# WIRELESS COMMUNICATIONS

Second Edition

**Andreas F. Molisch,** *Fellow, IEEE*
*University of Southern California, USA*

IEEE

WILEY

A John Wiley and Sons, Ltd., Publication



SAMSUNG 1048

This edition first published 2011
© 2011 John Wiley & Sons Ltd.

First edition published 2005

*Registered office*
John Wiley & Sons Ltd, The Atrium, Southern Gate, Chichester, West Sussex, PO19 8SQ, United Kingdom

For details of our global editorial offices, for customer services and for information about how to apply for permission to reuse the copyright material in this book please see our website at *www.wiley.com*.

The right of the author to be identified as the author of this work has been asserted in accordance with the Copyright, Designs and Patents Act 1988.

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, except as permitted by the UK Copyright, Designs and Patents Act 1988, without the prior permission of the publisher.

Wiley also publishes its books in a variety of electronic formats. Some content that appears in print may not be available in electronic books.

Designations used by companies to distinguish their products are often claimed as trademarks. All brand names and product names used in this book are trade names, service marks, trademarks or registered trademarks of their respective owners. The publisher is not associated with any product or vendor mentioned in this book. This publication is designed to provide accurate and authoritative information in regard to the subject matter covered. It is sold on the understanding that the publisher is not engaged in rendering professional services. If professional advice or other expert assistance is required, the services of a competent professional should be sought.

***Library of Congress Cataloguing-in-Publication Data***

Molisch, Andreas F.
Wireless communications / Andreas F. Molisch. – 2nd ed.
p. cm.
Includes bibliographical references and index.
ISBN 978-0-470-74187-0 (cloth) – ISBN 978-0-470-74186-3 (pbk.)
1. Wireless communication systems–Textbooks. I. Title.
TK5103.2.M65 2011
621.3845'6–dc22
2010017177

A catalogue record for this book is available from the British Library.

Print ISBN: 9780470741870 (H/B)
Print ISBN: 9780470741863 (P/B)
ePDF ISBN: 9780470666692

Typeset in 9/11 Times by Laserwords Private Limited, Chennai, India.

# 29

# Wireless Local Area Networks

## 29.1 Introduction

### *29.1.1 History*

In the late 1990s, wired fast Internet connections became widespread both in office buildings and in private residences. For companies, a fast intranet as well as fast connections to the Internet became a necessity. Furthermore, private consumers became frustrated with the long download times of dialup connections for elaborate webpages, music, etc., as connection speeds were limited to 56 kbit/s. They therefore opted for cable connections (several Mbit/s) or Digital Subscriber Lines (DSLs) (up to 1 Mbit/s in the U.S.A., and more than 20 Mbit/s in Japan) for their computer connections. At the same time, laptop computers started to be widely used in the workplace. This combination of factors spurred demand for wireless data connections – from the laptop to the nearest wired Ethernet port – that could match the speed of wired connections.

In the following years, two rival standards were developed. The ETSI (European Telecommunications Standards Institute) started to develop the HIPERLAN (*HIgh PERformance Local Area Network*) standard, while the IEEE (*Institute of Electrical and Electronics Engineers*) established the 802.11 group – the number 802 refers to all standards of the IEEE dealing with local and metropolitan area networks, and the suffix 11 was assigned for Wireless Local Area Networks (WLANs). In subsequent years, the 802.11 standard gained widespread acceptance, while HIPERLAN became essentially extinct.

Actually, it is not correct to speak of *the* 802.11 standard. 802.11 encompasses a number of different standards (see Table 29.1), which are not all interoperable. To understand the terminology, we first have to summarize the history of the standard. The "original" 802.11 standard was intended to provide data rates of 1 and 2 Mbit/s; since it operated in the 2.45-GHz ISM (*Industrial, Scientific, and Medical*) band, the frequency regulator in the U.S.A. – the Federal Communications Commission (FCC) – required that spectrum-spreading techniques be used. For this reason, the original 802.11 standard defined two modes: (i) frequency hopping, and (ii) direct-sequence spreading; these two modes were incompatible with each other.

It soon became obvious that higher data rates were demanded by users. Two subgroups were formed: 802.11a, which investigated Orthogonal Frequency Division Multiplexing (OFDM)-based schemes, and 802.11b, which attempted to retain the direct-sequence approach. 802.11b became popular first; it defined a standard that allowed an 11-Mbit/s data rate in a 20-MHz channel. Though the scheme was no longer really spread spectrum, the FCC approved its use. The standard was later adopted by an industry group called WiFi (Wireless Fidelity), which was formed to ensure true

*Wireless Communications, Second Edition* Andreas F. Molisch
© 2011 John Wiley & Sons Ltd. ISBN: 978-0-470-74187-0

