or of protection as trial-preparation material, the person making the claim may notify any party that received the information of the claim and the basis for it. After being notified, a party must promptly return, sequester, or destroy the specified information and any copies it has; must not use or disclose the information until the claim is resolved; must take reasonable steps to retrieve the information if the party disclosed it before being notified; and may promptly present the information to the court under seal for a determination of the claim. The person who produced the information must preserve the information until the claim is resolved.

**(e) *Contempt.*** The issuing court may hold in contempt a person who, having been served, fails without adequate excuse to obey the subpoena. A nonparty’s failure to obey must be excused if the subpoena purports to require the nonparty to attend or produce at a place outside the limits of Rule 45(c)(3)(A)(ii).



The examination will be taken before a Notary Public or other person authorized to administer oaths and will be recorded stenographically and by video. Testimony derived pursuant to this Notice of Deposition shall be used for any and all appropriate purposes permitted by the Federal Rules of Evidence.

You are invited to attend and cross-examine.

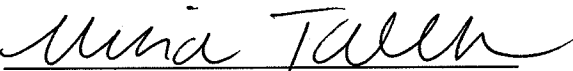
**OF COUNSEL:**

Richard L. Horwitz  
David E. Moore  
POTTER ANDERSON  
& CARROON LLP  
Hercules Plaza, 6<sup>th</sup> Floor  
1313 N. Market Street  
Wilmington, DE 19899  
Tel: (302) 984-6000

Kenneth H. Bridges  
Michael T. Pieja  
BRIDGES & MAVRAKAKIS LLP  
540 Cowper Street  
Suite 100  
Palo Alto, CA 94301  
Tel: (650) 681-4475

Dated: May 23, 2011

**WILMER CUTLER PICKERING HALE  
AND DORR LLP**

By: 

Nina S. Tallon (*Pro Hac Vice*)  
1875 Pennsylvania Avenue, NW  
Washington, DC 20006  
Tel: (202) 663-6000  
[Nina.Tallon@wilmerhale.com](mailto:Nina.Tallon@wilmerhale.com)

William F. Lee (*Pro Hac Vice*)  
60 State Street  
Boston, Massachusetts 02109  
Tel: (617) 526-6000  
[William.Lee@wilmerhale.com](mailto:William.Lee@wilmerhale.com)

Mark D. Selwyn (*Pro Hac Vice*)  
950 Page Mill Road  
Palo Alto, California 94304  
Tel: (650) 858-6000  
[Mark.Selwyn@wilmerhale.com](mailto:Mark.Selwyn@wilmerhale.com)

*Attorneys for Defendant and  
Counterclaim-Plaintiff Apple Inc.*

## ATTACHMENT A

### DEFINITIONS

The following definitions are applicable herein:

1. “You,” “your,” and IEEE refers to the Institute of Electronic and Electrical Engineers, Inc. (“IEEE”) and the Electronics Engineers Standards Association (“IEEE-SA”), or any other person who acted on or purported to act on IEEE’s behalf.
2. “Apple” means and refers to defendant and counterclaim plaintiff Apple, Inc., its officers, directors, employees, partners, corporate parent, subsidiaries, affiliates, divisions, attorneys, and agents.
3. “Nokia” collectively means and refers to plaintiff and counterclaim defendants Nokia Corporation and Nokia, Inc. and includes, without limitation, each of its predecessors, present or former parents, subsidiaries, affiliated or controlled companies or joint ventures, its respective current or former directors, officers, employees, agents, attorneys, accountants and any other person who acted on or purported to act on their or any of their behalf.
4. “This Litigation” means and refers to the above-referenced action, entitled *Nokia Corporation v. Apple Inc., et al.*, C.A. 09-cv-791-GMS.
5. The term “communication” means the transmittal of information (in the form of facts, ideas, inquiries, or otherwise).
6. The term “document” is used in its normally broad sense as defined in Rule 34(a) of the Federal Rules of Civil Procedure, and includes, without limitation: originals, final versions, drafts and every copy of writings and printed, handwritten, typed, and other graphic or photographic matter, including microfilm of any kind or nature, recordings (tape, disk, or other) of oral communications, electronic mail, and other data compilations from which information

can be obtained, in the possession, custody, or control of IEEE.

7. The term “identify,” when referring to a person, means to give, to the extent known, the person’s full name, present or last known address and when referring to a natural person, additionally, the present or last known place of employment. The term “identify,” when referring to documents, means to give, to the extent known, the (i) type of document, (ii) general subject matter; (iii) date of the document, (iv) author(s), (v) addressee(s), and (vi) recipient(s).

8. The term “concerning” means relating to, referring to, regarding, describing, discussing, evidencing, or constituting.

9. The term “relating to” means, without limitation, concerning, alluding to, referring to, constituting, describing, discussing, evidencing, or regarding.

10. The words “and” and “or” shall be construed conjunctively or disjunctively, whichever makes this subpoena more inclusive.

11. The words “any,” “all,” and “each” shall be construed as each and every.

12. The use of the singular form of any word includes the plural, and the use of the plural form of any word includes the singular.

13. “1997 802.11 IEEE Standard” means the document captioned “IEEE Std 802.11-1997” and titled “Information Technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements – Part II: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications,” sponsored by “LAN MAN Standards Committee of the IEEE Computer Society,” approved June 26, 1997, Copyright 1997 by IEEE, ISBN 1-55937-935-9.



## INSTRUCTIONS

The following instructions are applicable herein:

1. Produce all responsive documents and things in your possession, custody, or control.
2. Produce all documents and things requested in the same file or manner in which they are kept in the usual course of business.
3. Provide the following information for any responsive document or thing withheld from production on the grounds that it is protected from disclosure by the attorney-client privilege, the work product doctrine, or any other relevant privilege:
  - a. The author of the document;
  - b. The person(s) for whom the document was prepared, to whom it was sent, or who received copies;
  - c. The date of the document;
  - d. The subject matter of the document;
  - e. The type of document (e.g., letter, memorandum, note, report, etc.);
  - f. The number of pages and attachments; and
  - g. The nature and the basis for the claim of privilege.
4. This subpoena includes documents that exist in electronic form (including electronic mail, back-up tapes, magnetic tapes, and diskettes).
5. More than one paragraph of this request may ask for the same documents. The presence of such duplication is not to be interpreted to narrow or limit the normal interpretation placed upon each individual request. Where a writing is requested in more than one numbered

paragraph, only one copy of it need be produced.

6. If you object to a request, or any part of a request, produce all documents to which your objection does not apply.

7. In the event that multiple copies of a document exist, produce every copy on which appear any notations or marking of any sort not appearing on any other copy.

8. If you are aware of a document or thing, or group of documents or things, that once existed but has been destroyed or discarded, you are requested to state the type of document or thing or group of documents or things, the date it was created, the date it was destroyed or discarded, and the identity of the persons having knowledge of the contents of the document or thing, or group of documents and things.

9. A copy of the Protective Order entered in this case is attached.

## SCHEDULE A

### DOCUMENTS REQUESTED

1. Documents sufficient to show the date of first publication of the following documents:
  - a. 1997 802.11 IEEE Standard, attached hereto as Exhibit 1.
  - b. Atungsiri et al., "Error Control for Low-bit-rate Speech Communications Systems," IEEE Proceedings I, Vol. 140, No. 2, April 1993, attached hereto as Exhibit 2.
  - c. Chen et al. "Adaptive Postfiltering for Quality Enhancement of Coded Speech," IEEE Transactions on Speech and Audio Processing, Vol. 3, No. 1, January 1995, attached hereto as Exhibit 3.
  - d. Goodman et al., "Quality of Service and Bandwidth Efficiency of Cellular Mobile Radio with Variable Bit-Rate Speech Transmission," IEEE Transactions on Vehicular Technology, Vol. Vt-32, No. 3, August 1983, attached hereto as Exhibit 4.
  - e. Kasami et al., "A Concatenated Coding Scheme for Error Control," IEEE Transactions on Communications, Vol. Com-34, No. 5, May 1986, attached hereto as Exhibit 5.
  - f. Lee, "Concatenated Coding Systems Employing a Unit-Memory Convolutional Code and a Byte-Orientated Decoding Algorithm," IEEE Transactions on Communications, Vol. Com-25, No. 10, October 1977, attached hereto as Exhibit 6.
  - g. Järvinen et al., "GSM Enhanced Full Rate Speech CodeC," IEEE Acoustics, Speech, and Signal Processing, 1997, attached hereto as Exhibit 7.

- h. Thorpe et al., "A Good Job Well Done: The Latest Wireless Codecs Deliver Wireline Quality," IEEE Speech Coding for Telecommunications Proceeding, 1997, attached hereto as Exhibit 8.
- i. Schuessler, "A Compromise MAC Protocol Concept," IEEE 802.11 Wireless Access Method and Physical Specifications, 1993, attached hereto as Exhibit 9.
- j. Heide, "The CODIAC Protocol: Centralized or Distributed Integrated Access Control (CODIAC), A Wireless MAC Protocol," IEEE 802.11 Wireless Access Method and Physical Layer Specifications, 1993, attached hereto as Exhibit 10.
- k. Diepstraten, "A Wireless MAC Protocol Comparison," IEEE 802.11 Wireless Access Method and Physical Layer Specifications, 1992, attached hereto as Exhibit 11.
- l. Goodman, "Trends in Cellular and Cordless Communications," IEEE Communications Magazine, June 1991, attached hereto as Exhibit 12.
- m. Haine, "A New Radio Access Protocol and Network Architecture for Mobile Packet Data," Gateway to the Future Technology in Motion conference, May 19-22, 1991 , attached hereto as Exhibit 13.
- n. Jubin et al., "The DARPA Packet Radio Network Protocols," Proceedings of the IEEE, vol. 75, No. 1, January 1987 ("DARPA article"), attached hereto as Exhibit 14.
- o. Rypinksi, "Sequentially-Used Common Channel Access Method," IEEE P802.11 – 802 LAN Access method for Wireless Physical Medium, 1991, attached hereto as Exhibit 15.
- p. "Distribution Systems," IEEE P802.11 – 92/64, 1992, attached hereto as Exhibit

16.

- q. "Functional Requirements," IEEE Project 802.11, Version 0.2, IEEE P902.11-92/50, 1993, attached hereto as Exhibit 17.

2. Documents sufficient to show the earliest date on which a member of the public could obtain a copy of the following documents:

- a. 1997 802.11 IEEE Standard, attached hereto as Exhibit 1.
- b. Atungsiri et al., "Error Control for Low-bit-rate Speech Communications Systems," IEEE Proceedings-I, Vol. 140, No. 2, April 1993, attached hereto as Exhibit 2.
- c. Chen et al. "Adaptive Postfiltering for Quality Enhancement of Coded Speech," IEEE Transactions on Speech and Audio Processing, Vol. 3, No. 1, January 1995, attached hereto as Exhibit 3.
- d. Goodman et al., "Quality of Service and Bandwidth Efficiency of Cellular Mobile Radio with Variable Bit-Rate Speech Transmission," IEEE Transactions on Vehicular Technology, Vol. Vt-32, No. 3, August 1983, attached hereto as Exhibit 4.
- e. Kasami et al., "A Concatenated Coding Scheme for Error Control," IEEE Transactions on Communications, Vol. Com-34, No. 5, May 1986, attached hereto as Exhibit 5.
- f. Lee, "Concatenated Coding Systems Employing a Unit-Memory Convolutional Code and a Byte-Orientated Decoding Algorithm," IEEE Transactions on Communications, Vol. Com-25, No. 10, October 1977, attached hereto as Exhibit 6.

- g. Järvinen et. al., "GSM Enhanced Full Rate Speech CodeC," IEEE Acoustics, Speech, and Signal Processing, 1997, attached hereto as Exhibit 7.
- h. Thorpe et. al., "A Good Job Well Done: The Latest Wireless Codecs Deliver Wireline Quality," IEEE Speech Coding for Telecommunications Proceeding, 1997, attached hereto as Exhibit 8.
- i. Schuessler, "A Compromise MAC Protocol Concept," IEEE 802.11 Wireless Access Method and Physical Specifications, 1993, attached hereto as Exhibit 9.
- j. Heide, "The CODIAC Protocol: Centralized or Distributed Integrated Access Control (CODIAC), A Wireless MAC Protocol," IEEE 802.11 Wireless Access Method and Physical Layer Specifications, 1993, attached hereto as Exhibit 10.
- k. Diepstraten, "A Wireless MAC Protocol Comparison," IEEE 802.11 Wireless Access Method and Physical Layer Specifications, 1992, attached hereto as Exhibit 11.
- l. Goodman, "Trends in Cellular and Cordless Communications," IEEE Communications Magazine, June 1991, attached hereto as Exhibit 12.
- m. Haine, "A New Radio Access Protocol and Network Architecture for Mobile Packet Data," Gateway to the Future Technology in Motion conference, May 19-22, 1991 , attached hereto as Exhibit 13.
- n. Jubin et al., "The DARPA Packet Radio Network Protocols," Proceedings of the IEEE, vol. 75, No. 1, January 1987 ("DARPA article"), attached hereto as Exhibit 14.
- o. Rypinksi, "Sequentially-Used Common Channel Access Method," IEEE P802.11 – 802 LAN Access method for Wireless Physical Medium, 1991, attached hereto

as Exhibit 15.

p. “Distribution Systems,” IEEE P802.11 – 92/64, 1992, attached hereto as Exhibit 16.

q. “Functional Requirements,” IEEE Project 802.11, Version 0.2, IEEE P902.11-92/50, 1993, attached hereto as Exhibit 17.

## **SCHEDULE B**

### **TOPICS**

1. The authentication of the document attached to this Schedule A as Exhibits 1-17.
2. The nature of each of the documents attached to this Schedule A as Exhibits 1-17, as a record of regularly conducted business or professional activities of IEEE, including (a) whether it is “[a] memorandum, report, [or] record... in any form, of acts, events, conditions, opinions...”; (b) whether it was “made at or near the time by, or from information transmitted by, a person with knowledge” of its contents; (c) whether it was “kept in the course of a regularly conducted business [or professional] activity” of IEEE; (d) whether “it was the regular practice of that business activity to make the memorandum, report, record or data compilation.”
3. Facts and circumstances surrounding when and how the documents attached to this Schedule A as Exhibits 1-17 first became accessible to the public.



# **Protective Order**

**IN THE UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF DELAWARE**

NOKIA CORPORATION

Plaintiff,

v.

APPLE INC.

Defendant.

C.A. No. 09-791-GMS

---

APPLE INC.

Counterclaim-Plaintiff,

v.

NOKIA CORPORATION and NOKIA INC.,

Counterclaim-Defendants.

**[PROPOSED] JOINT PROTECTIVE ORDER**

1. PURPOSES AND LIMITATIONS

This Protective Order (the “Order”) governs the production or exchange of documents and other discovery materials in connection with the above-captioned action (the “Action”) by or between the Parties and any third parties, either through the formal discovery process or informally. If discovery is sought from third parties in connection with this litigation between the Parties, and this discovery would require a third party to disclose and/or produce Confidential or Highly Confidential Information, that third party may gain the protections of this Order through a written agreement by that third party to produce documents or information pursuant to this Order and to be bound by it. Under such agreement, the Parties hereto will be bound by this Order with respect to all Confidential or Highly Confidential Information produced by that third party.

2. DEFINITIONS

2.1 Party: any party to this Action, including all of its officers, directors, employees, consultants, retained experts, and in-house counsel (and their support staff).

2.2 Discovery Material: all items or information, regardless of the medium or manner generated, stored, or maintained (including, among other things, testimony, transcripts, or tangible things) that are produced in discovery in this Action.

2.3 “CONFIDENTIAL” Information or Items: information (regardless of how generated, stored or maintained) or tangible things the Designating Party believes in good faith is not generally known to others, and that the Designating Party (i) would not normally reveal to third parties except in confidence, or has undertaken with others to maintain in confidence; or (ii) believes in good faith is protected by a right to privacy under federal or state law, or any other applicable privilege or right related to confidentiality or privacy.

2.4 “HIGHLY CONFIDENTIAL – ATTORNEYS’ EYES ONLY” Information or Items: highly sensitive “Confidential Information or Items,” the disclosure of which to another Party or non-party would create a risk of competitive injury to the Producing Party. Highly Confidential Information designations should be used only for sensitive technical, financial, competitive, or personnel information, which is not generally known by third parties and that the Producing Party would not normally reveal to third parties or would require third parties to maintain in confidence either by agreements, policies, or procedures. For example, Highly Confidential Information may include, but is not limited to, materials such as design files, design drawings, design specifications, manufacturing techniques, laboratory notebooks, prototypes, materials submitted to regulatory agencies, financial and accounting information that is not made publicly available, business and marketing plans or analyses, licenses, surveys,

customer communications, meeting minutes, employment records, training materials, information obtained from a third party pursuant to a current Non-Disclosure Agreement, and similar information provided that the materials meet the foregoing requirements.

2.5 “HIGHLY CONFIDENTIAL – SOURCE CODE” Information or Items:

include human-readable programming language text that defines software, firmware, or electronic hardware descriptions. HIGHLY CONFIDENTIAL – SOURCE CODE includes, without limitation, computer code; scripts; assembly; object code; source code listings and descriptions of source code; object code listings and descriptions of object code; Hardware Description Language (HDL); Register Transfer Level (RTL) files that describe the hardware design of any ASIC or other chip; similarly sensitive implementation details; files containing text written in “C,” “C+,” assembler, VHDL, Verilog, and digital signal processor (DSP) programming languages; “.include files;” “make” files; link files; and other human-readable text files used in the generation and/or building of software directly executed on a microprocessor, microcontroller, or DSP. The restrictions herein on HIGHLY CONFIDENTIAL – SOURCE CODE do not apply to publicly-available source code available as open source source code.

2.6 Receiving Party: a Party that receives Discovery Material from a Producing Party.

2.7 Producing Party: a Party or non-party that produces Discovery Material in this Action.

2.8 Designating Party: a Party or non-party that designates information or items that is produced in disclosures or in responses to discovery as “CONFIDENTIAL,” “HIGHLY CONFIDENTIAL – ATTORNEYS’ EYES ONLY,” or “HIGHLY CONFIDENTIAL – SOURCE CODE.”

2.9 Challenging Party: a Party that elects to initiate a challenge to a Designating Party's confidentiality designation.

2.10 Protected Material: any Discovery Material that is designated as "CONFIDENTIAL," "HIGHLY CONFIDENTIAL – ATTORNEYS' EYES ONLY," or "HIGHLY CONFIDENTIAL – SOURCE CODE."

2.11 Outside Counsel: attorneys who are not employees of a Party, but who are retained to represent or advise a Party in this Action.

2.12 In-house Counsel: attorneys who are employees of a Party.

2.13 Counsel (without qualifier): Outside Counsel and In-house Counsel (as well as their necessary support staff).

2.14 Outside Consultant: a person with specialized knowledge or experience in a matter pertinent to the Action who has been retained by, or at the direction of, a Party or its Counsel to serve as an expert witness or as a consultant in this Action, and who is not a current employee or non-litigation consultant of a Party or of a competitor of a Party and who, at the time of retention, is not anticipated to become an employee or non-litigation consultant of a Party or of a competitor of a Party.

2.15 Professional Vendors: persons or entities that provide litigation support services (*e.g.*, photocopying, videotaping, translating, preparing exhibits or demonstrations, organizing, storing, retrieving data in any form or medium etc.) and their employees and subcontractors, and who are not current employees of a Party or of a competitor of a Party, and who, at the time of retention, are not anticipated to become employees of a Party or of a competitor of a Party. This definition includes ESI vendors, professional jury or trial consultants retained in connection with this Action, and mock jurors retained by such consultants to assist

them in their work. Professional Vendors do not include consultants who fall within the definition of Outside Consultant.

3. SCOPE AND APPLICABILITY

All documents, materials, items, testimony or information designated as “CONFIDENTIAL,” “HIGHLY CONFIDENTIAL – ATTORNEYS’ EYES ONLY,” and “HIGHLY CONFIDENTIAL – SOURCE CODE,” regardless of whether stored in electronic or paper form, produced or filed with the Court, submitted to the Court in connection with a hearing or trial, or produced or served either by a Party or a third party, to or for any of the other Parties, shall be governed by this Protective Order and used only for the purposes of this Action and not for any business, patent prosecution, competitive or governmental purpose or function, and shall not be disclosed to anyone except as provided in this Protective Order, absent a specific order by the Court.

The protections conferred by this Order cover not only Protected Material (as defined above), but also any information copied or extracted therefrom, as well as all copies, excerpts, summaries, or compilations thereof. Nothing herein shall alter or change in any way the discovery provisions of the Federal Rules of Civil Procedure. Identification of any individual pursuant to this Protective Order does not make that individual available for deposition or any other form of discovery outside of the restrictions and procedures of the Federal Rules of Civil Procedure or the Local Rules of the United States District Court for the District of Delaware.

4. DURATION

The confidentiality obligations imposed by this Order shall remain in effect until a Designating Party agrees otherwise in writing or a court order otherwise directs.

5. DESIGNATING PROTECTED MATERIAL

5.1 Manner and Timing of Designations. Except as otherwise provided in this Order, or as otherwise stipulated or ordered, Discovery Material that qualifies for protection under this Order must be clearly so designated before being disclosed or produced. Designation in conformity with this Order:

(a) for information in documentary form (apart from transcripts of depositions or other pretrial or trial proceedings), the Producing Party shall affix the legend “CONFIDENTIAL,” “HIGHLY CONFIDENTIAL – ATTORNEYS’ EYES ONLY,” or “HIGHLY CONFIDENTIAL – SOURCE CODE” on each document that contains Protected Material. Unless otherwise indicated, the designation of confidentiality shall apply to the entire document. If only a portion or portions of the document qualifies for protection, the Producing Party also must clearly identify the protected portion(s) and must specify, for each portion, the level of protection being asserted “CONFIDENTIAL,” “HIGHLY CONFIDENTIAL – ATTORNEYS’ EYES ONLY,” or “HIGHLY CONFIDENTIAL – SOURCE CODE”.

(b) for testimony given in deposition or in other pretrial or trial proceedings, the Party or non-party offering or sponsoring the testimony shall identify on the record all Protected Material and further specify any portions of the testimony that qualify as “CONFIDENTIAL,” “HIGHLY CONFIDENTIAL – ATTORNEYS’ EYES ONLY,” or “HIGHLY CONFIDENTIAL – SOURCE CODE.” When impractical to identify separately each portion of testimony that is entitled to protection, and when substantial portions of the testimony may qualify for protection, the Party or non-party that sponsors, offers, or gives the testimony may invoke on the record a right to designate the entire testimony or particular topic thereof “CONFIDENTIAL,” “HIGHLY CONFIDENTIAL – ATTORNEYS’ EYES ONLY,” or

“HIGHLY CONFIDENTIAL – SOURCE CODE.” Testimony in a deposition may also be designated “CONFIDENTIAL,” “HIGHLY CONFIDENTIAL – ATTORNEYS’ EYES ONLY,” or “HIGHLY CONFIDENTIAL – SOURCE CODE” by notifying the deposing party in writing within fourteen (14) calendar days of the conclusion of the deposition. No deposition may be read or produced to anyone other than the deponent, Outside Counsel, and those qualified to see “HIGHLY CONFIDENTIAL – SOURCE CODE” material under Paragraph 7 during the fourteen (14) calendar day period following a deposition unless otherwise agreed upon among the Outside Counsel. Upon being informed that certain portions of a deposition disclose either “CONFIDENTIAL,” “HIGHLY CONFIDENTIAL – ATTORNEYS’ EYES ONLY,” or “HIGHLY CONFIDENTIAL – SOURCE CODE” information, each party must cause each copy of the transcript in its custody or control to promptly be marked with the appropriate designation.

Transcript pages containing Protected Material must contain on each page the legend “CONFIDENTIAL,” “HIGHLY CONFIDENTIAL – ATTORNEYS’ EYES ONLY,” or “HIGHLY CONFIDENTIAL – SOURCE CODE,” as instructed by the Party or non-party offering or sponsoring the witness or presenting the testimony.

(c) for electronic documents and other electronic files, the Producing Party shall affix the legend “CONFIDENTIAL,” “HIGHLY CONFIDENTIAL – ATTORNEYS’ EYES ONLY,” or “HIGHLY CONFIDENTIAL – SOURCE CODE” as appropriate to the media containing the documents, or by indicating in writing those documents designated as “CONFIDENTIAL,” “HIGHLY CONFIDENTIAL – ATTORNEYS’ EYES ONLY,” or “HIGHLY CONFIDENTIAL – SOURCE CODE.”

(d) for information produced in some form other than documentary, and for any other tangible items, the Producing Party shall affix in a prominent place on the



exterior of the container or containers in which the information or item is stored the legend “CONFIDENTIAL,” “HIGHLY CONFIDENTIAL – ATTORNEYS’ EYES ONLY,” or “HIGHLY CONFIDENTIAL – SOURCE CODE.” If only portions of the information or item warrant protection, the Producing Party, to the extent practicable, shall identify the protected portions, specifying whether they qualify as “CONFIDENTIAL,” “HIGHLY CONFIDENTIAL – ATTORNEYS’ EYES ONLY,” or “HIGHLY CONFIDENTIAL – SOURCE CODE.”