**Table 29.1** The IEEE 802.11 standards and their main focus

| Standards | Scope |
|---|---|
| 802.11 (original) | Define a WLAN standard that includes both MAC and PHY functions |
| 802.11a | Define a high-speed (up to 54 Mbps) PHY supplement in the 5-GHz band |
| 802.11b | Define a high-speed (up to 11 Mbps) PHY extension in the 2.4-GHz band |
| 802.11d | Operation in additional regulatory domains |
| 802.11e | Enhance the original 802.11 MAC to support QoS (applies to 802.11a/b/g) |
| 802.11f | Define a recommended practice for interaccess point protocol (applies to 802.11a/b/g) |
| 802.11g | Define a higher rate (up to 54 Mbps) PHY extension in the 2.4-GHz band |
| 802.11h | Define MAC functions that allow 802.11a products to meet European regulatory requirements |
| 802.11i | Enhance 802.11 MAC to provide improvement in security (applies to 802.11a/b/g) |
| 802.11j | Enhance the current 802.11 MAC and 802.11a PHY to operate in Japanese 4.9-GHz and 5-GHz bands |
| 802.11n | Enhance the 802.11a and 802.11 PHY to operate at data rates up to 600 Mbit/s |
| 802.11p | Modify the 802.11a standard for car-to-car communications |
| 802.11s | Provide a protocol for autoconfiguring mesh networks |
| 802.11w | Provide data integrity and authentication |

interoperability between all WiFi-certified products.[1] WiFi gained widespread market acceptance after 2000. The data rate of 11 Mbit/s still was not sufficient for many applications – especially in light of the fact that actual throughput in practical situations is closer to 3–5 Mbit/s. For this reason, the work of the 802.11a group became of greater interest. 802.11a specified an alternative PHYsical layer (PHY) that uses OFDM and higher order modulation alphabets, allowing up to 54-Mbit/s data transfer rate (again, this rate is nominal, and true throughput is lower by about a factor of 2). This mode also works in a different frequency band (above 5 GHz), which is less "crowded" – i.e., has to deal with fewer interferers. The 802.11g group uses the same modulation format in the 2.45-GHz ISM band, and has by now become the most popular standard. Further modifications of the 802.11a standard are provided by the 802.11h and 802.11j standards, which adapt it to European and Japanese regulations, respectively. The 802.11n standard, which provides higher throughput by using Multiple Input Multiple Output system (MIMO) as well as possibly using larger bandwidth, was approved in 2009.

In addition, the original MAC (Medium Access Control) has been amended: the 802.11e standard provides modifications to the MAC that allow us to better ensure certain levels for *Quality of Service* (QoS). Additionally, a number of further subgroups of the 802.11 standardization group have been formed, all dealing with "amendments" and "additions" to the original standard. Realistically speaking, though, an 802.11a device, using the 802.11e MAC, bears no resemblance to the original 802.11 standard.

[1] Not all 802.11b products are completely interoperable.

Due to the multitude of 802.11 standards, we only present the most important. In the following, we give an overview of 802.11a as well as 802.11n PHYs, and the 802.11 MAC layer. More details can be found, as always, in the official standards publications [*www.802wirelessworld.com*] and the multitude of books that have been published on that topic. An excellent summary of the earlier versions of the standard can be found in O'Hara and Petrick [2005], and of the 802.11n standard in Perahia and Stacey [2008].

### *29.1.2 Applications*

The main markets for WLANs are as follows:

- Wireless networks in office buildings and private homes, to allow unhindered Internet access from anywhere within a building. Access points (equivalent to base stations in cellular systems) for WLANs need to follow the specifications, but also allow a certain amount of vendor leeway. For example, multiple antennas can be used at the access point, without leading to incompatibilities. As far as "clients" (equivalent to mobile stations in cellular systems) are concerned, WLAN cards have turned into a mass market with very little distinction between products from different vendors, and are often built into laptops. As a consequence, research tends to focus on methods for production cost reduction (implementation with smaller chip area, low-cost semiconductor technology), while research on access points includes a broader field of topics.
- "Hotspots" – i.e., wireless access points that allow the public to connect to the Internet. These hotspots are often set up in coffee shops, hotels, airports, etc. Several providers also have a "nationwide" or even "continentwide" network of hotspots, so that subscribers can log in at many different locations.[2] However, it must be stressed that coverage from these networks is *much* lower than for cellular networks. For this reason, research is ongoing on how to seamlessly integrate WLANs with cellular networks or large-area networks.

### *29.1.3 Relationship between the Medium Access Control Layer and the PHY*

Before going into details of the MAC and the PHY, we first have to establish some notation used by the 802.11 community. The data payload received from upper layers is attached to headers and trailers at both the MAC and PHY before it gets transmitted on the air. For example, each *MAC Service Data Unit* (MSDU) received from the *Logic Link Control* (LLC) layer is appended with a 30-byte-long MAC header and a 4-byte-long *Frame Check Sequence* (FCS) trailer to form the *MAC Protocol Data Unit* (MPDU). The same MPDU, once handed over to the PHY, is then called the *Physical Layer Service Data Unit* (PSDU). And, then a *Physical Layer Convergence Procedure* (PLCP) preamble and header, and proper tail bits and pad bits are attached to the PSDU to finally generate the *Physical Layer Protocol Data Unit* (PPDU) for transmission. The relationships among MSDU, MPDU, PSDU, and PPDU are illustrated in Figure 29.1.

From just this brief paragraph, the reader will have seen that – as with most standards – the alphabet soup of the numerous acronyms is a major hurdle to understanding this standard. For this reason, there is a list of acronyms and their meaning in the frontmatter of this book (see p. xxxi) and a separate list of abbreviations for some chapters in the appendices.

[2] In most cases, users are charged a per-minute fee or a flat rate for 24 hours of usage. Nationwide networks often have an option for monthly or annual subscriptions.

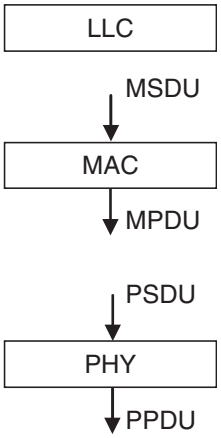


**Figure 29.1** Relations among the MAC service data unit, MAC protocol data unit, physical layer service data unit, and physical layer protocol data unit.
Reproduced with permission from IEEE 802.11 © IEEE.

## 29.2 802.11a/g – Orthogonal Frequency Division Multiplexing-Based Local Area Networks

In an attempt to attain higher data rates, the 802.11 Working Group (WG) published their 802.11a standard defining a PHY for high-speed data communications based on OFDM in 1999. The standard is defined for the 5-GHz band, where more bandwidth is available, and less interference is present. However, the achievable range is not as good as in the 2.45-GHz band. Therefore, the same PHY, but working in the 2.45-GHz band, was introduced as 802.11g standard. It is currently the dominant version of WLAN standards. Its main properties are the following (see also Table 29.2):

- use of the 5.15–5.825 GHz band (in the U.S.A.) for 11a and 2.4-2.27 GHz for the 11g standard;
- 20-MHz channel spacing;
- data rates include 6, 9, 12, 18, 24, 36, 48, and 54 Mbps, where support of 6, 12, and 24 Mbps is mandatory;
- OFDM with 64 subcarriers, out of which 52 are user modulated with Binary or Quadrature-Phase Shift Keying (BPSK/QPSK), 16-Quadrature Amplitude Modulation (16-QAM), or 64-QAM;
- forward error correction, using convolutional coding with coding rates of 1/2, 2/3, or 3/4 as Forward Error Correction (FEC) coding.

**Table 29.2** Important parameters of the 802.11a PHY layer

| | |
|---|---|
| Information data rate | 6, 9, 12, 18, 24, 36, 48, 54 Mbit/s |
| Modulation | BPSK, OPSK, 16-QAM, 64-QAM |
| FEC | $K = 7$ convolutional code |
| Coding rate | 1/2, 2/3, 3/4 |
| Number of subcarriers | 52 |
| OFDM symbol duration | 4 μs |
| Guard interval | 0.8 μs |
| Occupied bandwidth | 16.6 MHz |

### 29.2.1 Frequency Bands

In the U.S.A., the frequency bands 5.15–5.25, 5.25–5.35, and 5.725–5.825 GHz, called the *Unlicensed National Information Infrastructure* (U-NII) bands, are used for 802.11a. These channels are numbered, starting every 5 MHz, according to the formula:

$$\text{Channel center frequency} = 5{,}000 + 5 \times n_{\text{ch}}(MHz) \tag{29.1}$$

where $n_{\text{ch}} = 0, 1, \ldots, 200$. The transmit powers in the 5.15–5.25, 5.25–5.35, and 5.725–5.825–GHz bands are limited to 40, 200, and 800 mW, respectively.

Obviously, each 20-MHz channel used by 802.11a occupies four channels in the U-NII band. Recommended channel usage in the U.S.A. is given in Table 29.3. In Japan, the assigned carrier frequencies are slightly lower.

The band plan for 802.11a in the U.S.A. is also given in Figure 29.2.

**Table 29.3** Frequency assignment for 802.11a in the U.S.A

| Bands (GHz) | Allowed power | Channel numbers ($n_{ch}$) | Channel center frequency (MHz) |
|---|---|---|---|
| U-NII lower band | 40 mW | 36 | 5,180 |
| (5.15–5.25) | (2.5 mW/MHz) | 40 | 5,200 |
| | | 44 | 5,220 |
| | | 48 | 5,240 |
| U-NII middle band | 200 mW | 52 | 5,260 |
| (5.25–5.35) | (12.5 mW/MHz) | 56 | 5,280 |
| | | 60 | 5,300 |
| | | 64 | 5,320 |
| U-NII upper band | 800 mW | 149 | 5,745 |
| (5.725–5.825) | (50 mW/MHz) | 153 | 5,765 |
| | | 157 | 5,785 |
| | | 161 | 5,805 |

### 29.2.2 Modulation and Coding

802.11a uses OFDM as its modulation format, enabling high data rates. The principles of OFDM were described in Chapter 19, so here we simply analyze details specific to 802.11a. A typical block diagram of a transceiver is shown in Figure 29.3.