5.2 Inadvertent Failure to Designate. The inadvertent or unintentional production by the Producing Party, or any third party subject to an obligation of confidentiality, of confidential material or information without designating such material or information as “CONFIDENTIAL,” “HIGHLY CONFIDENTIAL – ATTORNEYS’ EYES ONLY,” or “HIGHLY CONFIDENTIAL – SOURCE CODE” shall not be deemed a waiver in whole or in part of a party’s claim of confidentiality, either as to that specific information or as to any other information. In the event that the Producing Party discovers that it or a third party subject to an obligation of confidentiality inadvertently or unintentionally provided Confidential Information without designation or with an improper designation, that party shall, within ten (10) business days of learning of the disclosure, by letter sent to opposing counsel, designate all documents or portions thereto containing such information “CONFIDENTIAL,” “HIGHLY CONFIDENTIAL – ATTORNEYS’ EYES ONLY,” or “HIGHLY CONFIDENTIAL – SOURCE CODE” subject to the protections of this Order, and the Receiving Party shall make all reasonable efforts to assure that the material is treated in accordance with the provisions of this Order. If inadvertently or unintentionally provided Confidential Information has been disclosed by a Receiving Party in any filing, motion, hearing, trial or proceeding, then the Receiving Party, after being duly notified by letter, shall, to the extent necessary, designate all documents or portions

containing such information as “CONFIDENTIAL,” “HIGHLY CONFIDENTIAL – ATTORNEYS’ EYES ONLY,” or “HIGHLY CONFIDENTIAL – SOURCE CODE.” To the extent this Confidential Information was submitted in a filing or motion, the party submitting the filing shall cooperate in any motion or request to the Court to seal such information, in accordance with the Court’s rules and procedures. If inadvertently or unintentionally provided Confidential Information has been disclosed by the Receiving Party to any person (including employees of the Receiving Party) that would not be entitled pursuant to Paragraph 7 to receive the Confidential Information as designated pursuant to this Paragraph, the Requesting Party shall (a) use its best efforts to retrieve all copies of the Confidential Information; (b) inform the person or persons to whom the disclosures were made of all the terms of this Order, and (c) request that such person or persons execute the “Acknowledgment and Agreement to Be Bound By Protective Order” that is attached hereto as Exhibit A. Nothing herein shall prevent the Receiving Party from challenging the propriety of the designation of the documents by submitting a written challenge to the Court.

5.3 Inadvertent Production of Work Product or Privileged Information. Any inadvertent disclosure or production of document(s) shall not be deemed a waiver of, nor prejudice to, any privilege or immunity with respect to such information or document(s) or of any work product doctrine or other immunity that may attach thereto, including without limitation the attorney-client privilege, the joint defense privilege, and the work product doctrine, provided that the producing party notifies the receiving party in writing promptly after discovery of such inadvertent production. All copies of such document(s) shall be returned to the Producing Party or destroyed within five (5) calendar days of such notice. Also within five (5) calendar days of such notice, the Producing Party shall serve a privilege log for the document(s).

The Producing Party shall maintain the referenced document(s) until the parties resolve any dispute concerning the privileged nature of such documents or the Court rules on any motion to compel such documents. If a dispute arises concerning the privileged nature of the document(s) demanded or returned, the parties shall meet and confer in good faith in an effort to resolve the dispute. If the parties are unable to resolve the dispute, the receiving party may file a motion to compel the production of such document(s). In the event of such a motion to compel, the Producing Party shall have the burden to demonstrate the claimed privilege, work product immunity or other immunity. However, in no case will the return of any demanded document be delayed or refused by reason of a party's objection to the demand or by the filing of a motion to compel, nor may a party assert the fact of the inadvertent production as a ground for any such motion. The responding party shall not use or refer to any information contained within the document(s) at issue, including in deposition or at trial or in any Court filing, unless and until such a motion to compel that document is granted by a Court, except as such information may appear in any applicable privilege log.

6. CHALLENGING CONFIDENTIALITY DESIGNATIONS

6.1 Objections to Confidentiality Designations and Judicial Intervention. Any party may object to the designation of particular "CONFIDENTIAL," "HIGHLY CONFIDENTIAL – ATTORNEYS' EYES ONLY," or "HIGHLY CONFIDENTIAL – SOURCE CODE" information by identifying the information to which the objection is made in a written notice to the party designating the disputed information. However, a Party shall not be obligated to challenge the propriety of such designations at the time made, and the failure to do so shall not preclude a subsequent challenge thereto. If the parties cannot resolve the objection, it shall be the obligation of the party challenging the "CONFIDENTIAL," "HIGHLY

CONFIDENTIAL – ATTORNEYS’ EYES ONLY,” or “HIGHLY CONFIDENTIAL – SOURCE CODE” designation to file and serve a motion in compliance with Local Rule 5.1.3, if applicable, that identifies the challenged material and sets forth in detail the basis for the challenge.

6.2 Meet and Confer. A Party that elects to initiate a challenge to a Designating Party’s confidentiality designation, or Challenging Party, must do so in good faith and must begin the process by conferring with the Designating Party. In conferring, the Challenging Party must explain the basis for its belief that the confidentiality designation was not proper and must give the Designating Party an opportunity to review the designated material, to reconsider the circumstances, and, if no change in designation is offered, to explain the basis for the chosen designation. The Designating Party must cooperate in scheduling such conference. If the Designating Party is unavailable to meet and confer within a reasonable amount of time or fails to cooperate in scheduling the conference, the Challenging Party may proceed to file its motion with the Court.

6.3 Judicial Intervention. A Party that elects to initiate a challenge to a confidentiality designation after considering the justification offered by the Designating Party may file and serve a motion in compliance with Local Rule 5.1.3, if applicable, that identifies the challenged material and sets forth in detail the basis for the challenge. Each such motion must be accompanied by a competent declaration that affirms that the movant has complied with the meet and confer requirements imposed in the preceding paragraph and that sets forth with specificity the justification for the confidentiality designation that was given by the Designating Party in the meet and confer dialogue. The burden of persuasion in any such challenge proceeding shall be on the Designating Party to establish that the information is, in fact, properly designated . Until

the Court rules on the challenge, all parties shall continue to afford the material in question the level of protection to which it is entitled under the Designating Party's designation.

7. PRESERVATION AND USE OF PROTECTED MATERIAL

7.1 Basic Principles. A Receiving Party may use Protected Material that is disclosed or produced by another Party or by a non-party in connection with this case only for the purposes of this Action and not for any business, patent prosecution, competitive or governmental purpose or function, and shall not be disclosed to anyone except as provided in this Order absent a specific order by the Court. When the Action has been terminated, a Receiving Party must comply with the provisions of Section 12 below (FINAL DISPOSITION).

Except as otherwise provided in Paragraph 8, all "CONFIDENTIAL," "HIGHLY CONFIDENTIAL – ATTORNEYS' EYES ONLY," or "HIGHLY CONFIDENTIAL – SOURCE CODE" material or information shall be maintained under the control of Outside Counsel, who shall make best efforts to prevent any disclosure thereof except in accordance with the terms of this Order.

7.2 Disclosure of "CONFIDENTIAL" Information or Items. Unless otherwise ordered by the Court or permitted in writing by the Designating Party, a Receiving Party may disclose information or items designated "CONFIDENTIAL" only to:

(a) the Receiving Party's Outside Counsel, as well as employees of said Outside Counsel to whom it is reasonably necessary to disclose the information for this Action;

(b) In-house Counsel of the Receiving Party to whom disclosure is reasonably necessary for this Action, who have signed the "Agreement To Be Bound By Protective Order" (Exhibit A);

(c) Outside Consultants (as defined in this Order) (1) to whom disclosure is reasonably necessary for this Action, (2) who have signed the “Agreement to Be Bound by Protective Order” (Exhibit A), and (3) as to whom the procedures set forth in Section 7.6 below, have been followed;

(d) the Court and its personnel;

(e) court reporters, their staffs, and Professional Vendors to whom disclosure is reasonably necessary for this Action;

(f) any designated mediator who is assigned to hear this matter, or who has been selected by the Parties, and his or her staff, who have signed the “Agreement To Be Bound by Protective Order” (Exhibit A);

(g) during their depositions, witnesses in the Action who are current officers or employees of the Producing Party and to whom disclosure is reasonably necessary for this Action;

(h) each person the document or information identifies as an author, source or recipient of such document or information; and

(i) any person that evidence demonstrates to have already viewed the information or document or been told of its content, provided that the party desiring such disclosure first provides five (5) calendar days advanced written notice to the Designating Party of the planned disclosure describing precisely what is to be disclosed, to whom it will be disclosed, and the evidentiary basis for believing the document or information has already been disclosed to such person. Should the Designating Party object to such disclosure within the five (5) calendar days, disclosure shall not be made under this provision.

7.3 Disclosure of “HIGHLY CONFIDENTIAL – ATTORNEYS’ EYES

ONLY” Information or Items. Unless otherwise ordered by the Court or permitted in writing by the Designating Party, a Receiving Party may disclose information or items designated “HIGHLY CONFIDENTIAL — ATTORNEYS’ EYES ONLY” only to:

(a) The Receiving Party’s Outside Counsel, as well as employees of said Outside Counsel to whom it is reasonably necessary to disclose the information for this Action;

(b) Outside Consultants (as defined in this Order) (1) to whom disclosure is reasonably necessary for this Action, (2) who have signed the “Agreement to Be Bound by Protective Order” (Exhibit A), and (3) as to whom the procedures set forth in Section 7.6 below, have been followed;

(c) the Court and its personnel;

(d) court reporters, their staffs, and Professional Vendors to whom disclosure is reasonably necessary for this Action;

(e) any designated mediator who is assigned to hear this matter, or who has been selected by the Parties, and his or her staff, who have signed the “Agreement To Be Bound by Protective Order” (Exhibit A);

(f) each person the document or information identifies as an author, source or recipient of such document or information; and

(g) any person that evidence demonstrates to have already viewed the information or document or been told of its content, provided that the party desiring such disclosure first provides five (5) calendar days advanced written notice to the Designating Party of the planned disclosure describing precisely what is to be disclosed, to whom it will be

disclosed, and the evidentiary basis for believing the document or information has already been disclosed to such person. Should the Designating Party object to such disclosure within the five (5) calendar days, disclosure shall not be made under this provision.

7.4 Disclosure of “HIGHLY CONFIDENTIAL – SOURCE CODE”

Information and Items. Unless otherwise ordered by the Court or permitted in writing by the Designating Party, a Receiving Party may disclose, subject to the provisions of Paragraph 7.5 and 8, information or items designated “HIGHLY CONFIDENTIAL – ATTORNEYS’ EYES ONLY” only to:

(a) Outside Counsel for the Receiving Party, as well as employees of said Outside Counsel to whom it is reasonably necessary to disclose the information for this Action, except that, unless otherwise agreed, no outside counsel who is involved in competitive decision-making, as defined by *U.S. Steel v. United States*, 730 F.2d 1465, 1468 n.3 (Fed. Cir. 1984), shall have access to “HIGHLY CONFIDENTIAL – SOURCE CODE” Information or Items;

(b) Outside Consultants (as defined in this Order) retained by the Receiving Party for purposes of this Action who (a) have signed the “Agreement to Be Bound by Protective Order” (Exhibit A), and (b) as to whom the procedures set forth in Section 7.6 below, have been followed, provided that disclosure is only to the extent necessary to perform that consultant’s work in this Action and such expert or consultant is not involved in competitive decision-making, as defined by *U.S. Steel v. United States*, 730 F.2d 1465, 1468 n.3 (Fed. Cir. 1984), on behalf of a party or a competitor of a party in the technical subject matter of the “HIGHLY CONFIDENTIAL – SOURCE CODE” Information or Items;

(c) the Court and its personnel;



(d) court reporters, stenographers, and videographers retained to record testimony taken in this Action;

(e) any persons who are witnesses during a deposition, court hearing, or trial where specific documentary or testimonial evidence establishes that the “HIGHLY CONFIDENTIAL – SOURCE CODE” Information or Items or portion of the “HIGHLY CONFIDENTIAL – SOURCE CODE” Information or Items was authored or received by the witness;

(f) any mediator who is assigned to hear this matter, and his or her staff, subject to their agreement to maintain confidentiality to the same degree as required by this Order;

(g) any other person with the prior written consent of the Producing Party.

7.5 Limits on Disclosure of “HIGHLY CONFIDENTIAL – ATTORNEYS’ EYES ONLY” and “HIGHLY CONFIDENTIAL – SOURCE CODE” Material, Information or Items.

(a) For avoidance of doubt, Receiving Parties shall not disclose “HIGHLY CONFIDENTIAL – ATTORNEYS’ EYES ONLY” or “HIGHLY CONFIDENTIAL – SOURCE CODE” Material, Information or Items to any of its In-house attorneys or employees. Outside Counsel for the Receiving Party may give advice and opinions to his or her client regarding this litigation based on his or her evaluation of designated “HIGHLY CONFIDENTIAL – ATTORNEYS’ EYES ONLY” or “HIGHLY CONFIDENTIAL – SOURCE CODE” Material, Information or Items – provided that such rendering of advice and opinions

shall not reveal the content of such Protected Material or any information contained therein except by prior written agreement with Outside Counsel for the Producing Party.

(b) Each person to whom Protected Material may be disclosed, and who is required to sign the “Agreement To Be Bound By Protective Order” attached hereto as Exhibit A, shall do so prior to the time such Protected Material is disclosed to him or her.

Outside Counsel for a Party who makes any disclosure of Protected Material shall retain each original executed agreement and, upon written request, shall provide copies to counsel to all other Parties at the termination of this action.

(c) At the request of the Designating Party, persons not permitted access to Protected Material under the terms of this Protective Order shall not be present at depositions while the Designating Party’s Protected Material is discussed or otherwise disclosed. Pre-trial and trial proceedings shall be conducted in a manner, subject to the supervision of the Court, to protect Protected Material from disclosure to persons not authorized to have access to such Material. Any Party intending to disclose or discuss Protected Material at pretrial or trial proceedings must give advance notice to assure the implementation of the terms of this Protective Order.

(d) Any consultant or expert retained on behalf of a Receiving Party who is to be given access to a Producing Party’s “HIGHLY CONFIDENTIAL – SOURCE CODE” Material, Information or Items — whether in electronic form or otherwise — must agree in writing not to use the accessed code to write source code directly intended for commercial purposes relating to wireless communications and user interface technology for a period of six (6) months after the issuance of a final, non-appealable decision resolving all issues in this Action. This shall not preclude such consultants and experts from any academic work or

consulting in future litigation, so long as such consulting does not involve writing source code directly intended for commercial purposes relating to the technology at issue in this Action.

(e) Absent the written consent of the Disclosing Party, any person who receives access to Protected Material shall not be involved in the prosecution of patents or patent applications relating to the subject matter of the patents-in-suit, before any foreign or domestic agency, including the United States Patent and Trademark Office. For purposes of this paragraph, “prosecution” includes, without limitation: (i) the drafting or amending of patent claims, or the supervising of the drafting or amending of patent claims; (ii) participating in or advising on any reexamination or reissue proceeding; and (iii) advising any client concerning strategies for obtaining or preserving patent rights in the above-listed field before the United States Patent and Trademark Office or other similar foreign government or agency.

Notwithstanding the preceding, for purposes of this paragraph, “prosecution” does not include (i) any acts taken to discharge the duty of candor and good faith in any proceeding related to the asserted patents or the technical subject matter of the asserted patents; (ii) participating in or advising on any reexamination or reissue proceeding by Nokia’s lawyers with respect to any patents in which Apple has any interest, or participating in or advising on any reexamination or reissue proceeding (except for participating in or advising on, directly or indirectly, claim drafting or amending claims) by Apple’s lawyers with respect to any patents in which Apple has any interest; (iii) participating in or advising on any reexamination or reissue proceeding by Apple’s lawyers with respect to any patents in which Nokia has any interest, or participating in or advising on any reexamination or reissue proceeding (except for participating in or advising on, directly or indirectly, claim drafting or amending claims) by Nokia’s lawyers with respect to any patents in which Nokia has any interest. This prohibition on patent prosecution shall begin

when an individual obtains access to the Protective Material and shall end two (2) years after the final resolution of this Action, including all appeals. This prosecution bar is personal to the person receiving Protected Material in this Action and shall not be imputed to any other person or entity.

7.6 Procedures for Approving Disclosure of “CONFIDENTIAL,” “HIGHLY CONFIDENTIAL – ATTORNEYS’ EYES ONLY,” and “HIGHLY CONFIDENTIAL – SOURCE CODE” Information or Items to “Outside Consultants”

(a) Unless otherwise ordered by the Court or agreed in writing by the Designating Party, a Receiving Party that seeks to disclose to an Outside Consultant (as defined in this Order) any Protected Material first must notify the Designating Party at least ten (10) business days before the first of such disclosure. The notification must include: (i) the name of the Outside Consultant, (ii) and the name of his or her employer(s) during the last five (5) years, (iii) a current copy of the Outside Consultant’s resume or CV, (iv) if an Outside Consultant for Nokia, whether he or she has done any work for, or been adverse to, Apple, Inc. in the last five (5) years, and if an Outside Consultant for Apple, whether he or she has done any work for, or been adverse to, Nokia, Inc., Nokia, Corp. or Nokia Seimens Network in the last five (5) years, and (v) a list of any clients for whom the Outside Consultant has done any consulting in the area of wireless telecommunications during the last five (5) years. If any Outside Consultant is unable to comply fully with the requirements of this paragraph due to confidentiality restrictions, the Receiving Party must so state in the notification, and the parties must confer in good faith to address any reasonable concerns of the Designating Party.

(b) A Receiving Party that makes a request and provides to the Designating Party the information specified in Section 7.4 (a) above may disclose Protected

Material to the identified Outside Consultant unless, within ten (10) business days of making the notification, the Receiving Party receives a written objection from the Designating Party. Any such objection must be made for good cause and set forth in detail the grounds on which it is based.

(c) A Receiving Party that receives a timely written objection must meet and confer with the Designating Party to try to resolve the matter by agreement. If no agreement is reached within five (5) business days, the Party challenging the disclosure to the Outside Consultant may file a motion in compliance with Local Rule 5.1.3, if applicable, seeking a Protective Order from the Court to prohibit the disclosure to the Outside Consultant. Any such notice must describe the circumstances with specificity, set forth in detail the reasons for the challenge, assess the risk of harm from the use of the Designating Party's Protected Material for purposes other than this Action, and may suggest any additional means that might be used to reduce that risk. In addition, any such motion must be accompanied by a competent declaration in which the movant describes the Parties' efforts to resolve the matter by agreement. The Designating Party shall have the burden of proof by a preponderance of the evidence on the issue of the sufficiency of the objection(s). If the Party challenging the disclosure files a timely motion for Protective Order, Protected Material shall not be disclosed to the challenged individual until and unless a final ruling allowing such disclosure is made by this Court, or by the consent of the Producing Party, whichever occurs first. If the Party challenging the disclosure fails to file a proper motion within five (5) business days of having met and conferred, the Receiving Party may disclose the Protected Material to the Outside Consultant. Disagreement by the Designating Party that the Outside Consultant is competent to render an admissible opinion in this Action is not a valid basis for refusing disclosure. Likewise, the disclosure of designated

material to an Outside Consultant under the terms of this Order may not be used as evidence that the Producing Party acquiesced to the expertise or qualifications of the Outside Consultant.

8. PRODUCTION OF HIGHLY CONFIDENTIAL – SOURCE CODE MATERIALS.

8.1 To the extent that a party wishes to obtain access to HIGHLY CONFIDENTIAL – SOURCE CODE, the following procedures may apply at the option of the Producing Party. Nothing in this Order shall be construed as a representation or admission by a party that HIGHLY CONFIDENTIAL – SOURCE CODE is properly discoverable in this Action, or to obligate any party to produce HIGHLY CONFIDENTIAL – SOURCE CODE.

8.2 The following provisions apply to the production of HIGHLY CONFIDENTIAL – SOURCE CODE unless otherwise agreed by the Producing Party:

(a) All HIGHLY CONFIDENTIAL – SOURCE CODE shall be made available by the Producing Party to the Receiving Party in a secure room, the domestic location and facility of which the Producing Party shall select, on at least two secured, stand-alone computers (running a reasonably current version of the Microsoft Windows operating system) per software platform produced (in the case of Nokia HIGHLY CONFIDENTIAL – SOURCE CODE, for example, produced software platforms may include S60, S40, Qt, and Maemo), without Internet access or network access to other computers, as necessary and appropriate to prevent and protect against any unauthorized copying, transmission, removal, or other transfer of any HIGHLY CONFIDENTIAL – SOURCE CODE outside or away from the computer on which the HIGHLY CONFIDENTIAL – SOURCE CODE is provided for inspection (hereinafter “HIGHLY CONFIDENTIAL – SOURCE CODE Computer”). If it should be necessary, the HIGHLY CONFIDENTIAL – SOURCE CODE Computer may be configured by the Producing

Party to run other mutually agreed upon operating systems. No more than a total of 25 individuals indentified by the receiving party shall have access to the secure room in which the Producing Party produces its HIGHLY CONFIDENTIAL – SOURCE CODE.

(b) The Producing shall install tools that are sufficient for viewing and searching the code produced, on the platform produced, if such tools exist and are presently used in the ordinary course of the Producing Party's business. The Receiving Party's Outside Counsel and/or Outside Consultants may request that commercially available software tools for viewing and searching HIGHLY CONFIDENTIAL – SOURCE CODE be installed on the secured computer, provided, however, that such other software tools are reasonably necessary for the Receiving Party to perform its review of the HIGHLY CONFIDENTIAL – SOURCE CODE consistent with all of the protections herein. Specific tools may include — but are not limited to: Visual Slick Edit, Source-Navigator, PowerGrep, and ExamDiff Pro, or other similar programs. The Receiving Party must provide the Producing Party with the CD or DVD containing such licensed software tool(s) at least five (5) days in advance of the date upon which the receiving party wishes to have the additional software tools available for use on the HIGHLY CONFIDENTIAL – SOURCE CODE Computer. The Receiving Party shall not at any time use any compilers, interpreters or simulators in connection with the Producing Party's HIGHLY CONFIDENTIAL – SOURCE CODE.

(c) The Producing Party shall make the HIGHLY CONFIDENTIAL – SOURCE CODE available electronically and in text searchable form in a secure room at the offices of the Producing Party's Outside Counsel or any other location mutually agreed by the parties.

(d) In order to verify that its HIGHLY CONFIDENTIAL – SOURCE CODE has not later been altered, the Producing Party may benchmark the materials before and after they are provided but shall not install any keystroke or other monitoring software on the HIGHLY CONFIDENTIAL – SOURCE CODE Computer.

(e) The HIGHLY CONFIDENTIAL – SOURCE CODE Computer shall be made available from 9 am to 7 pm local time, Monday through Friday (excluding holidays), and other days and/or times, including weekends, upon reasonable request until the close of discovery in this Action. Access on weekends or after hours shall be permitted only on three days advanced written notice.

(f) Prior to the first inspection of any requested piece of HIGHLY CONFIDENTIAL – SOURCE CODE, the Requesting Party shall provide fourteen (14) days notice of the HIGHLY CONFIDENTIAL – SOURCE CODE that it wishes to inspect. The requesting party shall provide two (2) days notice prior to any additional inspections of the same HIGHLY CONFIDENTIAL – SOURCE CODE, although the parties will be reasonable in accommodating requests of less than two (2) days. The Receiving Party shall identify any individual who will be given access to the HIGHLY CONFIDENTIAL – SOURCE CODE at least ten (10) days prior to the first time any such individual is given access to the HIGHLY CONFIDENTIAL – SOURCE CODE, after which time the Producing Party may object to providing access to any persons so identified. The Receiving Party shall provide two (2) days notice any time each such individual is given access to the HIGHLY CONFIDENTIAL – SOURCE CODE after the first time, although the parties will be reasonable in accommodating notice of less than two (2) days. If an objection to an individual is made by the Producing Party,



it will be the burden of the Producing Party to prove that the individual should not be authorized to inspect the Producing Party's HIGHLY CONFIDENTIAL – SOURCE CODE.

(g) Proper identification of all authorized persons shall be provided prior to any access to the secure room or the HIGHLY CONFIDENTIAL – SOURCE CODE Computer. Proper identification requires showing, at a minimum, a photo identification card sanctioned by the government of any State of the United States, by the government of the United States, or by the nation state of the authorized person's current citizenship. Access to the secure room or the HIGHLY CONFIDENTIAL – SOURCE CODE Computer may be denied, at the discretion of the Producing Party, to any individual who fails to provide proper identification.

(h) The HIGHLY CONFIDENTIAL – SOURCE CODE Computer shall be equipped with a printer (with commercially reasonable printing speeds) to print copies of the HIGHLY CONFIDENTIAL – SOURCE CODE on watermarked pre-Bates numbered paper, which shall be provided by the Producing Party. The Receiving Party may print limited portions of the HIGHLY CONFIDENTIAL – SOURCE CODE only when reasonably necessary to facilitate the Receiving Party's preparation of court filings, expert reports, and trial exhibits, and shall print only such portions as are relevant to the claims and defenses in the case and are reasonably necessary for such purpose. The Receiving Party shall not print HIGHLY CONFIDENTIAL – SOURCE CODE in order to review blocks of HIGHLY CONFIDENTIAL – SOURCE CODE elsewhere in the first instance, i.e., as an alternative to reviewing that HIGHLY CONFIDENTIAL – SOURCE CODE electronically on the HIGHLY CONFIDENTIAL – SOURCE CODE Computer, as the parties acknowledge and agree that the purpose of the protections herein would be frustrated by printing portions of code for review and analysis elsewhere. If the Producing Party objects that the printed portions are excessive and/or not done

for a permitted purpose, the Producing Party shall make such objection known to the receiving party within five (5) days. Printed portions which exceed 50 continuous pages or 10% or more of a specific software release shall be presumed excessive and not done for a permitted purpose. If, after meeting and conferring, the Producing Party and the Receiving Party cannot resolve the objection, the Producing Party shall be entitled to seek the Court's resolution of whether the printed HIGHLY CONFIDENTIAL – SOURCE CODE in question is narrowly tailored and was printed for a permitted purpose. The burden shall be on the Receiving Party to demonstrate that such printed portions are no more than is reasonably necessary for a permitted purpose and not merely printed for the purposes of review and analysis elsewhere. No more than a total of 30 individuals indentified by the receiving party shall have access to the printed portions of HIGHLY CONFIDENTIAL – SOURCE CODE (except insofar as such code appears in any filing with the Court or expert report in this Action).