In 802.11a, OFDM with 64 subcarriers is specified. Powers of 2 are habitually used as numbers for OFDM subcarriers, as they allow the most efficient implementation via Fast Fourier Transforms (FFTs). However, only 52 of the 64 subcarriers are actually used (modulated and transmitted), while the other 12 subcarriers are null-carriers that do not carry any useful information; useful carriers are indexed from −26 to 26, without a Direct Current (DC) component. Of these 52 subcarriers, 4 are used as pilots – namely, subcarriers number −21, −7, 7, 21. The pilot should be BPSK-modulated by a pseudorandom sequence to prevent generation of spectral lines.

The other 48 subcarriers carry the PSDU data. BPSK, QPSK, 16-QAM, or 64-QAM are all admissible modulation alphabets, depending on the channel state. Note, however, that the standard does *not* foresee truly adaptive modulation in the sense that the modulation alphabet can differ from subcarrier to subcarrier. Rather, the system uses an average "transmission quality" criterion

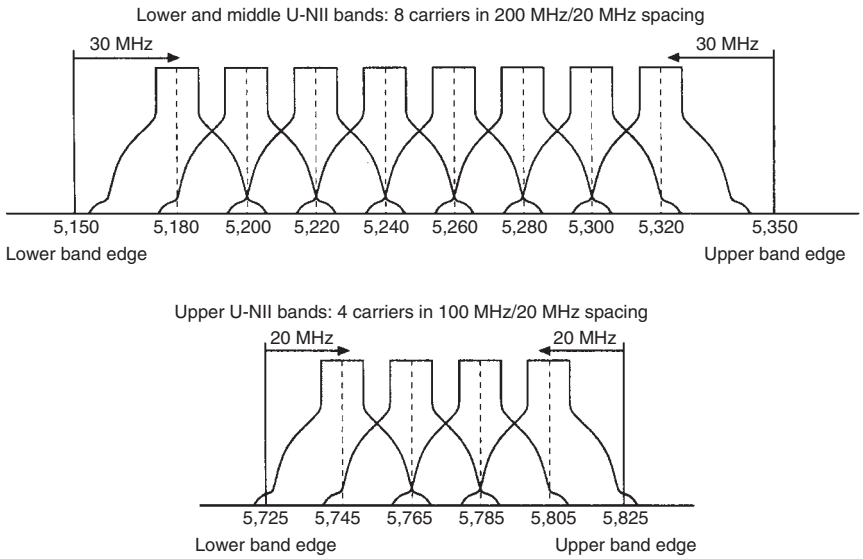


**Figure 29.2** 802.11a channel plan.

Reproduced with permission from IEEE 802.11 © IEEE.

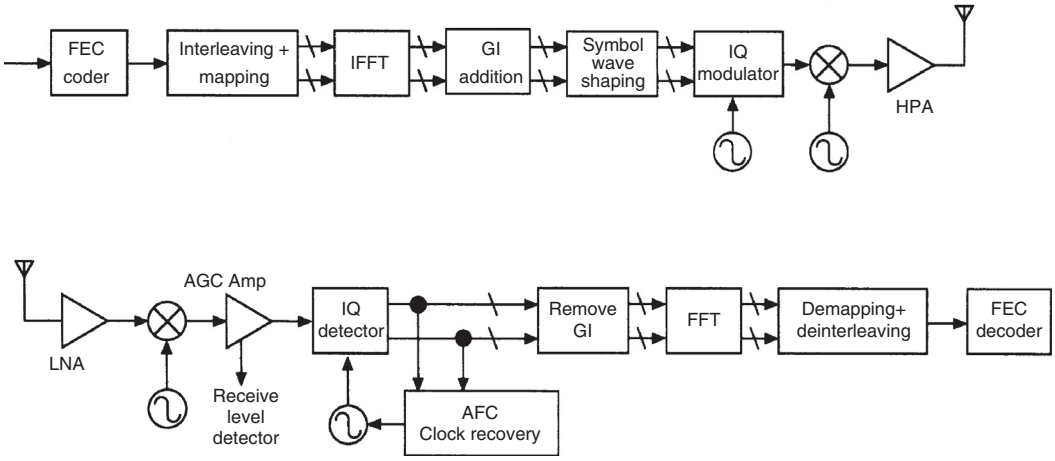


**Figure 29.3** Block diagram of a 802.11a transceiver.

Reproduced with permission from IEEE 802.11 © IEEE. HPA, High Power Amplifier; LNA, Low Noise Amplifier.

to adapt the data rate to the current channel state. Rate adaptation is achieved by modifying either the modulation alphabet or the rate of the error correction code (see below), or both.

The duration of an OFDM symbol is 4 μs, including a cyclic prefix of 0.8 μs. This is sufficient to accommodate the maximum excess delay of most indoor propagation channels, including factory halls and other challenging environments.

For FEC, 802.11a uses a convolutional encoder with coding rates 1/2, 2/3, or 3/4, depending on the desired data rate. The generator vectors are G1 = 133 and G2 = 171 (in octal notation), for the rate-1/2 coder shown in Figure 29.4. Higher rates are derived from this "mother code" by puncturing.

All encoded data bits are interleaved by a block interleaver with a blocksize equal to the number of bits in a single OFDM symbol. The interleaver works in two steps (permutations). The first permutation ensures that adjacent coded bits are mapped onto nonadjacent subcarriers.

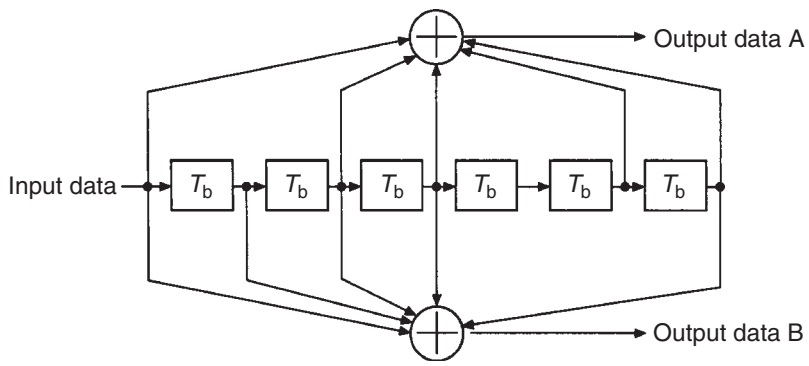


**Figure 29.4** Convolutional encoder (K = 7).
Reproduced with permission from IEEE 802.11 © IEEE.

The second ensures that adjacent coded bits are mapped alternately onto both less and more significant bits of the constellation and, thereby, long runs of low-reliability bits are avoided.

Table 29.4 summarizes the rates that can be achieved with different combinations of alphabets and coding rates, as well as the OFDM modulation parameters.

**Table 29.4** Data rates in 802.11a

| Data rate (Mbit/s) | Modulation | Coding rate | Coded bits per subcarrier | Coded bits per OFDM symbol | Data bits per OFDM symbol |
|---|---|---|---|---|---|
| 6 | BPSK | 1/2 | 1 | 48 | 24 |
| 9 | BPSK | 3/4 | 1 | 48 | 36 |
| 12 | QPSK | 1/2 | 2 | 96 | 48 |
| 18 | QPSK | 3/4 | 2 | 96 | 72 |
| 24 | 16-QAM | 1/2 | 4 | 192 | 96 |
| 36 | 16-QAM | 3/4 | 4 | 192 | 144 |
| 48 | 64-QAM | 2/3 | 6 | 288 | 192 |
| 54 | 64-QAM | 3/4 | 6 | 288 | 216 |

## *29.2.3 Headers*

For transmission, a preamble and a PLCP header are prepended to the encoded PSDU data[3] that are received from the MAC layer, creating a PPDU. At the receiver (RX), the PLCP preamble and header are used to aid demodulation and data delivery. A PPDU frame format is shown in Figure 29.5.

The PLCP header is transmitted in the SIGNAL field of the PPDU. It incorporates the RATE field, a LENGTH field, a TAIL field, and so on:

- *RATE (4 bits)*: indicates transmission data rate.
- *LENGTH (12 bits)*: indicates the number of octets in the PSDU.
- *Parity (1 bit)*: parity check.
- *Reserved (1 bit)*: future use.

[3] Plus pilot tones.

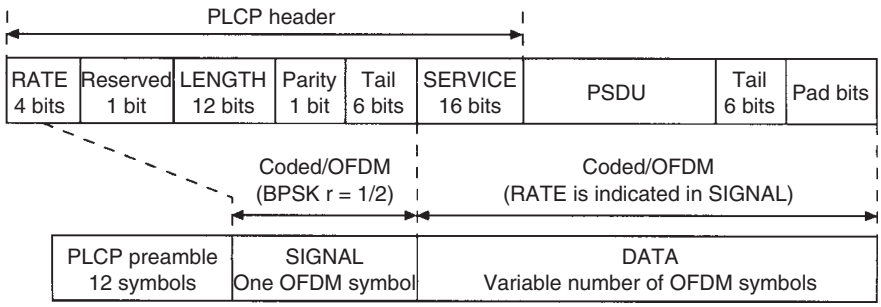


**Figure 29.5** PHY-protocol-data-unit frame format.
Reproduced with permission from IEEE 802.11 © IEEE.

- *TAIL (6 bits)*: convolutional-coding tail.
- *SERVICE (16 bits)*: initialization of the scrambler.

## 29.2.4 Synchronization and Channel Estimation

Synchronization is achieved by means of the PLCP preamble field. It consists of 10 short symbols and 2 long symbols (Figure 29.6).