(i) The printed HIGHLY CONFIDENTIAL – SOURCE CODE shall be labeled with “[PRODUCING PARTY’S NAME] HIGHLY CONFIDENTIAL – SOURCE CODE – SUBJECT TO PROTECTIVE ORDER.” Outside Counsel for the Producing Party will keep the originals of these printed documents, and copies shall be made for Outside Counsel for the Receiving Party on watermarked paper within 48 hours. The Receiving Party’s Outside Counsel may make no more than ten (10) additional paper copies of any portions of the HIGHLY CONFIDENTIAL – SOURCE CODE received from a Producing Party, not including copies attached to court filings or used at depositions.

(j) In addition to other reasonable steps to maintain the security and confidentiality of the Producing Party’s HIGHLY CONFIDENTIAL – SOURCE CODE, printed copies of the HIGHLY CONFIDENTIAL – SOURCE CODE maintained by the Receiving Party

must be kept in a locked storage container when not in use. No electronic copies of the HIGHLY CONFIDENTIAL – SOURCE CODE shall be provided by the Producing Party beyond the HIGHLY CONFIDENTIAL – SOURCE CODE Computer.

(k) Except as provided herein, absent express written permission from the Producing Party, the Receiving Party may not create electronic images, or any other images, or make electronic copies, of the HIGHLY CONFIDENTIAL – SOURCE CODE from any paper copy of HIGHLY CONFIDENTIAL – SOURCE CODE for use in any manner (including, by way of example only, the Receiving Party may not scan the HIGHLY CONFIDENTIAL – SOURCE CODE to a PDF or photograph the code). Images or copies of HIGHLY CONFIDENTIAL – SOURCE CODE shall not be included in correspondence between the parties (references to production numbers shall be used instead), and shall be omitted from pleadings and other papers whenever possible. If a party reasonably believes that it needs to submit a portion of HIGHLY CONFIDENTIAL – SOURCE CODE as part of a filing with the Court, the Parties shall meet and confer as to how to make such a filing while protecting the confidentiality of the HIGHLY CONFIDENTIAL – SOURCE CODE and such filing will not be made absent agreement from the Producing Party that the confidentiality protections will be adequate. If a Producing Party agrees to produce an electronic copy of all or any portion of its HIGHLY CONFIDENTIAL – SOURCE CODE or provide written permission to the receiving party that an electronic or any other copy needs to be made for a Court filing, the Receiving Party's communication and/or disclosure of electronic files or other materials containing any portion of HIGHLY CONFIDENTIAL – SOURCE CODE (paper or electronic) shall at all times be limited to solely individuals who are expressly authorized to view HIGHLY CONFIDENTIAL – SOURCE CODE under the provisions of this Order, and all such individuals

must be identified on the log as reviewers and/or recipients of paper copies in accordance with paragraph 8.2(p). In the case where the Producing Party has provided the express written permission required under this provision for a receiving party to create electronic copies of HIGHLY CONFIDENTIAL – SOURCE CODE, the electronic copies shall be included on the log required by paragraph 8.2(p) and any other information required by paragraph 8.2(p) shall be included on the log. Additionally, any such electronic copies must be labeled “[PRODUCING PARTY’S NAME] HIGHLY CONFIDENTIAL – SOURCE CODE – SUBJECT TO PROTECTIVE ORDER” as provided for in this Order.

(l) For depositions, the Receiving Party shall not bring copies of any printed HIGHLY CONFIDENTIAL – SOURCE CODE. Rather, at least five (5) days before the date of the deposition, the Receiving Party shall notify the Producing Party about the specific portions of HIGHLY CONFIDENTIAL – SOURCE CODE it wishes to use at the deposition, and the Producing Party shall bring printed copies of those portions to the deposition for use by the receiving party. Copies of HIGHLY CONFIDENTIAL – SOURCE CODE that are marked as deposition exhibits shall not be provided to the court reporter or attached to deposition transcripts; rather, the deposition record will identify the exhibit by its production numbers. All paper copies of HIGHLY CONFIDENTIAL – SOURCE CODE brought to the deposition shall be securely destroyed in a timely manner following the deposition.

(m) Other than the HIGHLY CONFIDENTIAL – SOURCE CODE Computer and printer provided by the Producing Party, no electronic devices, including but not limited to laptops, floppy drives, zip drives, or other hardware shall be permitted in the secure room. Nor shall any cellular telephones, personal digital assistants, Blackberries, cameras, voice recorders, Dictaphones, telephone jacks, or other devices be permitted inside the secure room. No non-

electronic devices capable of similar functionality shall be permitted in the secure room. The Receiving Party shall be entitled to take notes relating to the HIGHLY CONFIDENTIAL – SOURCE CODE but may not copy the HIGHLY CONFIDENTIAL – SOURCE CODE into the notes and may not take such notes electronically on the HIGHLY CONFIDENTIAL – SOURCE CODE Computer itself or any other computer. No copies of all or any portion of the HIGHLY CONFIDENTIAL – SOURCE CODE may leave the room in which the HIGHLY CONFIDENTIAL – SOURCE CODE is inspected except as otherwise provided herein. Further, no other written or electronic record of the HIGHLY CONFIDENTIAL – SOURCE CODE is permitted except as otherwise provided herein. The Producing Party may visually monitor the activities of the Receiving Party’s representatives during any HIGHLY CONFIDENTIAL – SOURCE CODE review, but only to ensure that no unauthorized electronic records of the HIGHLY CONFIDENTIAL – SOURCE CODE and that no information concerning the HIGHLY CONFIDENTIAL – SOURCE CODE are being created or transmitted in any way.

(n) Other than as provided 8.1(i), the Receiving Party will not copy, remove, or otherwise transfer any HIGHLY CONFIDENTIAL – SOURCE CODE from the HIGHLY CONFIDENTIAL – SOURCE CODE Computer including, without limitation, copying, removing, or transferring the HIGHLY CONFIDENTIAL – SOURCE CODE onto any recordable media or recordable device, including without limitation sound recorders, computers, cellular telephones, peripheral equipment, cameras, CDs, DVDs, or drives of any kind. The Receiving Party will not transmit any HIGHLY CONFIDENTIAL – SOURCE CODE in any way from the Producing Party’s facilities or the offices of its outside counsel.

(o) Unless otherwise agreed in advance by the parties in writing, following each day on which inspection is done under this Order, the Receiving Party’s Outside Counsel

and/or Outside Consultants shall remove all notes, documents, and all other materials from the secure room. The Producing Party shall not be responsible for any items left in the room following each inspection session, and the receiving party shall have no expectation of confidentiality for any items left in the room following each inspection session without a prior agreement to that effect.

(p) The Receiving Party shall maintain a HIGHLY CONFIDENTIAL – SOURCE CODE Access Log identifying each hard copy (or electronic copy as permitted by paragraph 8.2(k)) of HIGHLY CONFIDENTIAL – SOURCE CODE that it has in its possession and, for each and every time the hard copy (or electronic copy as permitted by paragraph 8.2(k)) of the HIGHLY CONFIDENTIAL – SOURCE CODE is viewed: (i) the name of each person who viewed the HIGHLY CONFIDENTIAL – SOURCE CODE; (ii) the date and time of access; (iii) the length of time of access; and (iv) whether any, and if so what, portion of the HIGHLY CONFIDENTIAL – SOURCE CODE was copied. The Producing Party shall be entitled to a copy of the log upon one (1) day's advance notice to the receiving party. Within thirty (30) days after the issuance of a final, non-appealable decision resolving all issues in the Action, the Receiving Party must serve upon the Producing Party the HIGHLY CONFIDENTIAL – SOURCE CODE Access Log. All persons to whom the paper copies of the HIGHLY CONFIDENTIAL – SOURCE CODE were provided must certify in writing that all copies of the HIGHLY CONFIDENTIAL – SOURCE CODE were returned to Outside Counsel for the Producing Party and that they will make no use of the HIGHLY CONFIDENTIAL – SOURCE CODE or of any knowledge gained from the HIGHLY CONFIDENTIAL – SOURCE CODE in any future endeavor.

8.3. Access to and review of the HIGHLY CONFIDENTIAL – SOURCE CODE shall be strictly for the purpose of investigating the claims and defenses at issue in this Action. No person shall review or analyze any HIGHLY CONFIDENTIAL – SOURCE CODE for purposes unrelated to this Action, nor may any person use any knowledge gained as a result of reviewing HIGHLY CONFIDENTIAL – SOURCE CODE in this Action in any other pending or future dispute, proceeding, patent prosecution, or litigation.

8.4. Nothing herein shall be deemed a waiver of a party's right to object to the production of HIGHLY CONFIDENTIAL – SOURCE CODE. Absent a subsequent and specific court or agency order, nothing herein shall obligate a party to breach any non-party license agreement relating to such HIGHLY CONFIDENTIAL – SOURCE CODE.

8.5. The parties further acknowledge that some or all of the HIGHLY CONFIDENTIAL – SOURCE CODE may be owned by non-parties and outside a party's possession, custody or control. Nothing herein shall be deemed a waiver of any non-party's right to object to the production of HIGHLY CONFIDENTIAL – SOURCE CODE or object to the manner of any such production.

9. PROTECTED MATERIAL SUBPOENAED OR ORDERED PRODUCED IN OTHER LITIGATION

9.1 If a Receiving Party is served with a subpoena or an order issued in other litigation that would compel disclosure of any information or items designated in this action as "CONFIDENTIAL," "HIGHLY CONFIDENTIAL – ATTORNEYS' EYES ONLY," or "HIGHLY CONFIDENTIAL – SOURCE CODE," the Receiving Party must so notify the Designating Party, in writing, promptly and in no event more than ten (10) business days after

receiving the subpoena or order. Such notification must include a copy of the subpoena or court order.

9.2 The Receiving Party also must immediately inform in writing the party who caused the subpoena or order to issue in the other litigation that some or all the material covered by the subpoena or order is the subject of this Order. In addition, the Receiving Party must deliver a copy of this Order promptly to the party in the other action that caused the subpoena or order to issue.

9.3 The purpose of imposing these duties is to alert the interested parties to the existence of this Order and to afford the Designating Party in this case an opportunity to try to protect its confidentiality interests in the court from which the subpoena or order issued. The Designating Party shall bear the burdens and the expenses of seeking protection in that court of its confidential material, and nothing in these provisions should be construed as authorizing or encouraging a Receiving Party in this action to disobey a lawful directive from another court.

10. UNAUTHORIZED DISCLOSURE OF PROTECTED MATERIAL

If a Receiving Party learns that, by inadvertence or otherwise, it has disclosed Protected Material to any person or in any circumstance not authorized under this Order, the Receiving Party must immediately (a) notify in writing the Designating Party of the unauthorized disclosures, (b) use its best efforts to retrieve all copies of the Protected Material, (c) inform the person or persons to whom unauthorized disclosures were made of all the terms of this Order, and (d) request that such person or persons execute the “Acknowledgment and Agreement to Be Bound By Protective Order” that is attached hereto as Exhibit A.



11. FILING PROTECTED MATERIAL

Without written permission from the Designating Party or a court order secured after appropriate notice to all interested persons, a Party may not publicly file in this Action any Protected Material. With regard to filing Protected Material under seal in accordance with Local Rule 5.1.3, the parties submit and the Court finds that there will be documents filed in this case that include confidential, proprietary and commercially sensitive information that can only be protected by sealing the documents and those portions of the memoranda that discuss the documents. The Court finds that this information is of a private business nature and is not of great public interest.

In the event that any “CONFIDENTIAL,” “HIGHLY CONFIDENTIAL – ATTORNEYS’ EYES ONLY,” or “HIGHLY CONFIDENTIAL – SOURCE CODE” information is included with, or the contents thereof are in any way disclosed in any pleading, motion, deposition, transcript or other paper filed with the Clerk of this Court, such information shall be filed with the Clerk of the Court, without need of a motion, in sealed envelopes or containers marked with the caption of the case, a general description of the contents of the envelope or container and a legend substantially in the following form:

“UNDER SEAL – SUBJECT TO PROTECTIVE ORDER –  
CONTAINS CONFIDENTIAL OR HIGHLY CONFIDENTIAL  
MATERIAL – TO BE OPENED ONLY BY OR AS DIRECTED  
BY THE COURT.”

Notwithstanding the foregoing, however, “CONFIDENTIAL,” “HIGHLY CONFIDENTIAL – ATTORNEYS’ EYES ONLY,” or “HIGHLY CONFIDENTIAL – SOURCE CODE” documents or testimony introduced into evidence at trial shall not be sealed or otherwise treated as confidential by the Court except pursuant to a further order of the Court at the request of either party during pretrial proceedings or at trial.

12. DISCOVERY FROM OUTSIDE CONSULTANTS

(a). The Parties agree that they will not seek drafts of expert reports, declarations, affidavits, or notes taken by experts retained to testify in this Investigation, whether those reports, declarations, affidavits, or notes relate to this Action, to any prior investigation, litigation or proceeding which was disclosed to the parties under paragraph 7.6 of the Protective Order, or to any currently pending investigation, litigation or proceeding involving any of the Parties to this Action.<sup>1</sup> The Parties further agree that they will not seek documents relating to communications between such experts and counsel, including e-mail communications, whether generated in connection with this Action, a prior litigation, or any currently pending investigation, litigation or proceeding involving any of the Parties to this Action, except for documents, information and things included in or attached to such communications that are directly relied upon by the expert in his or her expert report, declaration, affidavit, or testimony.

(b). The Parties agree not to inquire at deposition or trial as to the contents of drafts of expert reports, declarations or affidavits, nor notes pertaining thereto, whether drafted in connection with this Action, a prior litigation, or any currently pending investigation, litigation or proceeding involving two or more of the Parties to this Action, and that the Parties will not inquire at deposition or at trial as to the expert's communications, written or oral, with counsel, whether generated in connection with this Action, a prior litigation, or any currently pending investigation, litigation or proceeding involving two or more of the Parties to this Action, except

---

<sup>1</sup> For purposes of this Paragraph, "any currently pending investigation, litigation or proceeding involving two or more of the Parties in this Action" includes: *In the Matter of Certain Electronic Devices, Including Mobile Phones, Portable Music Players, and Computers*, 337-TA-701; *In the Matter of Certain Mobile Communications and Computer Devices and Components Thereof*, 337-TA-704; *Nokia v. Apple*, Case No. 10-cv-00249 (W.D. Wis.) *Nokia v. Apple*, Case No. 09-cv-791 (D. Del.); and *Nokia v. Apple*, Case No. 09-cv-1002 (D. Del.).

to the extent that the expert explicitly references or cites information from counsel in his or her expert report, declaration, affidavit, or testimony.

(c). The Parties will, however, identify and produce copies of any documents referenced or cited by the expert in his or her expert report. Furthermore, nothing in this Paragraph is intended to restrict the Parties' ability to (i) inquire into the basis of any of the opinions expressed by any experts in his or her report, declaration, or affidavit, including the manner by which such opinions were reached, and information considered in reaching such opinions; (ii) otherwise inquire into the process by which an expert report, affidavit or declaration was drafted, provided that, in so doing, the Parties may not discover the contents of any such drafts of expert reports, declarations or affidavits, nor notes pertaining thereto; or (iii) obtain reports, testimony, or other discovery or evidence produced in any prior litigation or any currently pending investigation, litigation or proceeding involving two or more of the Parties to this Investigation.

13. COMMUNICATIONS BETWEEN PARTY AND COUNSEL

The parties agree that privileged or protected communications occurring on or after October 22, 2009 need not be recorded on the Party's privilege log in this case.

14. FINAL DISPOSITION

Unless otherwise ordered or agreed in writing by the Producing Party, within 90 calendar days after the final termination of this Action, each Receiving Party must return all Protected Material to the Producing Party. As used in this subdivision, "all Protected Material" includes all copies, abstracts, compilations, summaries or any other form of reproducing or capturing any of the Protected Material. In lieu of returning to the Producing Party, counsel for a Receiving Party may destroy any Protected Material that is intertwined with attorney work product or

privileged communications. With permission in writing from the Designating Party, the Receiving Party may destroy some or all of the remaining Protected Material instead of returning it. Whether the Protected Material is returned or destroyed, the Receiving Party must submit a written certification to the Producing Party (and, if not the same person or entity, to the Designating Party) by the 90 calendar day deadline that verifies all the Protected Material was returned or destroyed and that affirms that the Receiving Party has not retained any copies, abstracts, compilations, summaries or other forms of reproducing or capturing any of the Protected Material. Notwithstanding this provision, Counsel are entitled to retain an archival copy of all pleadings, expert reports, motion papers, deposition and hearing transcripts, legal memoranda, correspondence and attorney work product, even if such materials contain Protected Material. Any such archival copies that contain or constitute Protected Material remain subject to this Order as set forth in Section 4 (DURATION) above.

15. MISCELLANEOUS

15.1 Right to Further Relief. Nothing in this Order abridges the right of any person to seek its modification by the Court in the future. The Parties may by stipulation provide for exceptions to this Order, provided that such stipulation is presented to the Court as a Consent Order, and any Party may seek an order of this Court modifying or interpreting this Order.

15.2 Right to Assert Other Objections. By stipulating to the entry of this Order, no Party waives any right it otherwise would have to object to disclosing or producing any information or item on any ground not addressed in this Order or from asserting that certain discovery materials should receive greater confidentiality protection than that provided herein, in accordance with Rule 26(c) of the Federal Rules of Civil Procedure. Similarly, no Party waives any right to object on any ground to use in evidence of any of the material covered by this Order.

15.3 Waiver of Notice. Any of the notice requirements herein may be waived, in whole or in part, but only by a writing signed by Counsel for the Party against whom such waiver will be effective.

15.4 Enforcement. The United States District Court for the District of Delaware is responsible for the interpretation and enforcement of this Order. All disputes concerning Protected Material produced under the protection of this Order shall be resolved by this Court. In the event anyone shall violate or threaten to violate the terms of this Order, subject to meet and confer obligations in the Court's Local Rules, the aggrieved party may apply to obtain injunctive relief against any such person, and in such event, the respondent, subject to the terms of this Order, shall not employ as a defense thereto the claim that the aggrieved party possesses an adequate remedy at law. The parties and any other person subject to the terms of this Order agree that they will subject themselves to the jurisdiction of this Court for the purpose of any proceedings related to performance under, compliance with, or violation of this Order.

15.5 No Waiver. Nothing in this Order, or the taking of any action in accordance with the provisions of this Order, or the failure to object thereto, shall be construed as a waiver or admission of any claim or defense in the Action. The failure to object to a designation shall not constitute an admission by the Receiving Party that the designated information is in fact trade secret or proprietary information. This Order shall not in any way limit what a party may do or disclose with its own documents or information. Nothing in this Order shall be deemed to preclude a party from seeking and obtaining, on an appropriate showing, different or additional protections or relief regarding matter designated as containing "CONFIDENTIAL," "HIGHLY CONFIDENTIAL – ATTORNEYS' EYES ONLY," or "HIGHLY CONFIDENTIAL – SOURCE CODE" information.

MORRIS, NICHOLS, ARSHT & TUNNELL LLP

POTTER, ANDERSON & CORROON LLP

*/s/ Jack B. Blumenfeld*

*/s/ David E. Moore*

---

Jack B. Blumenfeld (#1014)  
Rodger D. Smith II (#3778)  
1201 North Market Street  
P.O. Box 1347  
Wilmington, DE 19899  
(302) 658-9200  
[jblumenfeld@mnat.com](mailto:jblumenfeld@mnat.com)  
[rsmith@mnat.com](mailto:rsmith@mnat.com)

---

Richard L. Horwitz (#2246)  
David E. Moore (#3983)  
Hercules Plaza, 6th Floor  
1313 N. Market Street  
Wilmington, DE 19899  
(302) 984-6000  
[rhorwitz@potteranderson.com](mailto:rhorwitz@potteranderson.com)  
[dmoore@potteranderson.com](mailto:dmoore@potteranderson.com)

*Attorneys for Nokia Corporation and Nokia  
Inc.*

*Attorneys for Apple Inc.*

Dated: June 1, 2010

SO ORDERED this \_\_\_\_ day of \_\_\_\_\_ 2010.

---

United States District Court Judge

# **Exhibit 1**

**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

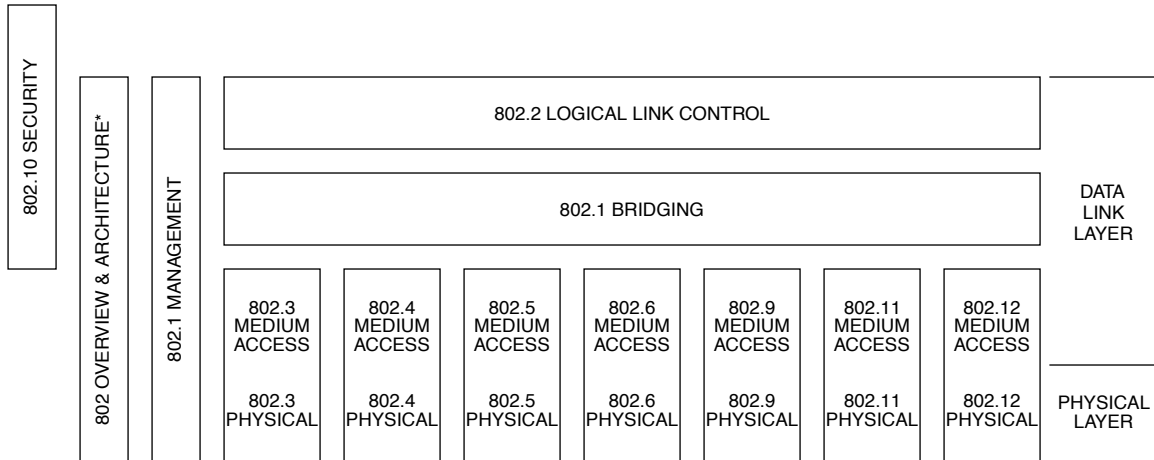
Note: Attention is called to the possibility that implementation of this standard may require use of subject matter covered by patent rights. By publication of this standard, no position is taken with respect to the existence or validity of any patent rights in connection therewith. The IEEE shall not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

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	Richard J. Iliff	Thomas L. Phinney
Jon M. Allingham	Tomoaki Ishifuji	Vikram Prabhu
Jack S. Andresen	Carlos Islas-Perez	Alberto Profumo
Kit Athul	Raj Jain	David L. Propp
Anthony L. Barnes	A. Kamerman	Vikram Punj
Robert T. Bell	Peter M. Kelly	Andris Putnins
Manuel J. Betancor	Yongbum Kim	Fernando Ramos
Simon Black	Mikio Kiyono	James W. Romlein
Alan L. Bridges	Thaddeus Kobylarz	Floyd E. Ross
Graham Campbell	Stephen B. Kruger	Michael Rothenberg
James T. Carlo	Joseph J. Kubler	Christoph Ruland
David E. Carlson	David J. Law	Chandos A. Rypinski
Peter E. Chadwick	Jai Yong Lee	Anil K. Sanwalka
Naftali Chayat	Jungtae Lee	Gregory D. Schumacher
Alan J. Chwick	Daniel E. Lewis	Rich Seifert
Ken Clements	Randolph S. Little	Lee A. Sendelbach
Robert S. Crowder	Ming T. Liu	Michael Serrone
Rifaat Dayem	Joseph C. J. Loo	Adarshpal S. Sethi
Wim Diepstraten	Donald C. Loughry	Donald A. Sheppard
Edward A. Dunlop	Robert D. Love	Nathan Silberman
Sourav K. Dutta	Ronald Mahany	Joseph S. Skorupa
Paul S. Eastman	Jim L. Mangin	Michael A. Smith
Peter Ecclesine	Peter Martini	Marvin L. Sojka
Gregory Elkmann	P. Takis Mathiopoulos	Efstathios D. Sykas
John E. Emrich	Steve Messenger	Geoffrey O. Thompson
Philip H. Enslow	Bennett Meyer	Robert C. Tripi
Changxin Fan	Ann Miller	Mike Trompower
Michael A. Fischer	David S. Millman	David B. Turner
Harvey A. Freeman	Hiroshi Miyano	Mark-Rene Uchida
Robert J. Gagliano	Stig Frode Mjolsnes	James Vorhies
Patrick S. Gonia	W. Melody Moh	Yun-Che Wang
N. Douglas Grant	John E. Montague	Raymond P. Wenig
Govert M. Griffioen	Wayne D. Moyers	Earl J. Whitaker
Joseph L. Hammond	Paul Nikolich	David W. Wilson
Victor Hayes	Ellis S. Nolley	Jerry A. Wyatt
Kenneth C. Heck	Robert O'Hara	Qian-Li Yang
Jan Hoogendoorn	Donal O'Mahony	Iwen Yao
Russell D. Housley	Roger Pandanda	Oren Yuen
Walter K. Hurwitz	Lalit Mohan Patnaik	Jonathan M. Zweig
	Lucy W. Person	

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 Rüsçh  
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



23.3.5	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).<sup>1</sup>

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.<sup>2</sup>

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.