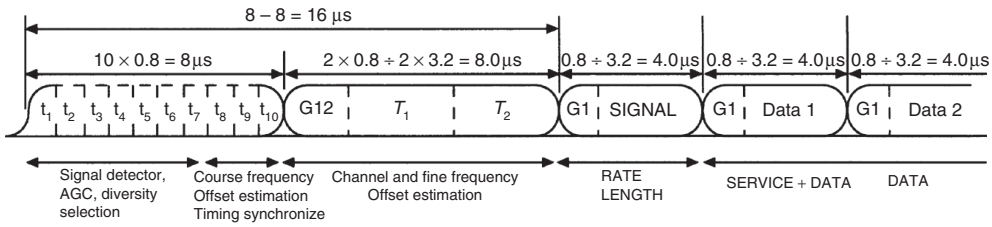


**Figure 29.6** Orthogonal frequency division multiplexing training structure.
Reproduced with permission from IEEE 802.11 © IEEE.

The training sequence starts out with 10 short symbols of duration 0.8 µs that allow the RX to detect the signal, adjust the Automatic Gain Control (AGC), and perform a coarse-frequency offset estimation. These short symbols consist of just 12 subcarriers, which are modulated by elements of the following sequence:

$$\begin{aligned} S_{-26,26} = \sqrt{(13/6)}\{&0, 0, 1+j, 0, 0, 0, -1-j, 0, 0, 0, 1+j, 0, 0, 0, -1-j, 0, 0, 0, \\ &-1-j, 0, 0, 0, 1+j, 0, 0, 0, 0, 0, 0, 0, -1-j, 0, 0, 0, -1-j, 0, 0, 0, 1 \\ &+j, 0, 0, 0, 1+j, 0, 0, 0, 1+j, 0, 0, 0, 1+j, 0, 0\} \end{aligned} \tag{29.2}$$

Multiplication by a factor of $\sqrt{(13/6)}$ is done so as to normalize the average power of the resulting OFDM symbol, which utilizes 12 of the 52 subcarriers.

These symbols are followed by 2 long training symbols that serve for both channel estimation and finer frequency offset estimation, preceded by a Guard Interval (GI). A long OFDM training symbol consists of 53 subcarriers (including a 0 value at DC), which are modulated by elements

of sequence $L$, given by

$$L_{-26,26} = \{1, 1, -1, -1, 1, 1, -1, 1, -1, 1, 1, 1, 1, 1, 1, -1, -1, 1, 1, -1, 1, -1, 1, 1, 1, 1, 0, 1, -1, -1, 1, 1, -1, 1, -1, 1, -1, -1, -1, -1, -1, 1, 1, -1, -1, 1, -1, 1, -1, 1, 1, 1, 1\} \tag{29.3}$$

The PLCP preamble is followed by the SIGNAL and DATA fields. The total training length is 16 µs. The dashed boundaries in the figure denote repetitions due to periodicity of the inverse Fourier transform.

Table 29.5 summarizes the most important parameters for 802.11a mode.

**Table 29.5** Parameters of 802.11a

| Parameter | Value |
|---|---|
| Number of data subcarriers | 48 |
| Number of pilot subcarriers | 4 |
| Subcarrier spacing | 0.3125 MHz |
| IFFT/FFT period | 3.2 µs |
| Preamble duration | 16 µs |
| Duration of OFDM symbol | 4.0 µs |
| Guard interval for signal symbol | 0.8 µs |
| Guard interval for training symbol | 1.6 µs |
| Short training sequence duration | 8 µs |
| Long training sequence duration | 8 µs |

## 29.3 IEEE 802.11n

### *29.3.1 Overview*

The 802.11n standard offers up to (nominal) 600 Mbit/s bit rate. These high data rates, as well as improved reliability, are necessitated by a number of new applications: (i) wireless computer networks require higher data transfer rates between various computers at home, and (due to the emergence of fiber-to-the-home) transfer rates from the computer to the wired Internet port at users' homes, (ii) Audio and Video (AV) applications, e.g., transfer of videos from laptops, hard-disk video recorders, and DVD players to TVs, and (iii) Voice over Internet Protocol (VoIP) applications, which require lower data rates, but high reliability.

The 802.11n group was established in 2002. In September 2004, a number of different technical proposals were presented, which were subsequently consolidated into two proposals supported by a major industry alliances each: TGnSync, and WWise. After more than a year of negotiations and fights, a compromise draft proposal was approved by 802.11n in January 2006. Since then, the draft was in the process of revisions and corrections, and a final version of the 11n standard was approved in 2009. But even before then, several companies already sold "pre-n" products that followed the 11n draft standard, and remain compatible with the final standard..

802.11n achieves high data rates mainly by two methods: use of multiple-antenna techniques (see Chapter 20), and increase of the available bandwidth from 20 to 40 MHz. The generic structure of an 11n transceiver is shown in Figure 29.7. The source data stream is first scrambled and then (only for data rates >300 Mbit/s) divided into two parallel data streams, to reduce the processing speed requirements of the encoder/decoder. A number of different codecs are available: binary convolutional codes are the default solution, while Low Density Parity Check