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

<sup>2</sup>ISO publications are available from the ISO Central Secretariat, Case Postale 56, 1 rue de Varembé, 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.<sup>3</sup>

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

---

<sup>3</sup>ITU 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  $\mu$ 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.

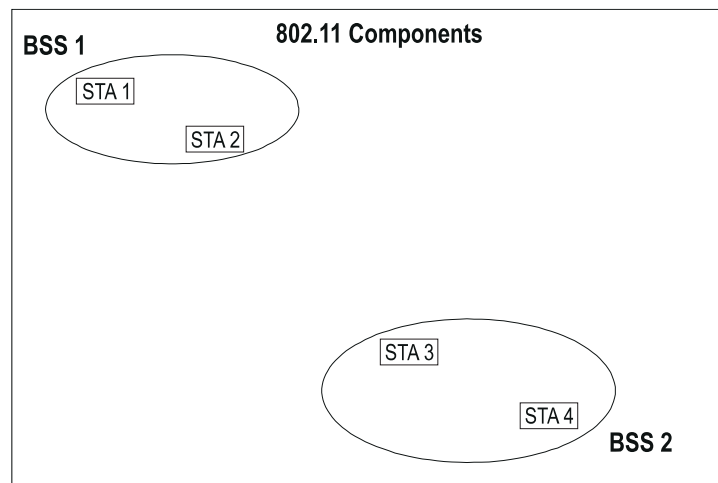


Figure 1—Basic service sets

#### 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).

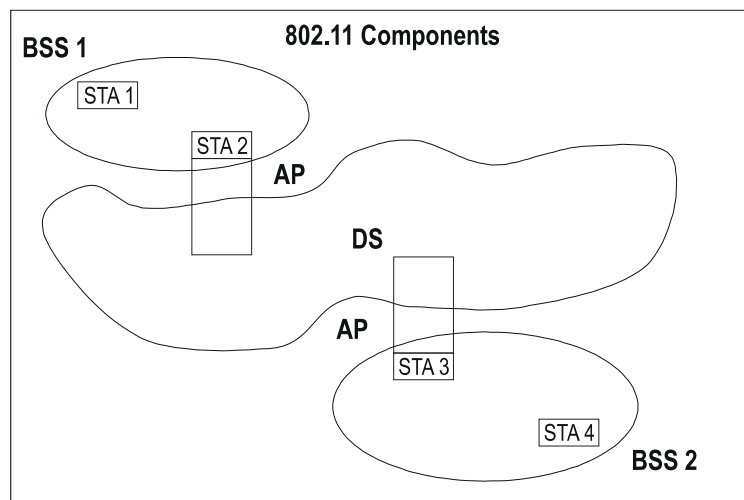
IEEE 802.11 logically separates the wireless medium (WM) from the distribution system medium (DSM). Each logical medium is used for different purposes, by a different component of the architecture. The IEEE 802.11 definitions neither preclude, nor demand, that the multiple media be either the same or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

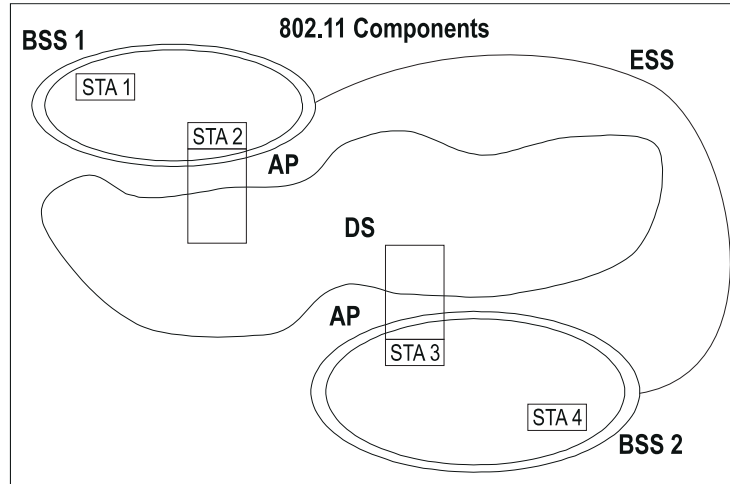


Figure 3—Extended service set

All of the following are possible:

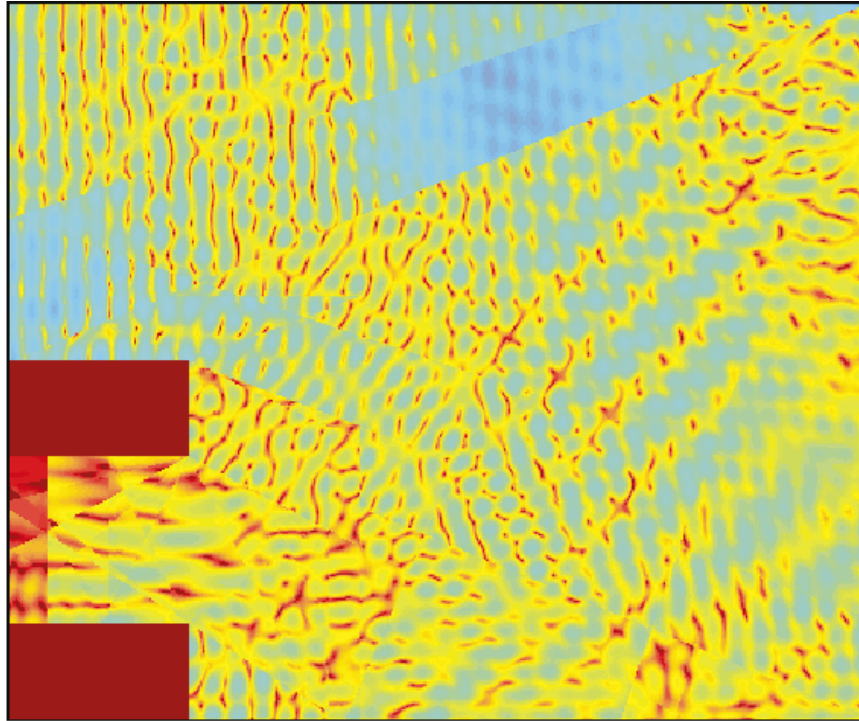
- The BSSs may partially overlap. This is commonly used to arrange contiguous coverage within a physical volume.
- The BSSs could be physically disjointed. Logically there is no limit to the distance between BSSs.
- The BSSs may be physically collocated. This may be done to provide redundancy.
- One (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).

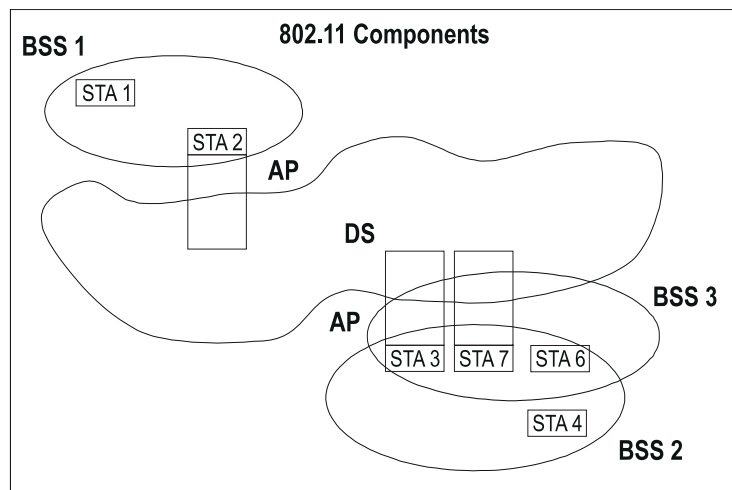
Figure 4 shows a signal strength map for a simple square room with a standard metal desk and an open doorway. Figure 4 is a static snapshot; the propagation patterns change dynamically as stations and objects in the environment move. In Figure 4 the dark (solid) blocks in the lower left are a metal desk 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.

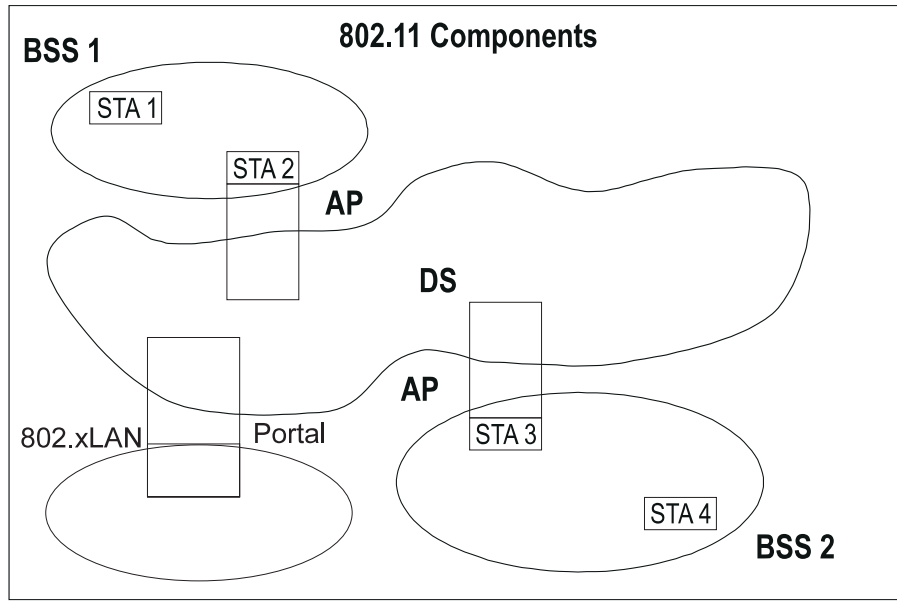


Figure 6—Connecting to other IEEE 802 LANs

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.

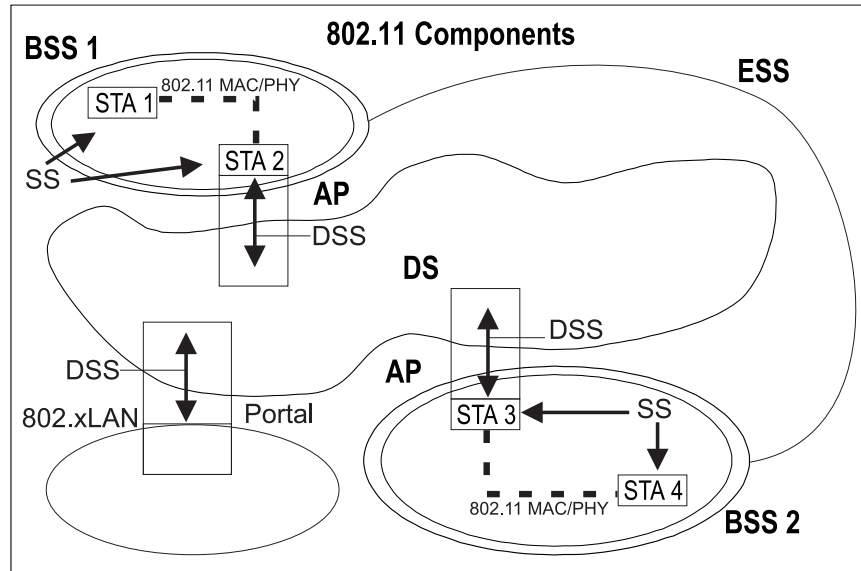


Figure 7—Complete IEEE 802.11 architecture

### 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]<sup>4</sup> 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.

---

<sup>4</sup>The 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:

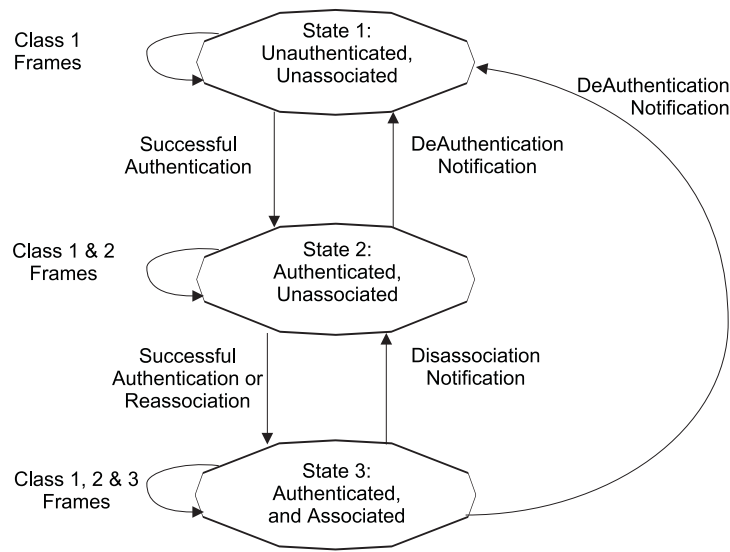
- *Authentication state*: The values are unauthenticated and authenticated.
- *Association state*: The values are unassociated and associated.

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.

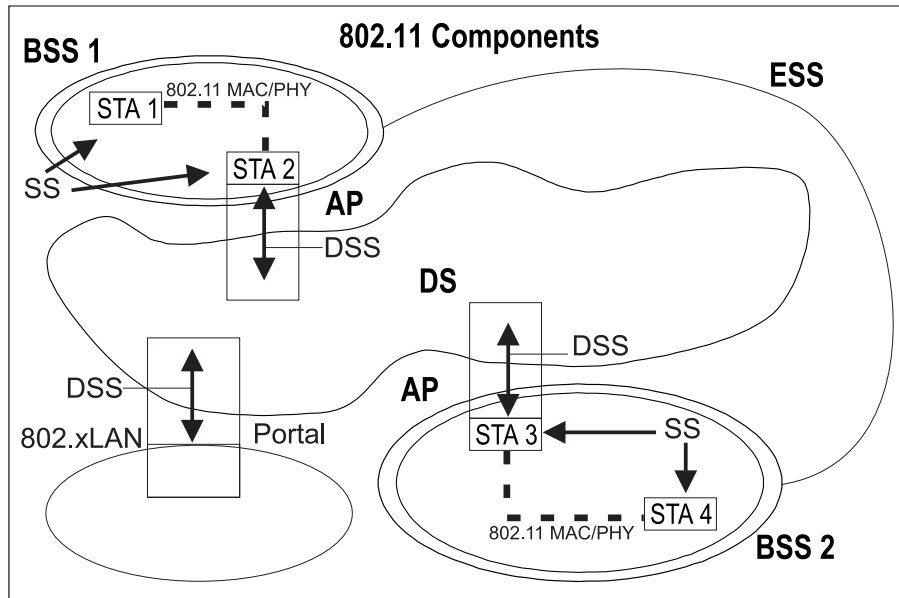


Figure 9—IEEE 802.11 architecture (again)

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.

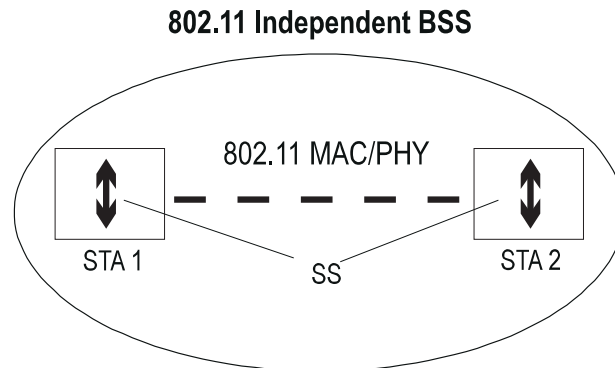


Figure 10—Logical architecture of an IBSS

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:

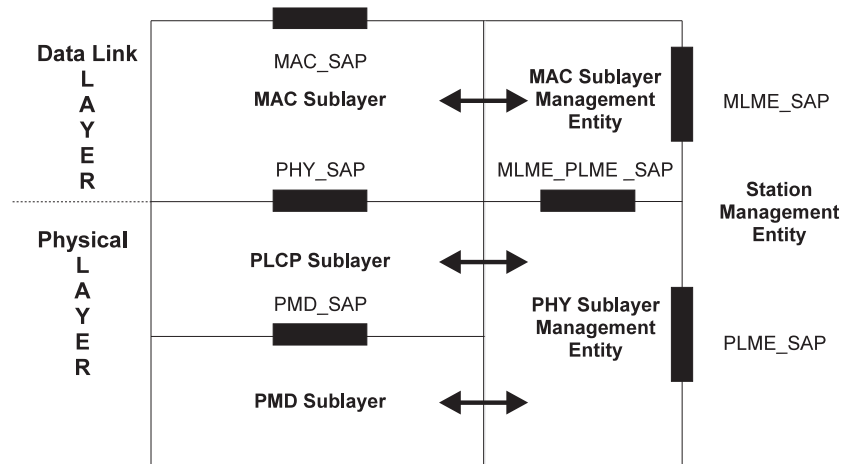
*Deauthentication*

- 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 7498-1:1994<sup>5</sup>). 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**

<sup>5</sup>Information 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.



In order for the MAC to operate properly, the DS must meet the requirements of ISO/IEC 15802-1: 1995.

Subclause 9.8 specifies operational restrictions that ensure the appropriate ordering of MSDUs.

## 6.2 Detailed service specification

### 6.2.1 MAC data services

The IEEE 802.11 MAC supports the following service primitives as defined in ISO/IEC 8802-2: 1994:

- MA-UNITDATA.request
- MA-UNITDATA.indication
- MA-UNITDATA-STATUS.indication

The following three subclauses (6.2.1.1 through 6.2.1.3) give the LLC definitions of the primitives and specify parameter value restrictions imposed by IEEE 802.11.

#### 6.2.1.1 MA-UNITDATA.request

##### 6.2.1.1.1 Function

This primitive requests a transfer of an MSDU from a local LLC sublayer entity to a single peer LLC sublayer entity, or multiple peer LLC sublayer entities in the case of group addresses.

##### 6.2.1.1.2 Semantics of the service primitive

The parameters of the primitive are as follows:

```
MA-UNITDATA.request    (
                        source address,
                        destination address,
                        routing information,
                        data,
                        priority,
                        service class
                        )
```

The source address (SA) parameter specifies an individual MAC sublayer address of the sublayer entity to which the MSDU is being transferred.

The destination address (DA) parameter specifies either an individual or a group MAC sublayer entity address.

The routing information parameter specifies the route desired for the data transfer (a null value indicates source routing is not to be used). For IEEE 802.11, the routing information parameter must be null.

The data parameter specifies the MSDU to be transmitted by the MAC sublayer entity. For IEEE 802.11, the length of the MSDU must be less than or equal to 2304 octets.

The priority parameter specifies the priority desired for the data unit transfer. IEEE 802.11 allows two values: Contention or ContentionFree.

The service class parameter specifies the service class desired for the data unit transfer. IEEE 802.11 allows two values: ReorderableMulticast or StrictlyOrdered.

#### **6.2.1.1.3 When generated**

This primitive is generated by the LLC sublayer entity whenever an MSDU is to be transferred to a peer LLC sublayer entity or entities.

#### **6.2.1.1.4 Effect of receipt**

The receipt of this primitive causes the MAC sublayer entity to append all MAC specified fields, including DA, SA, and all fields that are unique to IEEE 802.11, and pass the properly formatted frame to the lower layers for transfer to peer MAC sublayer entity or entities.

### **6.2.1.2 MA-UNITDATA.indication**

#### **6.2.1.2.1 Function**

This primitive defines the transfer of an MSDU from the MAC sublayer entity to the LLC sublayer entity, or entities in the case of group addresses. In the absence of error, the contents of the data parameter are logically complete and unchanged relative to the data parameter in the associated MA-UNITDATA.request primitive.

#### **6.2.1.2.2 Semantics of the service primitive**

The primitive provides parameters as follows:

```
MA-UNITDATA.indication (
    source address,
    destination address,
    routing information,
    data,
    reception status,
    priority,
    service class
)
```

The SA parameter is an individual address as specified by the SA field of the incoming frame.

The DA parameter is either an individual or a group address as specified by the DA field of the incoming frame.

The routing information parameter specifies the route that was used for the data transfer. IEEE 802.11 will always set this field to null.

The data parameter specifies the MSDU as received by the local MAC entity.

The reception status parameter indicates the success or failure of the received frame for those frames that IEEE 802.11 reports via a MA-UNITDATA.indication. This MAC only reports "success" as all failures of reception are discarded without generating MA-UNITDATA.indication.

The priority parameter specifies the receive processing priority that was used for the data unit transfer. IEEE 802.11 allows two values: Contention or ContentionFree.

The service class parameter specifies the receive service class that was used for the data unit transfer. IEEE 802.11 allows two values: ReorderableMulticast or StrictlyOrdered.

### 6.2.1.2.3 When generated

The MA-UNITDATA.indication primitive is passed from the MAC sublayer entity to the LLC sublayer entity or entities to indicate the arrival of a frame at the local MAC sublayer entity. Frames are reported only if they are validly formatted at the MAC sublayer, received without error, received with valid (or null) WEP encryption, and their destination address designates the local MAC sublayer entity.

### 6.2.1.2.4 Effect of receipt

The effect of receipt of this primitive by the LLC sublayer is dependent on the validity and content of the frame.

## 6.2.1.3 MA-UNITDATA-STATUS.indication

### 6.2.1.3.1 Function

This primitive has local significance and provides the LLC sublayer with status information for the corresponding preceding MA-UNITDATA.request primitive.

### 6.2.1.3.2 Semantics of the service primitive

The primitive parameters are as follows:

```
MA-UNITDATA-STATUS.indication (
    source address,
    destination address,
    transmission status,
    provided priority,
    provided service class
)
```

The SA parameter is an individual MAC sublayer entity address as specified in the associated MA-UNITDATA.request primitive.

The DA parameter is either an individual or group MAC sublayer entity address as specified in the associated MA-UNITDATA.request primitive.

The transmission status parameter will be used to pass status information back to the local requesting LLC sublayer entity. IEEE 802.11 specifies the following values for transmission status:

- a) Successful,
- b) Undeliverable (for unacknowledged directed MSDUs when the aShortRetryMax or aLongRetryMax retry limit would otherwise be exceeded),
- c) Excessive data length,
- d) Non-null source routing,
- e) Unsupported priority (for priorities other than Contention or ContentionFree),
- f) Unsupported service class (for service classes other than ReorderableMulticast or StrictlyOrdered),
- g) Unavailable priority (for ContentionFree when no point coordinator is available, in which case the MSDU is transmitted with a provided priority of Contention), and
- h) Unavailable service class (for StrictlyOrdered service when the station's power management mode is other than "active").

- i) Undeliverable (TransmitMSDUTimer reached aMaxTransmitMSDULifetime before successful delivery).
- j) Undeliverable (no BSS available).
- k) Undeliverable (the key referenced by aWEPDefaultKeyID or a specific key mapping is null).

The provided priority parameter specifies the priority that was used for the associated data unit transfer (Contention or ContentionFree).

The provided service class parameter specifies the class of service used for the associated data unit transfer (ReorderableMulticast or StrictlyOrdered).

#### **6.2.1.3.3 When generated**

The MA-UNITDATA-STATUS.indication primitive is passed from the MAC sublayer entity to the LLC sublayer entity to indicate the status of the service provided for the corresponding MA-UNITDATA.request primitive.

#### **6.2.1.3.4 Effect of receipt**

The effect of receipt of this primitive by the LLC sublayer is dependent upon the type of operation employed by the LLC sublayer entity.



### 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.

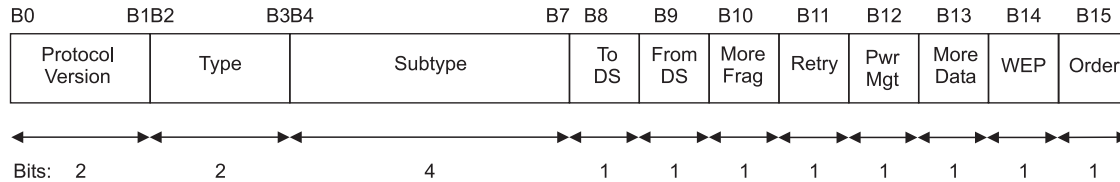


Figure 13—Frame Control field

##### 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 IEEE Std 802.11. 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 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.

Table 1—Valid type/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

**Table 1 – Valid type/subtype combinations (continued)**

Type value b3 b2	Type description	Subtype value b7 b6 b5 b4	Subtype description
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

#### 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 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 MAC management PDUs (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 the this field is 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 BSS 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 two types:

- a) *Individual address*. The address associated with a particular station on the network.
- b) *Group address*. A multideestination address, associated with one or more stations on a given network. There are two kinds of group addresses:
  - 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 1's 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 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 an unique BSSID.

The value of all 1's 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 Destination Address (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 Source Address (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 receiver address (RA) field contains an IEEE MAC individual or group address that identifies the intended immediate recipient STA(s), on the wireless medium (WM), for the information contained in the frame body field.

### 7.1.3.3.7 Transmitter Address (TA) field

The transmitter address (TA) field contains an IEEE MAC individual address that identifies the STA that 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.

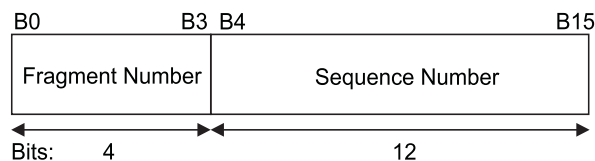


Figure 14—Sequence Control field

#### 7.1.3.4.1 Sequence Number field

The Sequence Number 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 (zero) and incrementing by 1 (one) 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 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 and contains information specific to individual frame types and subtypes. The minimum frame body is zero 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 one'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 ones and is then modified by division of the calculation fields by the generator polynomial  $G(x)$ . The one's complement of this remainder is transmitted, with the high-order bit first, as the FCS field.

At the receiver, the initial remainder is preset to all ones 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.

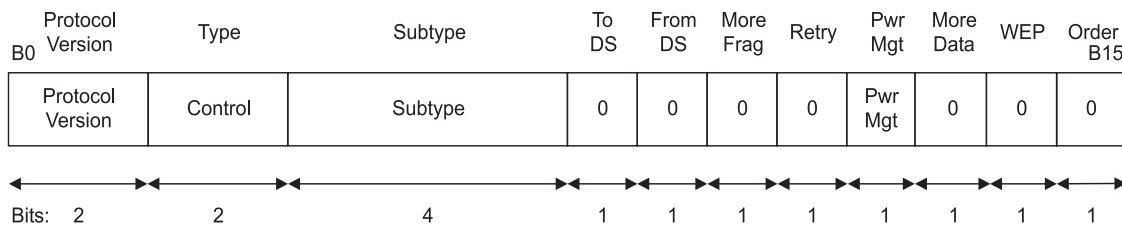


Figure 15—Frame Control field subfield values within control frames

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

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

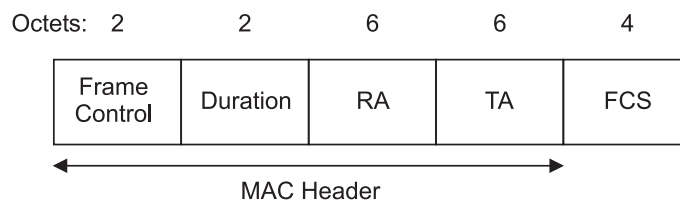


Figure 16—RTS frame

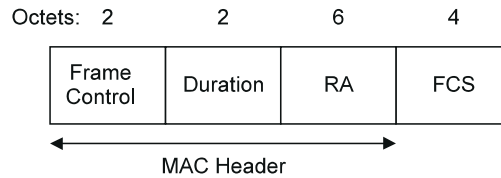
The RA of the RTS frame is the address of the STA, on the WM, that is the intended immediate recipient of the pending directed data or management frame.

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.



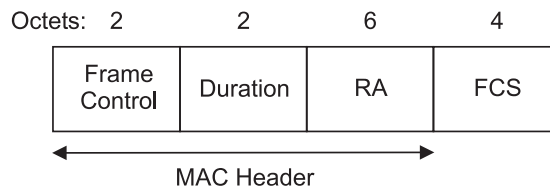
**Figure 17—CTS frame**

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.



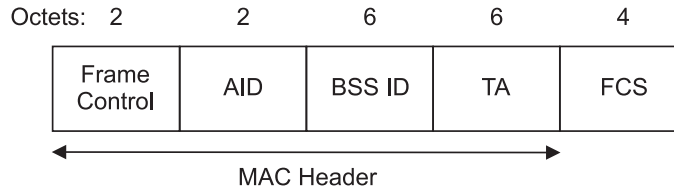
**Figure 18—ACK frame**

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.

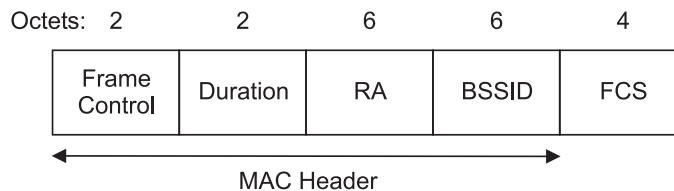
**Figure 19—PS-Poll frame**

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.

The AID value always has its 2 msb both 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.

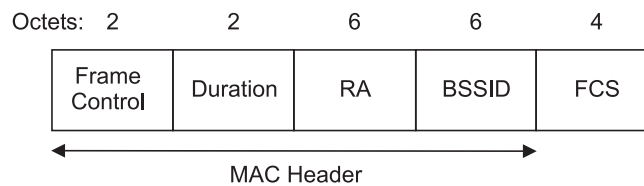
**Figure 20—CF-End frame**

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.

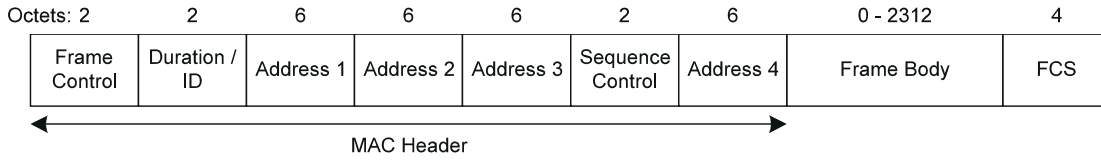
**Figure 21—CF-End + CF-Ack Frame**

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 N/A, the field is omitted. Note that Address 1 always holds the receiver address of the intended receiver (or, in the case of multicast 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 (zero 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).

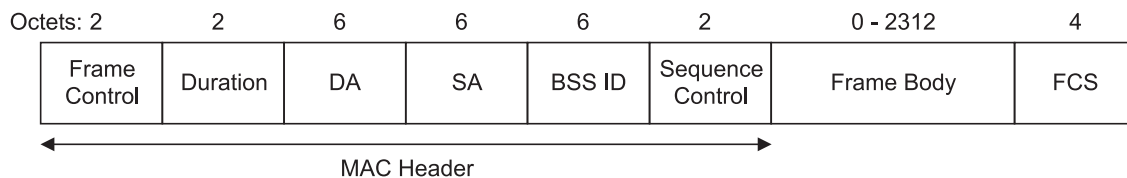
Within all data type frames sent during the CFP, the Duration field is set to the value 32 768. Within all data type frames sent during the contention period, the Duration field is set according to the following rules:

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

NOTES

1—The FH Parameter Set information element is only present within Probe Response frames generated by STAs using frequency-hopping PHYs.

2—The DS Parameter Set information element is only present within Probe Response frames generated by STAs using direct sequence PHYs.

3—The CF Parameter Set information element is only present within Probe Response frames generated by APs supporting a PCF.

4—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	Note
1	Authentication algorithm number	
2	Authentication transaction sequence number	
3	Status code	1
4	Challenge text	2

NOTES

1—The status code information is reserved and set to 0 in certain Authentication frames as defined in Table 14.

2—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 number	Authentication trans. sequence number	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	Note
1	Reason code	

## 7.3 Management frame body components

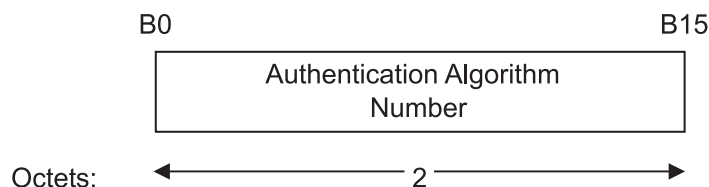
Within management frames, fixed-length mandatory frame body components are defined as fixed fields; variable length mandatory and all optional frame body components are defined as information elements.

### 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 two octets. The Authentication Algorithm Number field is illustrated in Figure 24. The following values are defined for authentication algorithm number:

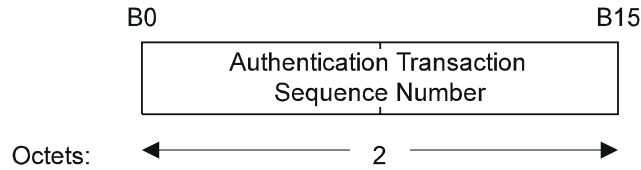
- Authentication algorithm number = 0: Open System
- Authentication algorithm number = 1: Shared Key
- All other values of authentication number are reserved.



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

### 7.3.1.2 Authentication Transaction Sequence Number field

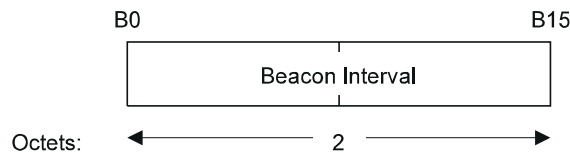
The Authentication Transaction Sequence Number field indicates the current state of progress through a multistep transaction. The length of the Authentication Transaction Sequence Number field is two octets. The Authentication Transaction Sequence Number field is illustrated in Figure 25.



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

### 7.3.1.3 Beacon Interval field

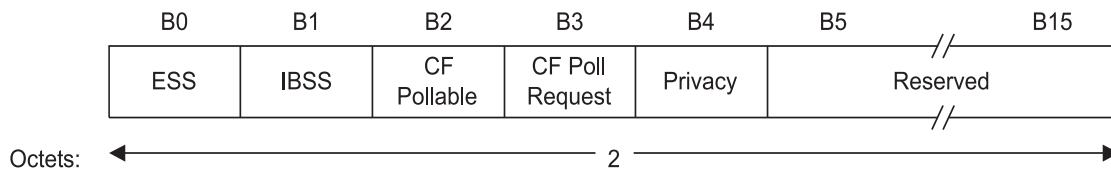
The Beacon Interval field represents the number of time units (TU) between target beacon transmission times (TBTTs). The length of the Beacon Interval field is two octets. The Beacon Interval field is illustrated in Figure 26.



**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 two 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**

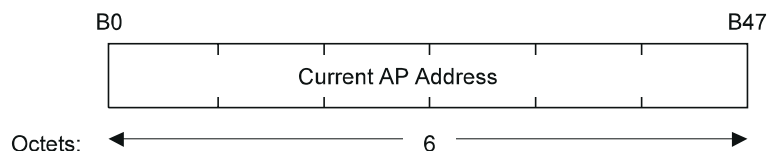
CF-Pollable	CF-Poll Request	Meaning
0	0	No point coordinator at AP
0	1	Point coordinator at AP for delivery only (no polling)
1	0	Point coordinator at AP for delivery and polling
1	1	Reserved

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

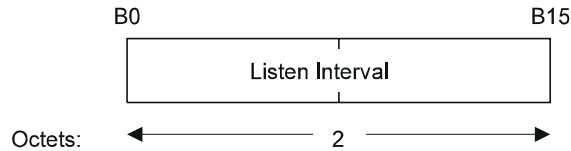
The Current AP Address field is the MAC address of the AP with which the station is currently associated. The length of the Current AP Address field is six octets. The Current AP Address field is illustrated in Figure 28.



**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 `aListenInterval` MIB attribute and is expressed in units of Beacon Interval. The length of the Listen Interval field is two octets. The Listen Interval field is illustrated in Figure 29.

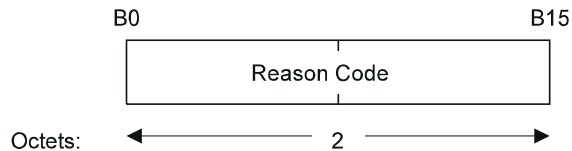


**Figure 29—Listen Interval fixed field**

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 two octets. The Reason Code field is illustrated in Figure 30.



**Figure 30—Reason Code fixed field**

The reason codes are defined in Table 18.

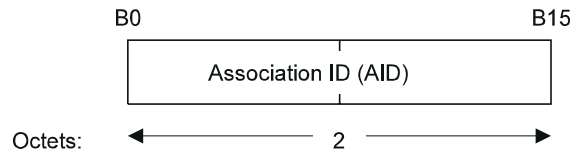
**Table 18—Reason codes**

Reason code	Meaning
0	Reserved
1	Unspecified reason
2	Previous authentication no longer valid
3	Deauthenticated because sending station is leaving (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 nonassociation station
8	Disassociated because sending station is leaving (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 and represents the 16-bit ID of a STA. The length of the AID field is two octets. The AID field is illustrated in Figure 31.



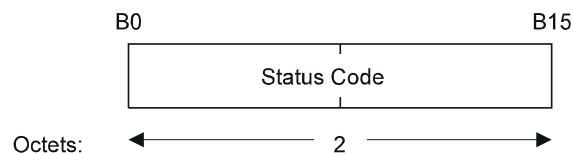
**Figure 31—AID fixed field**

The value assigned as the Association ID is in the range 1–2007 and is placed in the 14 lsb of the AID field, with the 2 msb of the AID field both set to 1 (see 7.1.3.2).

The AID value 0 is used to announce broadcast and multicast frames in traffic indication map information elements.

### 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 two 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**

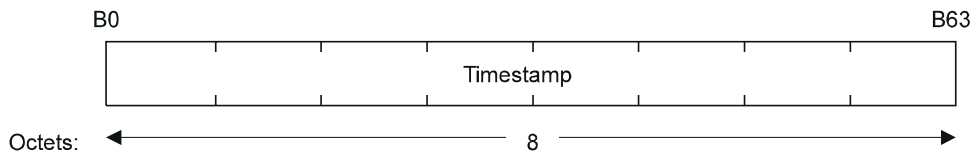
Status code	Meaning
0	Successful
1	Unspecified failure
2–9	Reserved
10	Cannot support all requested capabilities in the Capability Information field
11	Reassociation denied due to inability to confirm that association exists
12	Association denied due to reason outside the scope of this standard
13	Responding 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

**Table 19—Status codes (continued)**

Status code	Meaning
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**

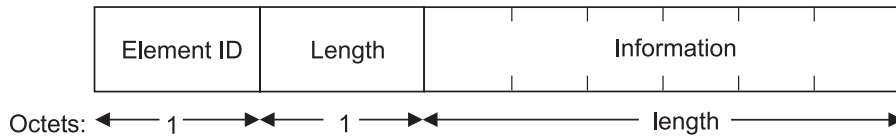
This field represents the value of the TSFTIMER (see 11.1) of a frame’s source. The length of the Timestamp field is eight octets. The Timestamp field is illustrated in Figure 33.



**Figure 33—Timestamp fixed field**

**7.3.2 Information elements**

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



**Figure 34—Element format**

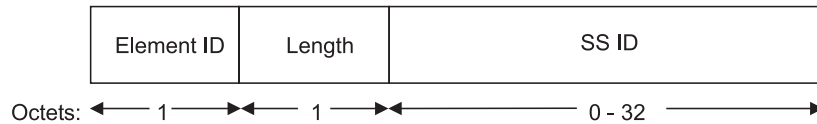
The set of valid elements is defined in Table 20.

**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 Service Set Identity (SSID) element indicates the identity of an extended service set (ESS) or IBSS. See Figure 35.



**Figure 35—SSID element format**

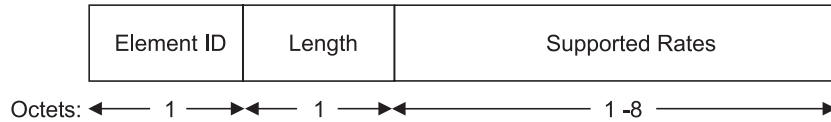
The length of the SSID information field is between 0 and 32 octets. A zero length information field indicates the broadcast SSID.

### 7.3.2.2 Supported Rates element

The Supported Rates element specifies all the rates that this STA is capable of receiving. 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 BSSBasicRate Set is encoded as X'04'). The msb of each Supported Rate octet in other management frame types is ignored by receiving STAs.

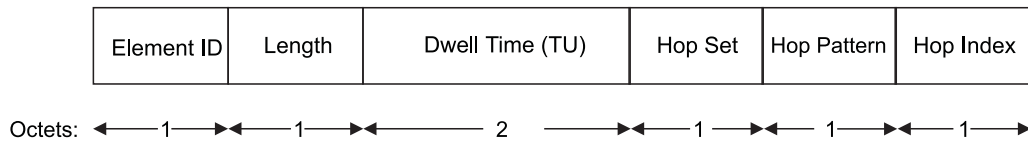
BSSBasicRateSet information in Beacon and Probe Response management frames is used by STAs in order to avoid associating with a BSS if they do not support all the data rates in the BSSBasicRateSet. See Figure 36.



**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 two octets in length and contains the dwell time in TU.

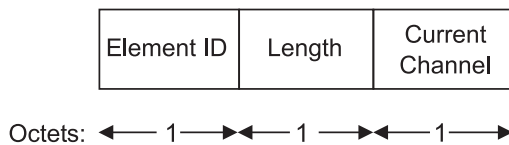
The Hop Set field identifies the particular set of hop patterns and is a single octet.

The Hop Pattern field identifies the individual pattern within a set of hop patterns and is a single octet.

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

**7.3.2.4 DS Parameter Set element**

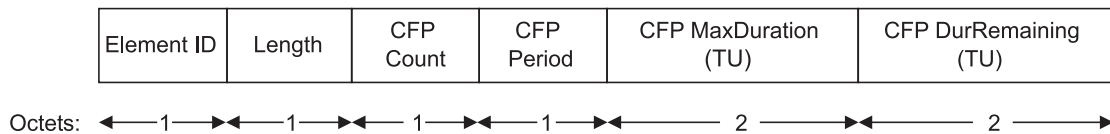
The DS Parameter Set element contains information to allow channel number identification for STAs using a direct sequence spread spectrum (DSSS) PHY. The information field contains a single parameter containing the current channel number. The length of the current channel number parameter is one octet.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



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

**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.



**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.

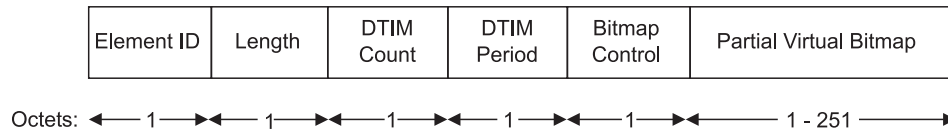
CFPeriod indicates the number of DTIM intervals between the start of CFPs. The value is an integral number of DTIM intervals.

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.



**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. The low-order bit 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 high-order 7 bit forms the Bitmap Offset subfield. The Bitmap Offset subfield is a number between 0 and 250, formed by using the Bitmap Control field with the low-order bit set to 0, and is further described below.

The traffic-indication virtual bitmap, maintained by the AP that generates a TIM, consists of 2008 b, 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  $\lceil N / 8 \rceil$  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).

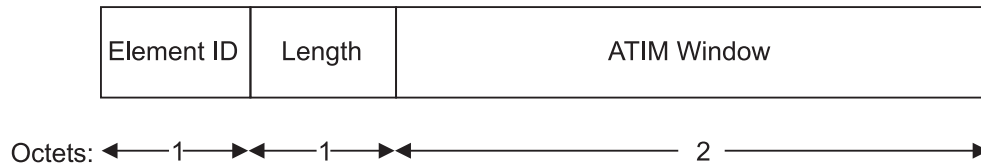
The Partial Virtual Bitmap field consists of octets numbered  $N1$  through  $N2$  of the traffic indication virtual bitmap, where  $N1$  is the largest number such that bits numbered 1 through  $(N1 \times 8) - 1$  in the bitmap are all

0 and  $N_2$  is the smallest number such that bits numbered  $(N_2 + 1) \times 8$  through 2007 in the bitmap are all 0. In this case, the Bitmap Offset subfield value contains the number  $N_1$ , and the Length field will be set to  $(N_2 - N_1) + 4$ .

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.

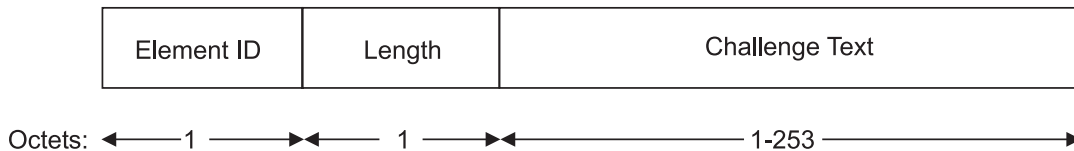


**Figure 41—IBSS Parameter Set element format**

The ATIM Window field is 2 octets in length and contain 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**

## 8. Authentication and privacy

### 8.1 Authentication services

IEEE 802.11 defines two subtypes of authentication service: *Open System* and *Shared Key*. The subtype invoked is indicated in the body of authentication management frames. Thus authentication frames are self-identifying with respect to authentication algorithm. All management frames of subtype Authentication shall be unicast frames as authentication is done between pairs of stations (i.e., multicast authentication is not allowed). Management frames of subtype Deauthentication are advisory, and may therefore be sent as group-addressed frames.

A mutual authentication relationship shall exist between two stations following a successful authentication exchange as described below. Authentication shall be used between stations and the AP in an infrastructure BSS. Authentication may be used between two STAs in an IBSS.

#### 8.1.1 Open System authentication

Open System authentication is the simplest of the available authentication algorithms. Essentially it is a null authentication algorithm. Any STA that requests authentication with this algorithm may become authenticated if aAuthenticationType at the recipient station is set to Open System authentication. Open System authentication is not required to be successful as a STA may decline to authenticate with any particular other STA. Open System authentication is the default authentication algorithm.

Open System authentication involves a two-step authentication transaction sequence. The first step in the sequence is the identity assertion and request for authentication. The second frame in the sequence is the authentication result. If the result is “successful,” the STAs shall be mutually authenticated.

##### 8.1.1.1 Open System authentication (first frame)

- Message type: Management
- Message subtype: Authentication
- Information items:
  - Authentication Algorithm Identification = “Open System”
  - Station Identity Assertion (in SA field of header)
  - Authentication transaction sequence number = 1
  - Authentication algorithm dependent information (none)
- Direction of message: From authentication initiating STA

##### 8.1.1.2 Open System authentication (final frame)

- Message type: Management
- Message subtype: Authentication
- Information items:
  - Authentication Algorithm Identification = “Open System”
  - Authentication transaction sequence number = 2
  - Authentication algorithm dependent information (none)
  - The result of the requested authentication as defined in 7.3.1.9.
- Direction of message: From authenticating STA to initiating STA

If aAuthenticationType does not include the value “Open System,” the result code shall not take the value “successful.”

### 8.1.2 Shared Key authentication

Shared Key authentication supports authentication of STAs as either a member of those who know a shared secret key or a member of those who do not. IEEE 802.11 Shared Key authentication accomplishes this without the need to transmit the secret key in the clear; requiring the use of the WEP privacy mechanism. Therefore, this authentication scheme is only available if the WEP option is implemented. Additionally, the Shared Key authentication algorithm shall be implemented as one of `aAuthenticationAlgorithms` at any STA where WEP is implemented.

The required secret, shared key is presumed to have been delivered to participating STAs via a secure channel that is independent of IEEE 802.11. This shared key is contained in a write-only MIB attribute via the MAC management path. The attribute is write-only so that the key value remains internal to the MAC.

During the Shared Key authentication exchange, both the challenge and the encrypted challenge are transmitted. This facilitates unauthorized discovery of the PRN (pseudorandom number) sequence for the key/IV pair used for the exchange. Implementations should therefore avoid using the same key/IV pair for subsequent frames.

A STA shall not initiate a Shared Key authentication exchange unless its `aPrivacyOptionImplemented` attribute is “true.”

In the following description, the STA initiating the authentication exchange is referred to as the requester, and the STA to which the initial frame in the exchange is addressed is referred to as the responder.

#### 8.1.2.1 Shared Key authentication (first frame)

- Message type: Management
- Message subtype: Authentication
- Information Items:
  - Station Identity Assertion (in SA field of header)
  - Authentication Algorithm Identification = “Shared Key”
  - Authentication transaction sequence number = 1
  - Authentication algorithm dependent information (none)
- Direction of message: From requester to responder

#### 8.1.2.2 Shared Key authentication (second frame)

Before sending the second frame in the Shared Key authentication sequence, the responder shall use WEP to generate a string of octets that shall be used as the authentication challenge text.

- Message type: Management
- Message subtype: Authentication
- Information Items:
  - Authentication Algorithm Identification = “Shared Key”
  - Authentication transaction sequence number = 2
  - Authentication algorithm dependent information = the authentication result.  
The result of the requested authentication as defined in 7.3.1.9.

If the status code is not “successful,” this shall be the last frame of the transaction sequence. If the status code is not “successful,” the content of the challenge text field is unspecified.

If the status code is “successful,” the following additional information items shall have valid contents:

Authentication algorithm dependent information = challenge text.



This field shall be of fixed length of 128 octets. The field shall be filled with octets generated by the WEP PRNG. The actual value of the challenge field is unimportant, but the value shall not be a single static value. The key and initialization vector (IV) used when generating the challenge text are unspecified because this key/IV value does not have to be shared and does not affect interoperability.

- Direction of message: From responder to requester

### 8.1.2.3 Shared Key authentication (third frame)

The requester shall copy the challenge text from the second frame into the third frame. The third frame shall be transmitted after encryption by WEP, as defined in 8.2.3 using the shared secret key.

- Message type: Management
- Message subtype: Authentication
- Information Items:
  - Authentication Algorithm Identification = “Shared Key”
  - Authentication transaction sequence number = 3
  - Authentication algorithm dependent information = challenge text from sequence two frame.
- Direction of message: From requester to responder

This frame shall be encrypted as described below.

### 8.1.2.4 Shared Key authentication (final frame)

The responder shall attempt to decrypt the contents of the third frame in the authentication sequence as described below. If the WEP ICV check is successful, the responder shall then compare the decrypted contents of the Challenge Text field to the challenge text that was sent in frame 2 of the sequence. If they are the same, then the responder shall respond with a successful status code in frame 4 of the sequence. If the WEP ICV check fails, the responder shall respond with an unsuccessful status code in frame 4 of the sequence as described below.