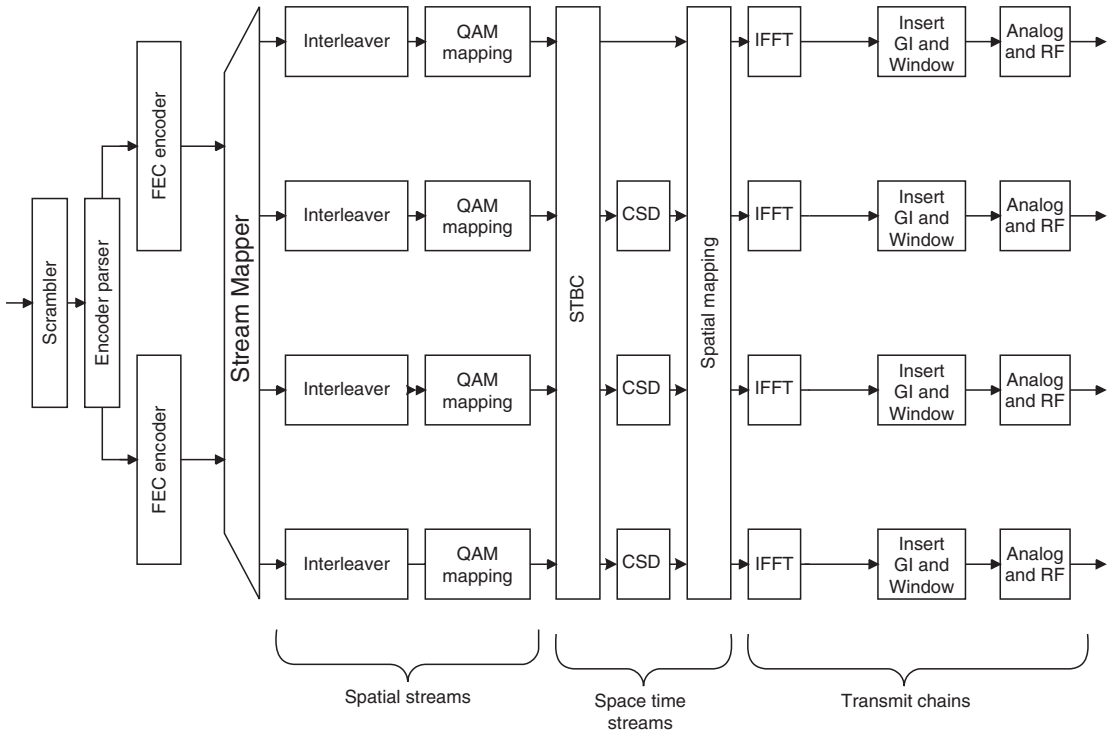


**Figure 29.7** Block diagram of an IEEE 802.11n transmitter.

Reproduced with permission from [IEEE P802.11n] © IEEE.

(LDPC) codes are an option for high-performance transmission (for more details see Section 14.7). The thus-encoded bits are divided into a number of spatial streams (compare Section 20.2), which are to be transmitted in parallel from the antennas. Each of the spatial streams is then interleaved, mapped onto complex modulation symbols, and grouped into OFDM symbols. Next, the spatial streams can be modulated by Alamouti codes and/or cyclic shift diversity (for details see Section 29.4.3). Next, the "spatial mapping" distributes the spatial streams onto the modulation/upconversion chains. In each of the chains, the symbols are submitted to an Inverse Fast Fourier Transformation (IFFT), a guard interval is inserted, and the signal is upconverted to the passband; this part of the processing is identical to 802.11a.

## *29.3.2 Modulation and Coding*

For a single spatial stream, the modulation and coding schemes are very similar to those of 802.11a. The modulation formats are BPSK, QPSK, 16-QAM, and 64-QAM. When convolutional coding is used, code rates 1/2, 2/3, and 3/4 are the same as for 802.11a; an additional code rate of 5/6 (for higher throughput in very good channel conditions) was introduced as well. This results in a total of 8 Modulation and Coding Scheme (MCS) schemes with data rates from 6.5 to 65 Mbit/s. When multiple antennas are present, the transmitter (TX) can either use the same MCS for all spatial streams (this makes sense if the TX has no channel state information), or it can have different MCSs for different streams. A total of 32 MCSs are defined for the case of equal modulation (the 8 "fundamental" MCSs equally used on 1, 2, 3, or 4 spatial streams). For unequal modulation, a further 44 MCSs (different combinations of the existing MCSs on the various spatial streams) are defined, though they are not mandatory.

802.11n also introduces the concept of a short GI: the system can adaptively decide whether the length of the cyclic prefix is the "normal" 800 ns or shortened to 400 ns; the latter is used to

increase the spectral efficiency in environments where the delay spread is so small that a short cyclic prefix is sufficient.

The 802.11n standard also introduces LDPC encoding (compare Section 14.7), which achieves extremely low error probability at the price of higher decoding complexity. The parity-check matrices can be partitioned into square subblocks (submatrices), which are either cyclic permutations of the identity matrix, or all-zero matrices. Twelve different codes are defined, which are all based on the same codestructure. The codeword sizes and submatrix sizes are 648 (27), 1296 (54), and 1944 (81).