- Message type: Management
- Message subtype: Authentication
- Information Items:
  - Authentication Algorithm Identification = “Shared Key”
  - Authentication transaction sequence number = 4
  - Authentication algorithm dependent information = the authentication result.
    - The result of the requested authentication.
    - This is a fixed length item with values “successful” and “unsuccessful.”
- Direction of message: From responder to requester

## 8.2 The Wired Equivalent Privacy (WEP) algorithm

### 8.2.1 Introduction

Eavesdropping is a familiar problem to users of other types of wireless technology. IEEE 802.11 specifies a wired LAN equivalent data confidentiality algorithm. *Wired equivalent privacy* is defined as protecting authorized users of a wireless LAN from casual eavesdropping. This service is intended to provide functionality for the wireless LAN equivalent to that provided by the physical security attributes inherent to a wired medium.

Data confidentiality depends on an external key management service to distribute data enciphering/deciphering keys. The IEEE 802.11 standards committee specifically recommends against running an IEEE 802.11

LAN with privacy but without authentication. While this combination is possible, it leaves the system open to significant security threats.

### 8.2.2 Properties of the WEP algorithm

The WEP algorithm has the following properties:

- *It is reasonably strong:* The security afforded by the algorithm relies on the difficulty of discovering the secret key through a brute-force attack. This in turn is related to the length of the secret key and the frequency of changing keys. WEP allows for the changing of the key ( $k$ ) and frequent changing of the IV.
- *It is self-synchronizing:* WEP is self-synchronizing for each message. This property is critical for a data-link level encryption algorithm, where “best effort” delivery is assumed and packet loss rates may be high.
- *It is efficient:* The WEP algorithm is efficient and may be implemented in either hardware or software.
- *It may be exportable:* Every effort has been made to design the WEP system operation so as to maximize the chances of approval, by the U.S. Department of Commerce, of export from the U.S. of products containing a WEP implementation. However, due to the legal and political climate toward cryptography at the time of publication, no guarantee can be made that any specific IEEE 802.11 implementations that use WEP will be exportable from the United States of America.
- *It is optional:* The implementation and use of WEP is an IEEE 802.11 option.

### 8.2.3 WEP theory of operation

The process of disguising (binary) data in order to hide its information content is called *encryption* (see [B4]). Data that is not enciphered is called *plaintext* (denoted by  $P$ ) and data that is enciphered is called *ciphertext* (denoted by  $C$ ). The process of turning ciphertext back into plaintext is called *decryption*. A *cryptographic algorithm*, or cipher, is a mathematical function used for enciphering or deciphering data. Modern cryptographic algorithms use a key sequence (denoted by  $k$ ) to modify their output. The encryption function  $E$  operates on  $P$  to produce  $C$ :

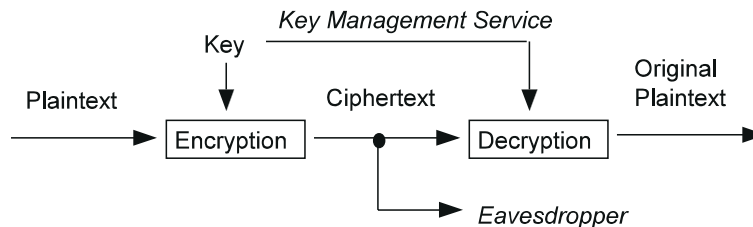
$$E_k(P) = C$$

In the reverse process, the decryption function  $D$  operates on  $C$  to produce  $P$ :

$$D_k(C) = P$$

As illustrated in Figure 43, note that if the same key can be used for encryption and decryption then

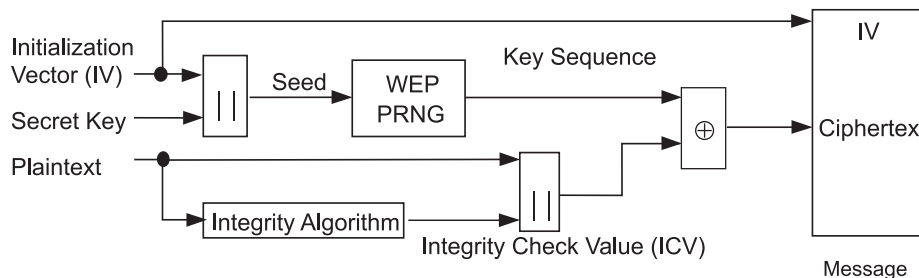
$$D_k(E_k(P)) = P$$



**Figure 43—A confidential data channel**

The WEP algorithm is a form of electronic code book in which a block of plaintext is bitwise XORed with a pseudorandom key sequence of equal length. The key sequence is generated by the WEP algorithm.

Referring to Figure 44 and viewing from left to right, encipherment begins with a *secret key* that has been distributed to cooperating STAs by an external key management service. WEP is a symmetric algorithm in which the same key is used for encipherment and decipherment.



**Figure 44—WEP encipherment block diagram**

The secret key is concatenated with an *initialization vector* (IV) and the resulting *seed* is input to a *pseudo-random number generator* (PRNG). The PRNG outputs a *key sequence*  $k$  of pseudorandom octets equal in length to the number of data octets that are to be transmitted in the expanded MPDU plus 4 [since the key sequence is used to protect the *integrity check value* (ICV) as well as the data]. Two processes are applied to the plaintext MPDU. To protect against unauthorized data modification, an integrity algorithm operates on  $P$  to produce an ICV. Encipherment is then accomplished by mathematically combining the key sequence with the plaintext concatenated with the ICV. The output of the process is a *message* containing the IV and ciphertext.

The WEP PRNG is the critical component of this process, since it transforms a relatively short secret key into an arbitrarily long key sequence. This greatly simplifies the task of key distribution, as only the secret key needs to be communicated between STAs. The IV extends the useful lifetime of the secret key and provides the self-synchronous property of the algorithm. The secret key remains constant while the IV changes periodically. Each new IV results in a new seed and key sequence, thus there is a one-to-one correspondence between the IV and  $k$ . The IV may be changed as frequently as every MPDU and, since it travels with the message, the receiver will always be able to decipher any message. The IV is transmitted in the clear since it does not provide an attacker with any information about the secret key, and since its value must be known by the recipient in order to perform the decryption.

When choosing how often to change IV values, implementors should consider that the contents of some fields in higher-layer protocol headers, as well as certain other higher-layer information, is constant or highly predictable. When such information is transmitted while encrypting with a particular key and IV, an eavesdropper can readily determine portions of the key sequence generated by that (key, IV) pair. If the same (key, IV) pair is used for successive MPDUs, this effect may substantially reduce the degree of privacy conferred by the WEP algorithm, allowing an eavesdropper to recover a subset of the user data without any knowledge of the secret key. Changing the IV after each MPDU is a simple method of preserving the effectiveness of WEP in this situation.

The WEP algorithm is applied to the frame body of an MPDU. The {IV, frame body, ICV} triplet forms the actual data to be sent in the data frame.

For WEP protected frames, the first four octets of the frame body contain the IV field for the MPDU. This field is defined in 8.2.5. The 64-bit PRNG seed is formed using the secret key as the most significant 40 bits and the initialization vector (IV) as the least significant 24 bits. The IV is followed by the MPDU, which is followed by the ICV. The WEP ICV is 32 bits. The WEP Integrity Check algorithm is CRC-32, as defined in 7.1.3.6.

As stated previously, WEP combines  $k$  with  $P$  using bitwise XOR.

Referring to Figure 45 and viewing from left to right, decipherment begins with the arrival of a message. The IV of the incoming message shall be used to generate the key sequence necessary to decipher the incoming message. Combining the ciphertext with the proper key sequence yields the original plaintext and ICV. Correct decipherment shall be verified by performing the integrity check algorithm on the recovered plaintext and comparing the output ICV' to the ICV transmitted with the message. If ICV' is not equal to ICV, the received MPDU is in error and an error indication is sent to MAC management. MSDUs with erroneous MPDUs (due to inability to decrypt) shall not be passed to LLC.

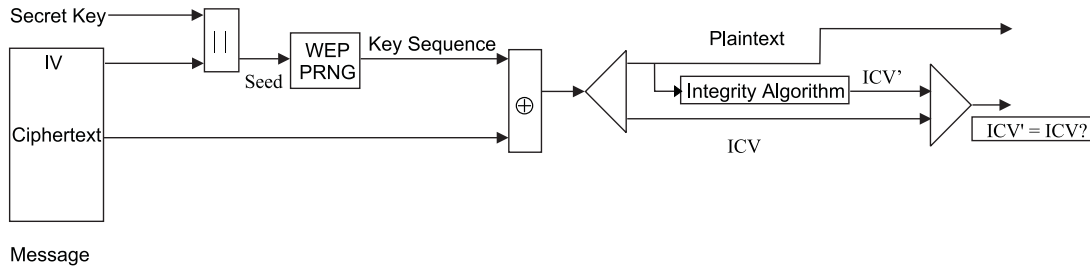


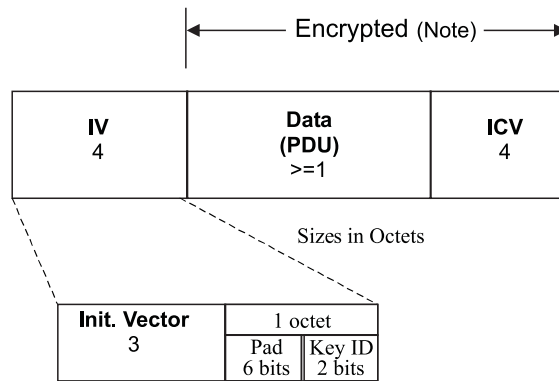
Figure 45—WEP decipherment block diagram

### 8.2.4 WEP algorithm specification

WEP uses the RC4 PRNG algorithm from RSA Data Security, Inc.<sup>6</sup>

### 8.2.5 WEP MPDU expansion

Figure 46 shows the encrypted MPDU as constructed by the WEP algorithm.



NOTE-The encipherment process has expanded the original MPDU by 8 octets, 4 for the Initialization Vector (IV) field and 4 for the Integrity Check Value (ICV). The ICV is calculated on the Data field only.

Figure 46—Construction of expanded WEP MPDU

The WEP ICV shall be a 32-bit field containing the 32-bit cyclic redundancy code (CRC) defined in 7.1.3.6 calculated over the Data (PDU) field as depicted in Figure 46. The expanded MPDU shall include a 32-bit IV field immediately preceding the MPDU. This field shall contain three subfields: a three-octet field that contains the initialization vector, a 2-bit key ID field, and a 6-bit pad field. The ordering conventions defined in 7.1.1 apply to the IV fields and its subfields and to the ICV field. The key ID subfield contents select one

<sup>6</sup>Details of the RC4 algorithm are available from RSA. Please contact RSA for algorithm details and the uniform RC4 licensee terms that RSA offers to anyone wishing to use RC4 for the purpose of implementing the IEEE 802.11 WEP option. If necessary, contact the IEEE Standards Department for details on how to communicate with RSA.

of four possible secret key values for use in decrypting this MPDU. Interpretation of these bits is discussed further in 8.3.2. The contents of the pad subfield shall be zero. The key ID occupies the two msb of the last octet of the IV field, while the pad occupies the six lsb of this octet.

The WEP mechanism is invisible to entities outside the IEEE 802.11 MAC data path.

### 8.3 Security-Related MIB attributes

The IEEE 802.11 security mechanisms are controlled via the MAC management path and related MIB attributes. This subclause gives an overview of the security related MIB attributes and how they are used. For details of the MIB attribute definitions, refer to 11.4.

#### 8.3.1 Authentication-Related MIB attributes

The type of authentication invoked when authentication is attempted is controlled by the AuthenticationType parameter to the MLME-AUTHENTICATE.request primitive. The type of authentication request that may be accepted by a STA is controlled by the MIB attribute aAuthenticationType. The type of authentication is selected from the following set of values:

- Open System
- Shared Key

All other values are reserved. The numeric encoding of these values is given in 7.3.1.1.

#### 8.3.2 Privacy-Related MIB attributes

WEP invocation is controlled by the parameters passed to the MLME-AUTHENTICATE.request primitive as well as a number of MIB attributes. An overview of the attributes and their usage is given in this clause. All MIB attributes that hold WEP keys are externally write-only; the contents shall not be readable via MAC management SAPs. See 11.4 for the formal MIB attribute definitions.

The boolean variable aPrivacyInvoked shall be set to “false” to prevent the STA from transmitting MPDUs of type Data with the WEP subfield of the Frame Control field set to 1. It does not affect MPDU or MMPDU reception.

The default value for all WEP keys shall be null. Note that encrypting a frame using WEP with a null key is not the same as failing to encrypt the frame. Any request to encrypt a frame with a null key shall result in the MSDU being discarded and an MA-UNIDATA-STATUS.indication with a transmission status indicating that the frame may not be encrypted with a null key. Decrypting a frame whose WEP subfield is set to 1 involves stripping the IV, and checking the ICV against the calculated ICV' value computed over the data contained in the MPDU.

To support shared key configurations, the MIB contains a four-element vector called “aWEPDefaultKeys.” The default value for each element of this vector is null. These elements contain the default keys to be used with WEP.

An additional attribute called “aWEPDefaultKeyID” is an integer. When set to a value of 0, 1, 2, or 3, MPDUs transmitted with the WEP subfield of the Frame Control field set to 1 shall be encrypted using the first, second, third, or fourth element, respectively, from aWEPDefaultKeys, unless the frame has an individual RA and a key mapping exists for the RA of the frame. On receive, the incoming MPDU shall be decrypted using the element from aWEPDefaultKeys specified by the received key ID field, unless the frame has an individual RA and a key mapping exists for the TA of the frame. The value in the transmitted key ID

field shall be zero in all cases except when aWEPDefaultKeyID is used to encrypt a frame and is set to a value of 1, 2, or 3, in which case the transmitted key ID field shall contain the value of aWEPDefaultKeyID.

When the boolean attribute aExcludeUnencrypted is set to True, MPDUs of type Data received by the STA with the WEP subfield of the Frame Control field equal to zero shall not be indicated at the MAC service interface. When aExcludeUnencrypted is set to True, only MSDUs that have been decrypted successfully shall be indicated at the MAC service interface.

IEEE 802.11 does not require that the same WEP key be used for all STAs. The MIB supports the ability to share a separate WEP key for each RA/TA pair. Key mapping is supported by a MIB attribute that is an array called "aWEPKeyMappings." aWEPKeyMappings contains zero or one entry for each MAC address, up to an implementation-defined maximum number of entries identified by aWEPKeyMappingLength, and contains two fields for each entry: a boolean "WEPOn" and the corresponding WEPKey. In an infrastructure BSS, the AP's WEPOn value in the entry in its aWEPKeyMapping table corresponding to a STA's MAC address shall not be set to True for a STA if that STA has not successfully initiated and completed an authentication sequence using an authentication type other than "Open System." The default value for all WEPOn fields is False. aWEPKeyMappings shall be indexed by either RA or TA addresses (since WEP is applied only to the wireless link), as described below. When an entry in the table exists for a particular MAC address, the values in the aWEPKeyMappings attribute shall be used instead of the aWEPDefaultKeyID and aWEPDefaultKeys variables.

The minimal value of aWEPKeyMappingLength shall be 10. This value represents a minimum capability that may be assumed for any STA implementing the WEP option.

When transmitting a frame of type Data, the values of aPrivacyInvoked, aWEPKeyMappings, aWEPDefaultKeys, and aWEPDefaultKeyID in effect at an unspecified time between receipt by the MAC of the MAUNITDATA.request primitive and the time of transmission of that frame shall be used according to the following decision tree:

```

if aPrivacyInvoked is "false"
    the MPDU is transmitted without encryption
else
    if (the MPDU has an individual RA and
        there is an entry in aWEPKeyMappings for that RA)
        if that entry has WEPOn set to "false"
            the MPDU is transmitted without encryption
        else
            if that entry contains a key that is null
                discard the entire MSDU and generate an
                MA-UNITDATA-STATUS.indication primitive to
                notify LLC that the MSDU was undeliverable due to
                a null WEP key
            else
                encrypt the MPDU using that entry's key, setting the keyID
                subfield of the IV field to zero
    else
        if (the MPDU has a group RA and the Privacy subfield
            of the Capability Information field in this BSS is set to 0)
            the MPDU is transmitted without encryption
        else
            if aWEPDefaultKeys[aWEPDefaultKeyID] is null
                discard the MSDU and generate an
                MA-UNITDATA-STATUS.indication primitive to
                notify LLC that the entire MSDU was undeliverable

```

```
        due to a null WEP key
    else
        encrypt the MPDU using
        aWEPDefaultKeys[aWEPDefaultKeyID],
        setting the KeyID subfield of the IV field to
        aWEPDefaultKeyID
```

When receiving a frame of type Data, the values of aPrivacyOptionImplemented, aWEPKeyMappings, aWEPDefaultKeys, aWEPDefaultKeyID, and aExcludeUnencrypted in effect at the time the PHY-RXSTART.indication primitive is received by the MAC shall be used according to the following decision tree:

```
    if the WEP subfield of the Frame Control Field is zero
        if aExcludeUnencrypted is "true"
            discard the frame body without indication to LLC and increment
            aWEPExcludedCount
        else
            receive the frame without decryption
    else
        if aPrivacyOptionImplemented is "true"
            if (the MPDU has individual RA and
                there is an entry in aWEPKeyMappings matching the MPDU's TA)
                if that entry has WEPOn set to "false"
                    discard the frame body and increment
                    aWEPUndecryptableCount
                else
                    if that entry contains a key that is null
                        discard the frame body and increment
                        aWEPUndecryptableCount
                    else
                        attempt to decrypt with that key, incrementing
                        aWEPICVErrorCount if the ICV check fails
            else
                if aWEPDefaultKeys[keyID] is null
                    discard the frame body and increment
                    aWEPUndecryptableCount
                else
                    attempt to decrypt with aWEPDefaultKeys[keyID],
                    incrementing aWEPICVErrorCount if the ICV check fails
        else
            discard the frame body and increment aWEPUndecryptableCount
```

When transmitting a frame of type Management, subtype Authentication with an Authentication Transaction Sequence Number field value of 2, the MAC shall operate according to the following decision tree:

```
    if aPrivacyOptionImplemented is "false"
        the MMPDU is transmitted with a sequence
        of zero octets in the Challenge Text field and a Status Code value of 13
    else
        the MMPDU is transmitted with a sequence of 128 octets generated using the
        WEP PRNG and a key whose value is unspecified and beyond the scope of this
        standard and a randomly chosen IV value (note that this will typically be selected
        by the same mechanism for choosing IV values for transmitted data MPDUs)
        in the Challenge Text field and a status code value of 0 (the IV used is
```

immaterial and is not transmitted). Note that there are cryptographic issues involved in the choice of key/IV for this process as the challenge text is sent unencrypted and therefore provides a known output sequence from the PRNG.

When receiving a frame of type Management, subtype Authentication with an Authentication Transaction Sequence Number field value of 2, the MAC shall operate according to the following decision tree:

```

if the WEP subfield of the Frame Control field is one
    respond with a status code value of 15
else
    if aPrivacyOptionImplemented is "true"
        if there is a mapping in aWEPKeyMappings matching the MSDU's TA
            if that key is null
                respond with a frame whose Authentication Transaction
                Sequence Number field is 3 that contains the appropriate
                Authentication Algorithm Number, a status code value of
                15 and no Challenge Text field, without encrypting the
                contents of the frame
            else
                respond with a frame whose Authentication Transaction
                Sequence Number field is 3 that contains the appropriate
                Authentication Algorithm Number, a status code value of
                0 and the identical Challenge Text field, encrypted using
                that key, and setting the key ID subfield in the IV field to 0
        else
            if aWEPDefaultKeys[aWEPDefaultKeyID] is null
                respond with a frame whose Authentication Transaction
                Sequence Number field is 3 that contains the appropriate
                Authentication Algorithm Number, a status code value of
                15 and no Challenge Text field, without encrypting the
                contents of the frame
            else
                respond with a frame whose Authentication Transaction
                Sequence Number field is 3 that contains the appropriate
                Authentication Algorithm Number, a status code value of 0
                and the identical Challenge Text field, encrypted using
                aWEPDefaultKeys[aWEPDefaultKeyID], setting the
                key ID subfield in the IV field to aWEPDefaultKeyID
    else
        respond with a frame whose Authentication Transaction
        Sequence Number field is 3 that contains the appropriate Authentication
        Algorithm Number, a status code value of 13 and no Challenge Text
        field, without encrypting the contents of the frame

```

When receiving a frame of type Management, subtype Authentication with an Authentication Transaction Sequence Number field value of 3, the MAC shall operate according to the following decision tree:

```

if the WEP subfield of the Frame Control field is zero
    respond with a status code value of 15
else
    if aPrivacyOptionImplemented is "true"
        if there is a mapping in aWEPKeyMappings matching the MSDU's TA
            if that key is null

```



```
        respond with a frame whose Authentication Transaction
        Sequence Number field is 4 that contains the appropriate
        Authentication Algorithm Number, and a status code value
        of 15 without encrypting the contents of the frame
    else
        attempt to decrypt with that key, incrementing
        aWEPICVErrorCount and responding with a status code value
        of 15 if the ICV check fails
    else
        if aWEPDefaultKeys[keyID] is null
            respond with a frame whose Authentication Transaction
            Sequence Number field is 4 that contains the appropriate
            Authentication Algorithm Number, and a status code value
            of 15 without encrypting the contents of the frame
        else
            attempt to decrypt with aWEPDefaultKeys[keyID],
            incrementing aWEPICVErrorCount and responding with
            a status code value of 15 if the ICV check fails
    else
        respond with a frame whose Authentication Transaction Sequence Number
        field is 4 that contains the appropriate Authentication Algorithm Number,
        and a status code value of 15
```

The attribute aPrivacyInvoked shall not take the value “true” if the attribute aPrivacyOptionImplemented is “false.” Setting the attribute aWEPKeyMappings to a value that includes more than aWEPKeyMappingLength entries is illegal and shall have an implementation-specific effect on the operation of the privacy service. Note that aWEPKeyMappings may contain between zero and aWEPKeyMappingLength entries, inclusive.

It is recommended that the values of the attributes in the aPrivacygrp not be changed during the authentication sequence as unintended operation may result.

## 9. MAC sublayer functional description

The MAC functional description is presented in this clause. The architecture of the MAC sublayer, including the distributed coordination function (DCF), the point coordination function (PCF), and their coexistence in an IEEE 802.11 LAN are introduced in 9.1. These functions are expanded on in 9.2 and 9.3, and a complete functional description of each is provided. Fragmentation and defragmentation are covered in 9.4 and 9.5. Multirate support is addressed in 9.6. The allowable frame exchange sequences are listed in 9.7. Finally, a number of additional restrictions to limit the cases in which MSDUs are reordered or discarded are described in 9.8.

### 9.1 MAC architecture

The MAC architecture can be described as shown in Figure 47 as providing the PCF through the services of the DCF.

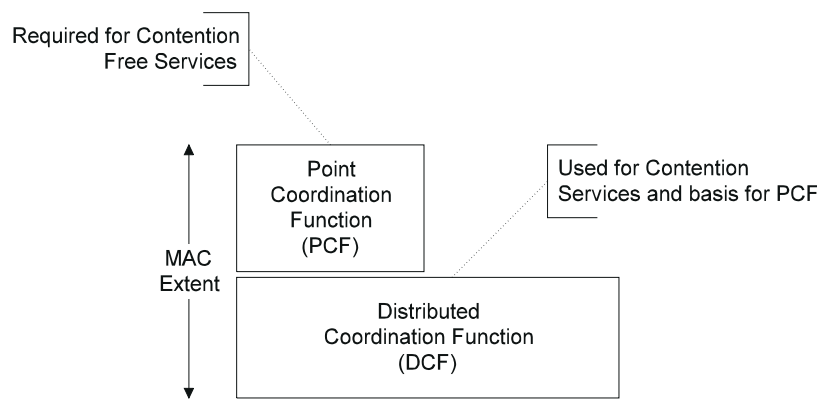


Figure 47—MAC architecture

#### 9.1.1 Distributed coordination function (DCF)

The fundamental access method of the IEEE 802.11 MAC is a DCF known as *carrier sense multiple access with collision avoidance*, or CSMA/CA. The DCF shall be implemented in all STAs, for use within both IBSS and infrastructure network configurations.

For a STA to transmit, it shall sense the medium to determine if another STA is transmitting. If the medium is not determined to be busy (see 9.2.1), the transmission may proceed. The CSMA/CA distributed algorithm mandates that a gap of a minimum specified duration exist between contiguous frame sequences. A transmitting STA shall ensure that the medium is idle for this required duration before attempting to transmit. If the medium is determined to be busy, the STA shall defer until the end of the current transmission. After deferral, or prior to attempting to transmit again immediately after a successful transmission, the STA shall select a random backoff interval and shall decrement the backoff interval counter while the medium is idle. A refinement of the method may be used under various circumstances to further minimize collisions—here the transmitting and receiving STA exchange short control frames [request to send (RTS) and clear to send (CTS) frames] after determining that the medium is idle and after any deferrals or backoffs, prior to data transmission. The details of CSMA/CA, deferrals, and backoffs are described in 9.2. RTS/CTS exchanges are also presented in 9.2.

#### 9.1.2 Point coordination function (PCF)

The IEEE 802.11 MAC may also incorporate an optional access method called a PCF, which is only usable on infrastructure network configurations. This access method uses a point coordinator (PC), which shall

operate at the access point of the BSS, to determine which STA currently has the right to transmit. The operation is essentially that of polling with the PC performing the role of the polling master. The operation of the PCF may require additional coordination, not specified in this standard, to permit efficient operation in cases where multiple point-coordinated BSSs are operating on the same channel, in overlapping physical space.

The PCF uses a virtual carrier sense mechanism aided by an access priority mechanism. The PCF shall distribute information within Beacon management frames to gain control of the medium by setting the network allocation vector (NAV) in STAs. In addition, all frame transmissions under the PCF may use an interframe space (IFS) that is smaller than the IFS for frames transmitted via the DCF. The use of a smaller IFS implies that point-coordinated traffic shall have priority access to the medium over STAs in overlapping BSSs operating under the DCF access method.

The access priority provided by a PCF may be utilized to create a *contention-free* (CF) access method. The PC controls the frame transmissions of the STAs so as to eliminate contention for a limited period of time.

### 9.1.3 Coexistence of DCF and PCF

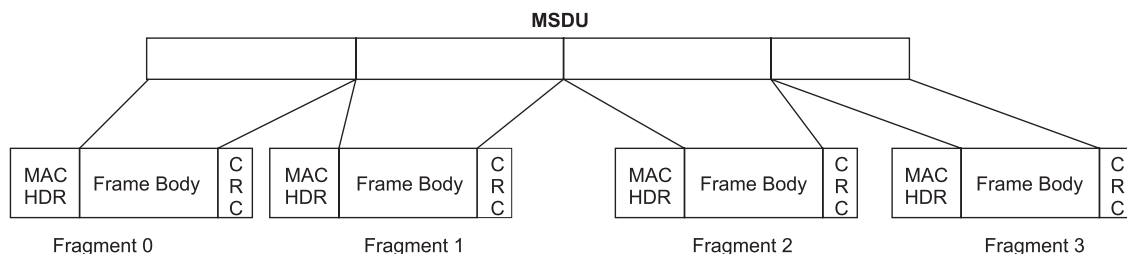
The DCF and the PCF shall coexist in a manner that permits both to operate concurrently within the same BSS. When a PC is operating in a BSS, the two access methods alternate, with a contention-free period (CFP) followed by a contention period (CP). This is described in greater detail in 9.3.

### 9.1.4 Fragmentation/defragmentation overview

The process of partitioning a MAC service data unit (MSDU) or a MAC management protocol data unit (MMPDU) into smaller MAC level frames, MAC protocol data units (MPDUs), is called fragmentation. Fragmentation creates MPDUs smaller than the original MSDU or MMPDU length to increase reliability, by increasing the probability of successful transmission of the MSDU or MMPDU in cases where channel characteristics limit reception reliability for longer frames. Fragmentation is accomplished at each immediate transmitter. The process of recombining MPDUs into a single MSDU or MMPDU is defined as defragmentation. Defragmentation is accomplished at each immediate recipient.

Only MPDUs with a unicast receiver address shall be fragmented. Broadcast/multicast frames shall not be fragmented even if their length exceeds aFragmentationThreshold.

When a directed MSDU is received from the LLC or a directed MMPDU is received from the MAC sublayer management entity (MLME) with a length greater than aFragmentationThreshold, the MSDU or MMPDU shall be fragmented. The MSDU or MMPDU is divided into MPDUs. Each fragment is a frame no larger than aFragmentationThreshold. It is possible that any fragment may be a frame smaller than aFragmentationThreshold. An illustration of fragmentation is shown in Figure 48.



**Figure 48—Fragmentation**

The MPDUs resulting from the fragmentation of an MSDU or MMPDU are sent as independent transmissions, each of which is separately acknowledged. This permits transmission retries to occur per fragment,

rather than per MSDU or MMPDU. Unless interrupted due to medium occupancy limitations for a given PHY, the fragments of a single MSDU or MMPDU are sent as a burst during the CP, using a single invocation of the DCF medium access procedure. The fragments of a single MSDU or MMPDU are sent during a CFP as individual frames obeying the rules of the PC medium access procedure.

### 9.1.5 MAC data service

The MAC data service shall translate MAC service requests from LLC into input signals utilized by the MAC state machines. The MAC data service shall also translate output signals from the MAC state machines into service indications to LLC. The translations are given in the MAC data service state machine defined in Annex C.

## 9.2 DCF

The basic medium access protocol is a DCF that allows for automatic medium sharing between compatible PHYs through the use of CSMA/CA and a random backoff time following a busy medium condition. In addition, all directed traffic uses immediate positive acknowledgment (ACK frame) where retransmission is scheduled by the sender if no ACK is received.

The CSMA/CA protocol is designed to reduce the collision probability between multiple STAs accessing a medium, at the point where collisions would most likely occur. Just after the medium becomes idle following a busy medium (as indicated by the CS function) is when the highest probability of a collision exists. This is because multiple STAs could have been waiting for the medium to become available again. This is the situation that necessitates a random backoff procedure to resolve medium contention conflicts.

Carrier Sense shall be performed both through physical and virtual mechanisms.

The virtual carrier sense mechanism is achieved by distributing reservation information announcing the impending use of the medium. The exchange of RTS and CTS frames prior to the actual data frame is one means of distribution of this medium reservation information. The RTS and CTS frames contain a Duration/ID field that defines the period of time that the medium is to be reserved to transmit the actual data frame and the returning ACK frame. All STAs within the reception range of either the originating STA (which transmits the RTS) or the destination STA (which transmits the CTS) shall learn of the medium reservation. Thus a STA can be unable to receive from the originating STA, yet still know about the impending use of the medium to transmit a data frame.

Another means of distributing the medium reservation information is the Duration/ID field in directed frames. This field gives the time that the medium is reserved, either to the end of the immediately following ACK, or in the case of a fragment sequence, to the end of the ACK following the next fragment.

The RTS/CTS exchange also performs both a type of fast collision inference and a transmission path check. If the return CTS is not detected by the STA originating the RTS, the originating STA may repeat the process (after observing the other medium-use rules) more quickly than if the long data frame had been transmitted and a return ACK frame had not been detected.

Another advantage of the RTS/CTS mechanism occurs where multiple BSSs utilizing the same channel overlap. The medium reservation mechanism works across the BSA boundaries. The RTS/CTS mechanism may also improve operation in a typical situation where all STAs can receive from the AP, but cannot receive from all other STAs in the BSA.

The RTS/CTS mechanism cannot be used for MPDUs with broadcast and multicast immediate address because there are multiple destinations for the RTS, and thus potentially multiple concurrent senders of the CTS in response. The RTS/CTS mechanism need not be used for every data frame transmission. Because the

additional RTS and CTS frames add overhead inefficiency, the mechanism is not always justified, especially for short data frames.

The use of the RTS/CTS mechanism is under control of the `aRTSThreshold` attribute. This attribute may be set on a per-STA basis. This mechanism allows STAs to be configured to use RTS/CTS either always, never, or only on frames longer than a specified length.

A STA configured not to initiate the RTS/CTS mechanism shall still update its virtual carrier sense mechanism with the duration information contained in a received RTS or CTS frame, and shall always respond to an RTS addressed to it with a CTS.

The medium access protocol allows for STAs to support different sets of data rates. All STAs shall receive all the data rates in the `aBasicRateSet` and transmit at one or more of the `aBasicRateSet` data rates. To support the proper operation of the RTS/CTS and the virtual carrier sense mechanism, all STAs shall be able to detect the RTS and CTS frames. For this reason the RTS and CTS frames shall be transmitted at one of the `aBasicRateSet` rates. (See 9.6 for a description of multirate operation.)

Data frames sent under the DCF shall use the frame type Data and subtype Data or Null Function. STAs receiving Data type frames shall only consider the frame body as the basis of a possible indication to LLC.

### 9.2.1 Carrier sense mechanism

Physical and virtual carrier sense functions are used to determine the state of the medium. When either function indicates a busy medium, the medium shall be considered busy; otherwise, it shall be considered idle.

A physical carrier sense mechanism shall be provided by the PHY. See Clause 12 for how this information is conveyed to the MAC. The details of physical carrier sense are provided in the individual PHY specifications.

A virtual carrier sense mechanism shall be provided by the MAC. This mechanism is referred to as the network allocation vector (NAV). The NAV maintains a prediction of future traffic on the medium based on duration information that is announced in RTS/CTS frames prior to the actual exchange of data. The duration information is also available in the MAC headers of all frames sent during the CP other than PS-Poll Control frames. The mechanism for setting the NAV using RTS/CTS in the DCF is described in 9.2.5.4, and use of the NAV in PCF is described in 9.3.2.2.

The carrier sense mechanism combines the NAV state and the STA's transmitter status with physical carrier sense to determine the busy/idle state of the medium. The NAV may be thought of as a counter, which counts down to zero at a uniform rate. When the counter is zero, the virtual carrier sense indication is that the medium is idle; when nonzero, that it is busy. The medium shall be determined to be busy whenever the STA is transmitting.

### 9.2.2 MAC-Level acknowledgments

The reception of some frames, as described in 9.7, 9.2.8, and 9.3.3.4, require the receiving STA to respond with an acknowledgment, generally an ACK frame, if the FCS of the received frame is correct. This technique is known as positive acknowledgment.

Lack of reception of an expected ACK frame indicates to the source STA that an error has occurred. Note, however, that the destination STA may have received the frame correctly, and that the error occurred in the reception of the ACK frame. To the initiator of the frame exchange, this condition is indistinguishable from an error occurring in the initial frame.

### 9.2.3 Interframe space (IFS)

The time interval between frames is called the interframe space (IFS). A STA shall determine that the medium is idle through the use of the carrier sense function for the interval specified. Four different IFSs are defined to provide priority levels for access to the wireless media; they are listed in order, from the shortest to the longest. Figure 49 shows some of these relationships.

- a) SIFS short interframe space
- b) PIFS PCF interframe space
- c) DIFS DCF interframe space
- d) EIFS extended interframe space

The different IFSs shall be independent of the STA bit rate. The IFS timings shall be defined as time gaps on the medium, and shall be fixed for each PHY (even in multirate capable PHYs). The IFS values are determined from attributes specified in the PHY MIB.

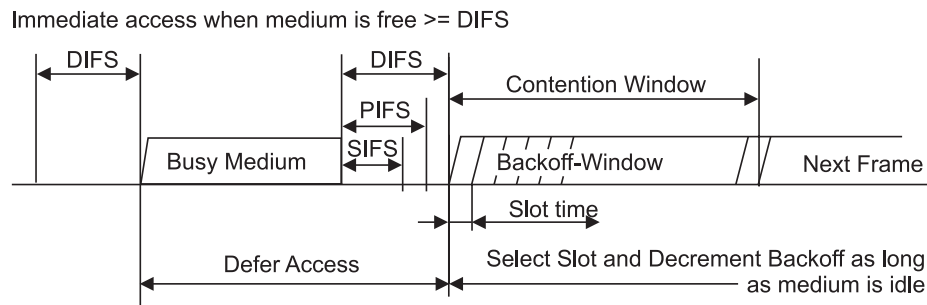


Figure 49—Some IFS relationships

#### 9.2.3.1 Short IFS (SIFS)

The SIFS shall be used for an ACK frame, a CTS frame, the second or subsequent MPDU of a fragment burst, by a STA responding to any polling by the PCF, and may be used by a PC for any types of frames during the CFP (see 9.3). The SIFS is the time from the end of the last symbol of the previous frame to the beginning of the first symbol of the preamble of the subsequent frame as seen at the air interface. The valid cases where the SIFS may or shall be used are listed in the frame exchange sequences found in 9.7.

The SIFS timing shall be achieved when the transmission of the subsequent frame is started at the TxSIFS Slot boundary as specified in 9.2.10. An IEEE 802.11 implementation shall not allow the space between frames that are defined to be separated by a SIFS time, as measured on the medium, to vary from the nominal SIFS value by more than  $\pm 10\%$  of aSlotTime for the PHY in use.

SIFS is the shortest of the interframe spaces. SIFS shall be used when STAs have seized the medium and need to keep it for the duration of the frame exchange sequence to be performed. Using the smallest gap between transmissions within the frame exchange sequence prevents other STAs, which are required to wait for the medium to be idle for a longer gap, from attempting to use the medium, thus giving priority to completion of the frame exchange sequence in progress.

#### 9.2.3.2 PCF IFS (PIFS)

The PIFS shall be used only by STAs operating under the PCF to gain priority access to the medium at the start of the CFP. A STA using the PCF shall be allowed to transmit contention-free traffic after its carrier sense mechanism (see 9.2.1) determines that the medium is idle at the TxPIFS slot boundary as defined in 9.2.10. Subclause 9.3 describes the use of the PIFS by STAs operating under the PCF.

### 9.2.3.3 DCF IFS (DIFS)

The DIFS shall be used by STAs operating under the DCF to transmit data frames (MPDUs) and management frames (MMPDUs). A STA using the DCF shall be allowed to transmit if its carrier sense mechanism (see 9.2.1) determines that the medium is idle at the TxDIFS slot boundary as defined in 9.2.10 after a correctly received frame, and its backoff time has expired. A STA using the DCF shall not transmit within an EIFS after it determines that the medium is idle following reception of a frame for which the PHYRX-END.indication primitive contained an error or a frame for which the MAC FCS value was not correct. A STA may transmit after subsequent reception of an error-free frame, resynchronizing the STA. This allows the STA to transmit using the DIFS following that frame.

### 9.2.3.4 Extended IFS (EIFS)

The EIFS shall be used by the DCF whenever the PHY has indicated to the MAC that a frame transmission was begun that did not result in the correct reception of a complete MAC frame with a correct FCS value. The duration of an EIFS is defined in 9.2.10. The EIFS interval shall begin following indication by the PHY that the medium is idle after detection of the erroneous frame, without regard to the virtual carrier-sense mechanism. The EIFS is defined to provide enough time for another STA to acknowledge what was, to this STA, an incorrectly received frame before this STA commences transmission. Reception of an error-free frame during the EIFS resynchronizes the STA to the actual busy/idle state of the medium, so the EIFS is terminated and normal medium-access (using DIFS and, if necessary, backoff) continues following reception of that frame.

### 9.2.4 Random backoff time

A STA desiring to initiate transfer of data MPDUs and/or management MMPDUs shall invoke the carrier sense mechanism (see 9.2.1) to determine the busy/idle state of the medium. If the medium is busy, the STA shall defer until the medium is determined to be idle without interruption for a period of time equal to DIFS when the last frame detected on the medium was received correctly, or after the medium is determined to be idle without interruption for a period of time equal to EIFS when the last frame detected on the medium was not received correctly. After this DIFS or EIFS medium idle time, the STA shall then generate a random backoff period for an additional deferral time before transmitting, unless the backoff timer already contains a nonzero value, in which case the selection of a random number is not needed and not performed. This process minimizes collisions during contention between multiple STAs that have been deferring to the same event.

$$\text{Backoff Time} = \text{Random}() \times \text{aSlotTime}$$

where

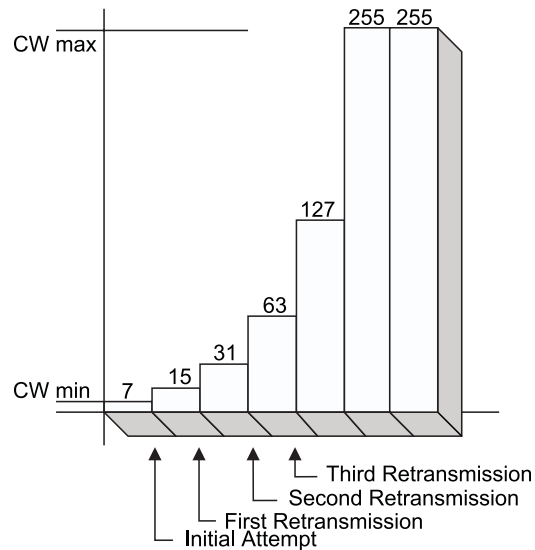
Random() = Pseudorandom integer drawn from a uniform distribution over the interval [0,CW], where CW is an integer within the range of values of the MIB attributes aCWmin and aCWmax,  $\text{aCWmin} \leq \text{CW} \leq \text{aCWmax}$ . It is important that designers recognize the need for statistical independence among the random number streams among STAs.

aSlotTime = The value of the correspondingly named MIB attribute.

The contention window (CW) parameter shall take an initial value of aCWmin. Every STA shall maintain a STA short retry count (SSRC) as well as a STA long retry count (SLRC), both of which shall take an initial value of zero. The SSRC shall be incremented whenever any short retry count associated with any MSDU is incremented. The SLRC shall be incremented whenever any long retry count associated with any MSDU is incremented. The CW shall take the next value in the series every time an unsuccessful attempt to transmit an MPDU causes either STA retry counter to increment, until the CW reaches the value of aCWmax. A retry is defined as the entire sequence of frames sent, separated by SIFS intervals, in an attempt to deliver an MPDU, as described in 9.7. Once it reaches aCWmax, the CW shall remain at the value of aCWmax until it is reset. This improves the stability of the access protocol under high load conditions. See Figure 50.

The CW shall be reset to aCWmin after every successful attempt to transmit an MSDU or MMPDU, when SLRC reaches aLongRetryLimit, or when SSRC reaches aShortRetryLimit. The SSRC shall be reset to 0 whenever a CTS frame is received in response to an RTS frame, whenever an ACK frame is received in response to an MPDU or MMPDU transmission, or whenever a frame with a group address in the Address1 field is transmitted. The SLRC shall be reset to 0 whenever an ACK frame is received in response to transmission of an MPDU or MMPDU of length greater than aRTSThreshold, or whenever a frame with a group address in the Address1 field is transmitted.

The set of CW values shall be sequentially ascending integer powers of 2, minus 1, beginning with a PHY-specific aCWmin value, and continuing up to and including a PHY-specific aCWmax value.



**Figure 50—An example of exponential increase of CW**

## 9.2.5 DCF access procedure

The CSMA/CA access method is the foundation of the DCF. The operational rules vary slightly between DCF and PCF.

### 9.2.5.1 Basic access

Basic access refers to the core mechanism a STA uses to determine whether it may transmit.

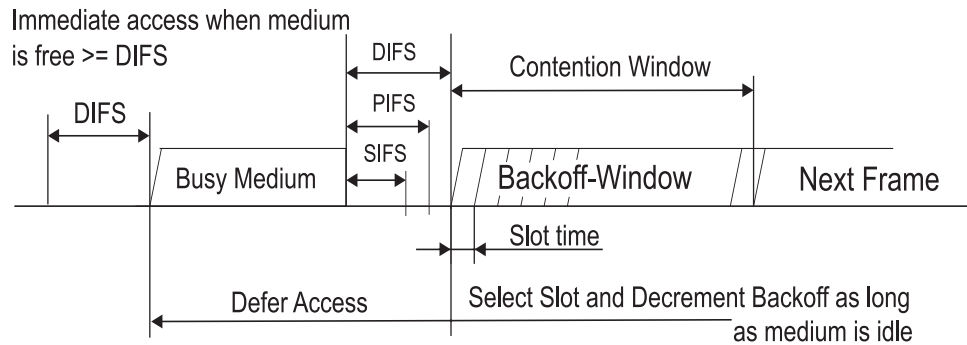
In general, a STA may transmit a pending MPDU when it is operating under the DCF access method, either in the absence of a PC, or in the CP of the PCF access method, when the STA determines that the medium is idle for greater than or equal to a DIFS period, or an EIFS period if the immediately preceding medium-busy event was caused by detection of a frame that was not received at this STA with a correct MAC FCS value. If, under these conditions, the medium is determined by the carrier sense mechanism to be busy when a STA desires to initiate the initial frame of one of the frame exchanges described in 9.7, exclusive of the CF period, the random backoff algorithm described in 9.2.5.2 shall be followed. There are conditions, specified elsewhere in Clause 9, where the random backoff algorithm shall be followed even for the first attempt to initiate a frame exchange sequence.

In a STA having an FH PHY, control of the channel is lost at a dwell time boundary and the STA shall have to contend for the channel after the dwell boundary. It is required that STAs having an FH PHY complete transmission of the entire MPDU and associated acknowledgment (if required) before the dwell time bound-



ary. If, when transmitting or retransmitting an MPDU, there is not enough time remaining in the dwell to allow transmission of the MPDU plus the acknowledgment (if required), the STA shall defer the transmission by selecting a random backoff time, using the present CW (without advancing to the next value in the series). The short retry counter and long retry counter for the MSDU are not affected.

The basic access mechanism is illustrated in Figure 51.



**Figure 51 – Basic access method**

### 9.2.5.2 Backoff procedure

The backoff procedure shall be invoked for a STA to transfer a frame when finding the medium busy as indicated by either the physical or virtual carrier sense mechanism (see Figure 52). The backoff procedure shall also be invoked when a transmitting STA infers a failed transmission as defined in 9.2.5.7 or 9.2.8.

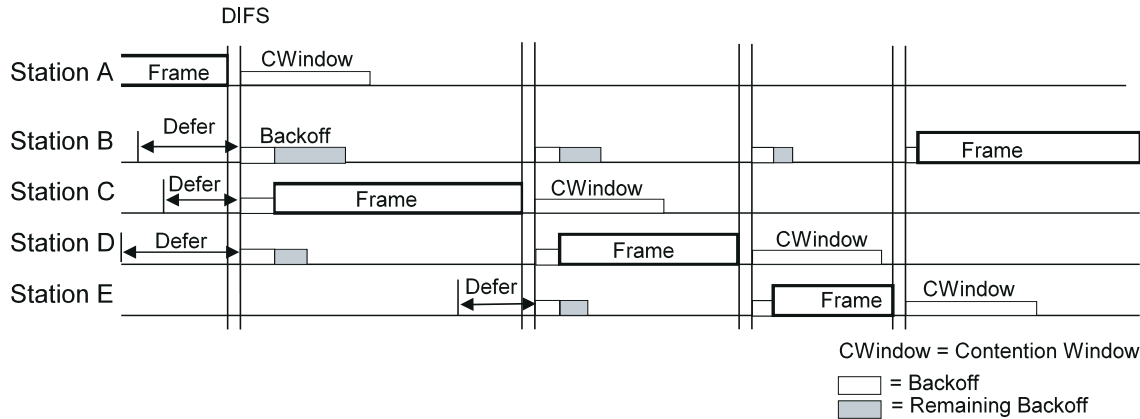
To begin the backoff procedure, the STA shall set its Backoff Timer to a random backoff time using the equation in 9.2.4. All backoff slots occur following a DIFS period during that the medium is determined to be idle for the duration of the DIFS period, or following an EIFS period during which the medium is determined to be idle for the duration of the EIFS period following detection of a frame that was not received correctly.

A STA performing the backoff procedure shall use the carrier sense mechanism (9.2.1) to determine whether there is activity during each backoff slot. If no medium activity is indicated for the duration of a particular backoff slot, then the backoff procedure shall decrement its backoff time by aSlotTime.

If the medium is determined to be busy at any time during a backoff slot, then the backoff procedure is suspended; that is, the backoff timer shall not decrement for that slot. The medium shall be determined to be idle for the duration of a DIFS period or EIFS, as appropriate (see 9.2.3), before the backoff procedure is allowed to resume. Transmission shall commence whenever the Backoff Timer reaches zero.

A backoff procedure shall be performed immediately after the end of every transmission with the More Fragments bit set to 0 of an MPDU of type Data, Management, or Control with subtype PS-Poll, even if no additional transmissions are currently queued. In the case of successful acknowledged transmissions, this backoff procedure shall begin at the end of the received ACK frame. In the case of unsuccessful transmissions requiring acknowledgment, this backoff procedure shall begin at the end of the ACK timeout interval. If the transmission was successful, the CW value reverts to aCW<sub>min</sub> before the random backoff interval is chosen, and the STA short retry count and/or STA long retry count are updated as described in 9.2.4. This assures that transmitted frames from a STA are always separated by at least one backoff interval.

The effect of this procedure is that when multiple STAs are deferring and go into random backoff, then the STA selecting the smallest backoff time using the random function will win the contention.



**Figure 52—Backoff procedure**

In an IBSS, the backoff time for a pending non-beacon or non-ATIM transmission shall not decrement in the period from the target beacon transmission time (TBTT) until the expiration of the ATIM window and the backoff time for a pending ATIM management frame shall decrement only within the ATIM window. (See Clause 11.) Within an IBSS, a separate backoff interval shall be generated to precede the transmission of a beacon, as described in 11.1.2.2.

### 9.2.5.3 Recovery procedures and retransmit limits

Error recovery is always the responsibility of the STA that initiates a frame exchange sequence, as defined in 9.7. Many circumstances may cause an error to occur that requires recovery. For example, the CTS frame may not be returned after an RTS frame is transmitted. This may happen due to a collision with another transmission, due to interference in the channel during the RTS or CTS frame, or because the STA receiving the RTS frame has an active virtual carrier sense condition (indicating a busy medium time period).

Error recovery shall be attempted by retrying transmissions for frame exchange sequences that the initiating STA infers have failed. Retries shall continue, for each failing frame exchange sequence, until the transmission is successful, or until the relevant retry limit is reached, whichever occurs first. STAs shall maintain a short retry count and a long retry count for each MSDU or MMPDU awaiting transmission. These counts are incremented and reset independently of each other.

After an RTS frame is transmitted, the STA shall perform the CTS procedure, as defined in 9.2.5.7. If the RTS transmission fails, the short retry count for the MSDU or MMPDU and the STA short retry count are incremented. This process shall continue until the number of attempts to transmit that MSDU or MMPDU reaches aShortRetryLimit.

After transmitting a frame that requires acknowledgment, the STA shall perform the ACK procedure, as defined in 9.2.8. The short retry count for an MSDU or MMPDU and the STA short retry count shall be incremented every time transmission of a MAC frame of length less than or equal to aRTSThreshold fails for that MSDU or MMPDU. This short retry count and the STA short retry count shall be reset when a MAC frame of length less than or equal to aRTSThreshold succeeds for that MSDU or MMPDU. The long retry count for an MSDU or MMPDU and the STA long retry count shall be incremented every time transmission of a MAC frame of length greater than aRTSThreshold fails for that MSDU or MMPDU. This long retry count and the STA long retry count shall be reset when a MAC frame of length greater than aRTSThreshold succeeds for that MSDU or MMPDU. All retransmission attempts for an MSDU or MMPDU that has failed the ACK procedure one or more times shall be made with the Retry field set to 1 in the Data or Management type frame.

Retries for failed transmission attempts shall continue until the short retry count for the MSDU or MMPDU is equal to aShortRetryLimit or until the long retry count for the MSDU or MMPDU is equal to aLongRetryLimit. When either of these limits is reached, retry attempts shall cease, and the MSDU or MMPDU shall be discarded.

A STA in power-save mode, in an ESS, initiates a frame exchange sequence by transmitting a PS-Poll frame to request data from an AP. In the event that neither an ACK frame nor a data frame is received from the AP in response to a PS-Poll frame, then the STA shall retry the sequence, by transmitting another PS-Poll frame, at its convenience. If the AP sends a data frame in response to a PS-Poll frame, but fails to receive the ACK frame acknowledging this data frame, the next PS-Poll frame from the same STA may cause a retransmission of the last MSDU. This duplicate MSDU shall be filtered at the receiving STA using the normal duplicate frame filtering mechanism. If the AP responds to a PS-Poll by transmitting an ACK frame, then responsibility for the data frame delivery error recovery shifts to the AP because the data is transferred in a subsequent frame exchange sequence, which is initiated by the AP. The AP shall attempt to deliver one MSDU to the STA that transmitted the PS-Poll, using any frame exchange sequence valid for a directed MSDU. If the power save STA that transmitted the PS-Poll returns to Doze state after transmitting the ACK frame in response to successful receipt of this MSDU, but the AP fails to receive this ACK frame, the AP will retry transmission of this MSDU until the relevant retry limit is reached. See Clause 11 for details on filtering of extra PS-Poll frames.

#### 9.2.5.4 Setting and resetting the NAV

STAs receiving a valid frame shall update their NAV with the information received in the Duration/ID field, but only when the new NAV value is greater than the current NAV value and only when the frame is not addressed to the receiving STA. Various additional conditions may set or reset the NAV, as described in 9.3.2.2. When the NAV is reset, a PHY-CCARESET.request shall be issued.

Figure 53 indicates the NAV for STAs that may hear the RTS frame, while other STAs may only receive the CTS frame, resulting in the lower NAV bar as shown (with the exception of the STA to which the RTS was addressed).

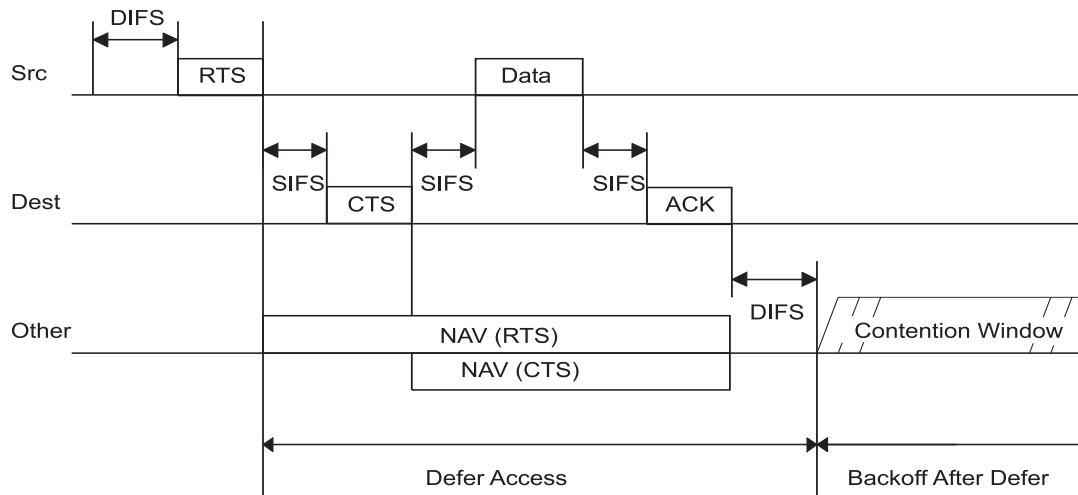


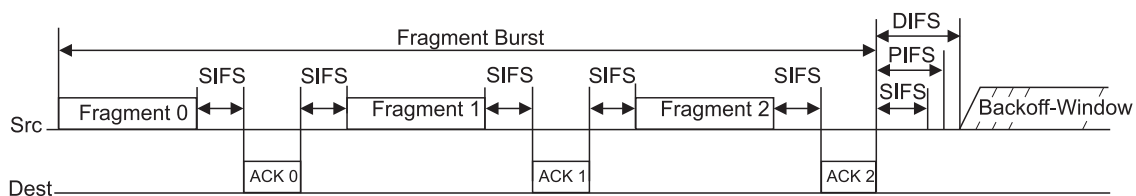
Figure 53—RTS/CTS/data/ACK and NAV setting

A STA that used information from an RTS frame as the most recent basis to update its NAV setting is permitted to reset its NAV if no PHY-RXSTART.indication is detected from the PHY during a period with a duration of  $(2 \times aSIFSTime) + (CTS\_Time) + (2 \times aSlotTime)$  starting at the PHY-RXEND.indication corresponding to the detection of the RTS frame. The “CTS\_Time” shall be calculated using the length of the CTS frame and the data rate at which the RTS frame used for the most recent NAV update was received.

### 9.2.5.5 Control of the channel

The SIFS is used to provide an efficient MSDU delivery mechanism. Once the STA has contended for the channel, that STA shall continue to send fragments until either all fragments of a single MSDU or MMPDU have been sent, an acknowledgment is not received, or the STA is restricted from sending any additional fragments due to a dwell time boundary. Should the sending of the fragments be interrupted due to one of these reasons, when the next opportunity for transmission occurs the STA shall resume transmission. The algorithm by which the STA decides which of the outstanding MSDUs shall next be attempted after an unsuccessful transmission attempt is beyond the scope of this standard, but any such algorithm shall comply with the restrictions listed in 9.8.

Figure 54 illustrates the transmission of a multiple-fragment MSDU using the SIFS.



**Figure 54—Transmission of a multiple-fragment MSDU using SIFS**

When the source STA transmits a fragment, it shall release the channel, then immediately monitor the channel for an acknowledgment as described in 9.2.8.

When the destination STA has finished sending the acknowledgment, the SIFS following the acknowledgment shall be reserved for the source STA to continue (if necessary) with another fragment. The STA sending the acknowledgment shall not transmit on the channel immediately following the acknowledgment.

The process of sending multiple fragments after contending for the channel is defined as a fragment burst.

If the source STA receives an acknowledgment but there is not enough time to transmit the next fragment and receive an acknowledgment due to an impending dwell boundary, it shall contend for the channel at the beginning of the next dwell time.

If the source STA does not receive an acknowledgment frame, it shall attempt to retransmit the failed MPDU or another eligible MPDU, as defined in 9.8, after performing the backoff procedure and the contention process.

After a STA contends for the channel to retransmit a fragment of an MSDU, it shall start with the last fragment that was not acknowledged. The destination STA shall receive the fragments in order (since the source sends them in order, and they are individually acknowledged). It is possible, however, that the destination STA may receive duplicate fragments. It shall be the responsibility of the receiving STA to detect and discard duplicate fragments.

A STA shall transmit after the SIFS only under the following conditions during a fragment burst:

- The STA has just received a fragment that requires acknowledging.

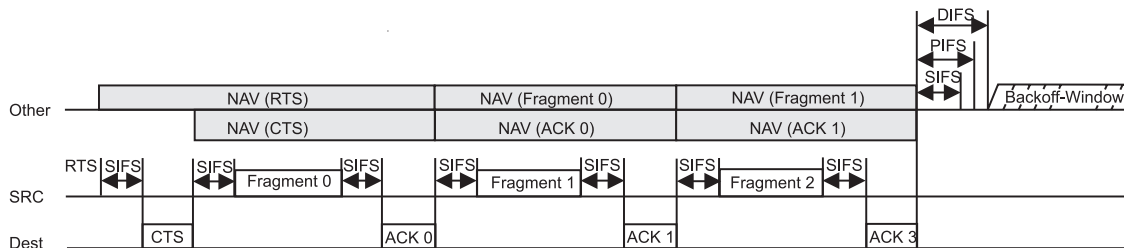
- The source STA has received an acknowledgment to a previous fragment, has more fragment(s) for the same MSDU to transmit, and there is enough time before the next dwell boundary to send the next fragment and receive its acknowledgment.

The following rules shall also apply:

- When a STA has transmitted a frame other than an initial or intermediate fragment, that STA shall not transmit on the channel following the acknowledgment for that frame, without performing the backoff procedure.
- When an MSDU has been successfully delivered or all retransmission attempts have been exhausted, and the STA has a subsequent MSDU to transmit, then the STA shall perform a backoff procedure.
- Only unacknowledged fragments shall be retransmitted.

### 9.2.5.6 RTS/CTS usage with fragmentation

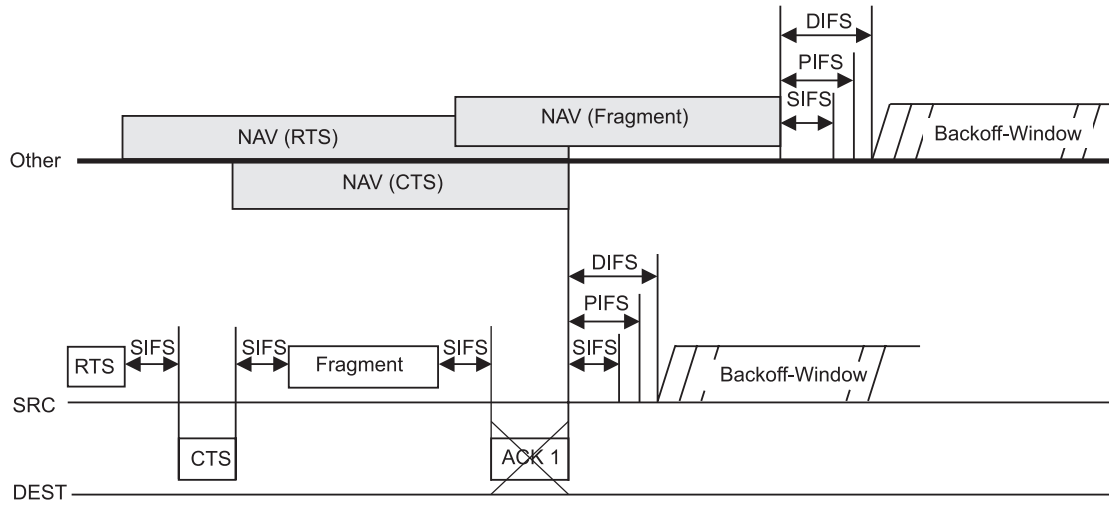
The following is a description of using RTS/CTS for a fragmented MSDU or MMPDU. The RTS/CTS frames define the duration of the following frame and acknowledgment. The Duration/ID field in the data and acknowledgment (ACK) frames specifies the total duration of the next fragment and acknowledgment. This is illustrated in Figure 55.



**Figure 55—RTS/CTS with fragmented MSDU**

Each frame contains information that defines the duration of the next transmission. The duration information from RTS frames shall be used to update the NAV to indicate busy until the end of ACK 0. The duration information from the CTS frame shall also be used to update the NAV to indicate busy until the end of ACK 0. Both Fragment 0 and ACK 0 shall contain duration information to update the NAV to indicate busy until the end of ACK 1. This shall be done by using the Duration/ID field in the Data and ACK frames. This shall continue until the last fragment, which shall have a duration of one ACK time plus one SIFS time, and its ACK, which shall have its Duration/ID field set to zero. Each fragment and ACK acts as a virtual RTS and CTS; therefore no further RTS/CTS frames need to be generated after the RTS/CTS that began the frame exchange sequence even though subsequent fragments may be larger than  $aRTSThreshold$ . At STAs using a frequency-hopping PHY, when there is insufficient time before the next dwell boundary to transmit the subsequent fragment, the STA initiating the frame exchange sequence may set the Duration/ID field in the last data or management frame to be transmitted before the dwell boundary to the duration of one ACK time plus one SIFS time.

In the case where an acknowledgment is sent but not received by the source STA, STAs that heard the fragment, or ACK, will mark the channel busy for the next frame exchange due to the NAV having been updated from these frames. This is the worst-case situation, and it is shown in Figure 56. If an acknowledgment is not sent by the destination STA, STAs that can only hear the destination STA will not update their NAV and may attempt to access the channel when their NAV updated from the previously received frame reaches zero. All STAs that hear the source will be free to access the channel after their NAV updated from the transmitted fragment has expired.



**Figure 56—RTS/CTS with transmitter priority and missed acknowledgment**

### 9.2.5.7 CTS procedure

A STA that is addressed by an RTS frame shall transmit a CTS frame after a SIFS period if the NAV at the STA receiving the RTS frame indicates that the medium is idle. If the NAV at the STA receiving the RTS frame indicates the medium is not idle, that STA shall not respond to the RTS frame. The RA field of the CTS frame shall be the value obtained from the TA field of the RTS frame to which this CTS frame is a response. The Duration/ID field in the CTS frame shall be the duration field from the received RTS frame, adjusted by subtraction of aSIFSTime and the number of microseconds required to transmit a CTS frame at the data rate used for the RTS frame to which this CTS frame is a response.

After transmitting an RTS frame, the STA shall wait for a CTSTimeout interval, starting at the PHY-TXEND.confirm. If a PHY-RXSTART.indication does not occur during the CTSTimeout interval, the STA shall conclude that the transmission of the RTS has failed, and this STA shall invoke its backoff procedure upon expiration of the CTSTimeout interval. If a PHY-RXSTART.indication does occur during the CTSTimeout interval, the STA shall wait for the corresponding PHY-RXEND.indication to determine whether the RTS transmission was successful. The recognition of a valid CTS frame sent by the recipient of the RTS frame, corresponding to this PHY-RXEND.indication, shall be interpreted as successful response, permitting the frame sequence to continue (see 9.7). The recognition of anything else, including any other valid frame, shall be interpreted as failure of the RTS transmission. In this instance, the STA shall invoke its backoff procedure at the PHY-RXEND.indication and may process the received frame.

### 9.2.6 Directed MPDU transfer procedure

A STA shall use an RTS/CTS exchange for directed frames only when the length of the MPDU is greater than the length threshold indicated by the aRTSThreshold attribute.

The aRTSThreshold attribute shall be a managed object within the MAC MIB, and its value may be set and retrieved by the MAC LME. The value 0 shall be used to indicate that all MPDUs shall be delivered with the use of RTS/CTS. Values of aRTSThreshold larger than the maximum MSDU length shall indicate that all MPDUs shall be delivered without RTS/CTS exchanges.

When an RTS/CTS exchange is used, the asynchronous data frame shall be transmitted after the end of the CTS frame and a SIFS period. No regard shall be given to the busy or idle status of the medium when transmitting this data frame.

When an RTS/CTS exchange is not used, the asynchronous data frame shall be transmitted following the success of the basic access procedure. With or without the use of the RTS/CTS exchange procedure, the STA that is the destination of an asynchronous data frame shall follow the ACK procedure.

### **9.2.7 Broadcast and multicast MPDU transfer procedure**

In the absence of a PCF, when broadcast or multicast MPDUs are transferred from a STA with the ToDS bit clear, only the basic access procedure shall be used. Regardless of the length of the frame, no RTS/CTS exchange shall be used. In addition, no ACK shall be transmitted by any of the recipients of the frame. Any broadcast or multicast MPDUs transferred from a STA with a ToDS bit set shall, in addition to conforming to the basic access procedure of CSMA/CA, obey the rules for RTS/CTS exchange, because the MPDU is directed to the AP. The broadcast/multicast message shall be distributed into the BSS. The STA originating the message shall receive the message as a broadcast/multicast message. Therefore, all STAs shall filter out broadcast/multicast messages that contain their address as the source address. Broadcast and multicast MSDUs shall be propagated throughout the ESS.

There is no MAC-level recovery on broadcast or multicast frames, except for those frames sent with the ToDS bit set. As a result, the reliability of this traffic is reduced, relative to the reliability of directed traffic, due to the increased probability of lost frames from interference or collisions or time-varying channel properties.

### **9.2.8 ACK procedure**

An ACK frame shall be generated as shown in the frame exchange sequences listed in 9.7.

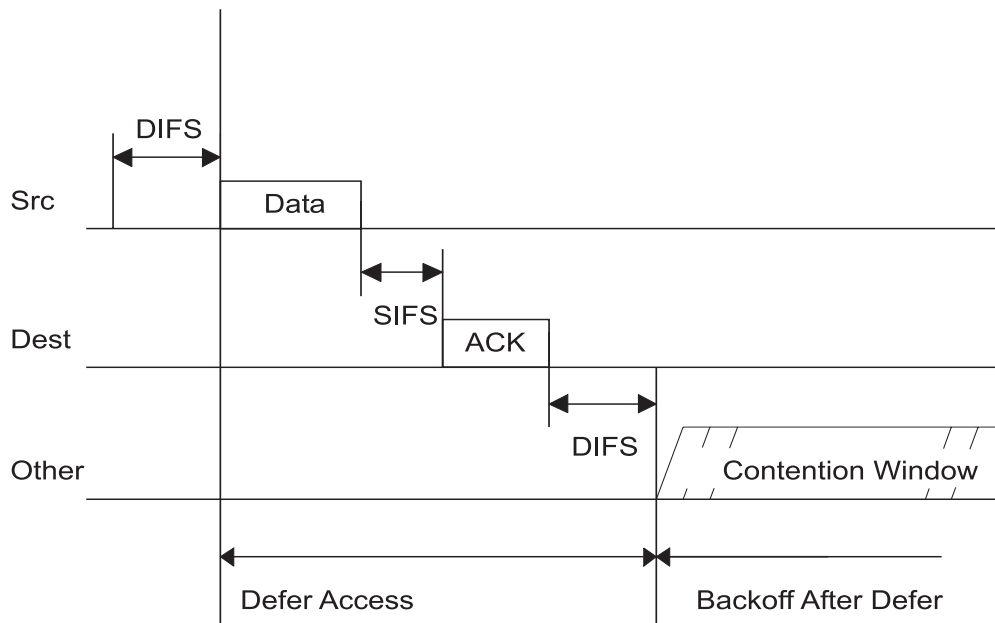
Upon successful reception of a frame of a type that requires acknowledgment with the ToDS bit set, an AP shall generate an ACK frame. An ACK frame shall be transmitted by the destination STA that is not an AP, whenever it successfully receives a unicast frame of a type that requires acknowledgment, but not if it receives a broadcast or multicast frame of such type. After a successful reception of a frame requiring acknowledgment, transmission of the ACK frame shall commence after a SIFS period, without regard to the busy/idle state of the medium.

The source STA shall wait ACKTimeout amount of time without receiving an ACK frame before concluding that the MPDU failed. (See Figure 57.)

After transmitting an MPDU that requires an ACK frame as a response (see 9.7), the STA shall wait for an ACK-Timeout interval, starting at the PHY-TXEND.confirm. If a PHY-RXSTART.indication does not occur during the ACKTimeout interval, the STA concludes that the transmission of the MPDU has failed, and this STA shall invoke its backoff procedure upon expiration of the ACKTimeout interval. If a PHY-RXSTART.indication does occur during the ACKTimeout interval, the STA shall wait for the corresponding PHY-RXEND.indication to determine whether the MPDU transmission was successful. The recognition of a valid ACK frame sent by the recipient of the MPDU requiring acknowledgment, corresponding to this PHY-RXEND.indication, shall be interpreted as successful acknowledgment, permitting the frame sequence to continue, or to end without retries, as appropriate for the particular frame sequence in progress. The recognition of anything else, including any other valid frame, shall be interpreted as failure of the MPDU transmission. In this instance, the STA shall invoke its backoff procedure at the PHY-RXEND.indication and may process the received frame. The sole exception is that recognition of a valid data frame sent by the recipient of a PS-Poll frame shall also be accepted as successful acknowledgment of the PS-Poll frame.

### **9.2.9 Duplicate detection and recovery**

Since MAC-level acknowledgments and retransmissions are incorporated into the protocol, there is the possibility that a frame may be received more than once. Such duplicate frames shall be filtered out within the destination MAC.



**Figure 57—Directed data/ACK MPDU**

Duplicate frame filtering is facilitated through the inclusion of a Sequence Control field (consisting of a sequence number and fragment number) within data and management frames. MPDUs that are part of the same MSDU shall have the same sequence number, and different MSDUs shall (with a high probability) have a different sequence number.

The sequence number is generated by the transmitting STA as an incrementing sequence of integers.

The receiving STA shall keep a cache of recently received <Address 2, sequence-number, fragment-number> tuples. A receiving STA is required to keep only the most recent cache entry per Address 2–sequence-number pair, storing only the most recently received fragment number for that pair. A receiving STA may omit tuples obtained from broadcast/multicast or ATIM frames from the cache.

A destination STA shall reject as a duplicate frame any frame that has the Retry bit set in the Frame Control field and that matches an <Address 2, sequence-number, and fragment-number> tuple of an entry in the cache.

There is a small possibility that a frame may be improperly rejected due to such a match; however, this occurrence would be rare and simply results in a lost frame (similar to an FCS error in other LAN protocols).

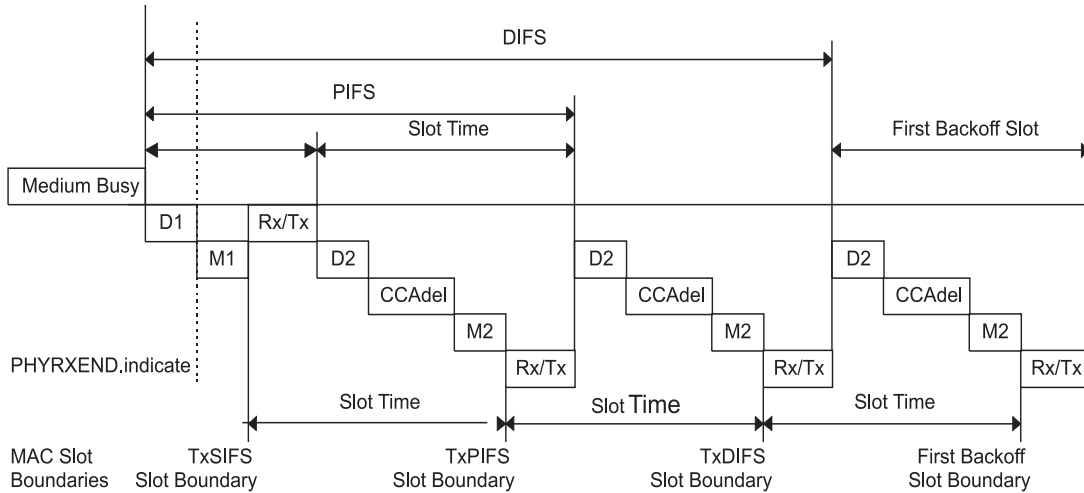
The destination STA shall perform the ACK procedure on all successfully received frames requiring acknowledgment, even if the frame is discarded due to duplicate filtering.

### 9.2.10 DCF timing relations

The relationships between the IFS specifications are defined as time gaps on the medium. The associated MIB attributes are provided by the specific PHY. (See Figure 58.)

All timings that are referenced from the end of the transmission are referenced from the end of the last symbol of a frame on the medium. The beginning of transmission refers to the first symbol of the next frame on the medium.





$D1 = aRxRFDelay + aRxPLCPDelay$  (referenced from the end of the last symbol of a frame on the medium)  
 $D2 = D1 + \text{Air Propagation Time}$   
 $Rx/Tx = aRXTXTurnaroundTime$  (begins with a PHYTXSTART.request)  
 $M1 = M2 = aMACPrcDelay$   
 $CCAdel = aCCA\ Time - D1$

**Figure 58—DCF timing relationships**

$aSIFSTime$  and  $aSlotTime$  are defined in the MIB, and are fixed per PHY.

$aSIFSTime$  is:  $aRxRFDelay + aRxPLCPDelay + aMACPrcDelay + aRxTxTurnaroundTime$ .

$aSlotTime$  is:  $aCCATime + aRxTxTurnaroundTime + aAirPropagationTime + aMACProcessingDelay$ .

The PIFS and DIFS are derived by the following equations, as illustrated in Figure 58.

$$PIFS = aSIFSTime + aSlotTime$$

$$DIFS = aSIFSTime + 2 \times aSlotTime$$

The EIFS is derived from the SIFS and the DIFS and the length of time it takes to transmit an ACK Control frame at 1 Mbit/s by the following equation:

$$EIFS = aSIFSTime + (8 \times ACKSize) + aPreambleLength + aPLCPHeaderLngth + DIFS$$

where

$ACKSize$  is the length, in bytes, of an ACK frame; and

$(8 \times ACKSize) + aPreambleLength + aPLCPHeaderLngth$  is expressed in microseconds required to transmit at the PHY's lowest mandatory rate.

Figure 58 illustrates the relation between the SIFS, PIFS, and DIFS as they are measured on the medium and the different MAC slot boundaries TxSIFS, TxPIFS, and TxDIFS. These slot boundaries define when the transmitter shall be turned on by the MAC to meet the different IFS timings on the medium, after subsequent detection of the CCA result of the previous slot time.