## *29.3.3 Multiple-Antenna Techniques*

The key to the 802.11n standard is the use of multiple-antenna techniques. The standard foresees a number of different techniques, in particular (i) spatial multiplexing, (ii) space–time block coding, (iii) eigenbeamforming, and (iv) antenna selection. The basics of most of those techniques are outlined in Section 20.2; here, we only deal with the specific implementation in 802.11n.

### Space–Time Coding

Space–time block codes can be used in an 802.11n system to increase the robustness of the system. In particular, Alamouti codes are used, and can be combined with spatial multiplexing. If there are two transmit Radio Frequency (RF) chains, then one spatial stream is mapped onto those chains (and from there to the antennas) by means of the standard Alamouti code. If there are three transmit antennas and two spatial streams, then one stream is mapped to two RF chains by means of Alamouti encoding, and one stream is mapped directly to the remaining chain. For four transmit chains, either three streams (where one of them is Alamouti encoded), or two streams (with each of them Alamouti encoded) can be used. Different modulation schemes can be used on the different streams; this is motivated by the fact that Alamouti-encoded streams are more robust and can sustain a higher modulation scheme than nonencoded schemes.

Another way of achieving transmit diversity is the use of "Cyclic Shift Diversity" (CSD). This method, which is somewhat similar to delay diversity as described in Chapter 13, introduces a different delay for each signal. In contrast to conventional delay diversity, where signals are linearly delayed, in CSD the OFDM symbols are *cyclically* shifted. In other words, this means that the signal on the $k$-th subcarrier is shifted by $\exp[-j2\pi k\Delta_{\mathrm{F}}\tau_i]$, where $k$ indexes the subcarrier frequency, $\Delta_{\mathrm{F}}$ is the spacing of the subcarriers, and $\tau_i$ is the cyclic shift applied to the $i-$th signal. The cyclic shifts are 0, $-400$, $-200$, and $-600$ ns for the first, second, third, and fourth spatial stream, respectively.

### Spatial Multiplexing and Beamforming

The dividing of the original data stream results in a total number $N_{\mathrm{SS}}$ spatial streams, which can be smaller than, or equal to, the number of available RF chains $N_{\mathrm{RF}}$ for the upconversion. In any case, linear combinations of the spatial streams are assigned to the RF chains; these combinations are described by means of the so-called "spatial mapping" matrix $\mathbf{Q}$, so that for each time instant the vector of spatial-stream vectors $\mathbf{x}$ is mapped onto the signals for the RF chains $\mathbf{y}$ as $\mathbf{y} = \mathbf{Q}\mathbf{x}$. The following possibilities are defined in the standard:

- *Direct mapping*: this method is used if $N_{\mathrm{SS}} = N_{\mathrm{RF}}$. In the simplest case, $\mathbf{Q}$ is either an identity matrix, or it is a diagonal matrix in which the elements perform CSD, so that $Q_{i,i} =$

$\exp[-j2\pi k\Delta_F\tau_i]$. The CSD serves to avoid inadvertent beamforming when similar signals occur in the different spatial streams.

- *Spatial mapping for the case* $N_{SS} = N_{RF}$: in this case, **Q** is the product of a CSD matrix with a square matrix with orthogonal columns, such as a Fourier matrix or a Hadamard matrix.
- *Spatial matrix for the case* $N_{SS} < N_{RF}$: in this case, some of the spatial streams are duplicated (so that the total number of streams becomes equal to $N_{RF}$). All the streams are then power adjusted (so that the total power stays constant) and mapped onto the transmit RF chains by means of a CSD matrix.
- *Beamforming steering matrix*: any matrix that improves the overall Bit Error Rate (BER) can be used as matrix **Q**. Realistically speaking, the matrix is based on channel state information at the TX (see Section 29.3.6). In particular, if the TX knows the instantaneous channel transfer matrix **H**, it can perform an eigenvalue decomposition of **H** on each subcarrier, precode with the right singular matrix (see Section 20.2.5), and possibly weight the streams according to the waterfilling rules.

**Antenna Selection**

There are situations where the number of available antenna elements is larger than the number of RF chains – either because of cost reasons, or because the maximum number of RF chains foreseen in the 802.11n standard is 4. In those cases, antenna selection allows improvement of the system performance.

The available RF chains are connected to the "instantaneously best" antenna elements via electronic switches. However, in order to determine the "best" antenna elements, the complete channel (from each transmit to each RX antenna element) has to be sounded. This is achieved in two or more subsequent packets. For example, for transmit antenna selection, the first packet is transmitted from the first subset of antennas, the next packet from a second subset of antennas, and so on. After all subsets have been tried out, the RX sends an information to the TX about which subset to use. Receive antenna selection works analogously.

## *29.3.4 20-MHz and 40-MHz Channels*

802.11n allows the use of either 20 MHz or 40 MHz bandwidth, see Figure 29.8. In the former case, 802.11n uses more subcarriers (56) than 802.11a (52). For 40-MHz bandwidth, 114 subcarriers are used. Subcarriers are added in the middle and in the place of the DC subcarrier. The phases of signals in the upper channel are rotated by $+90^\circ$ in reference to the lower channel.

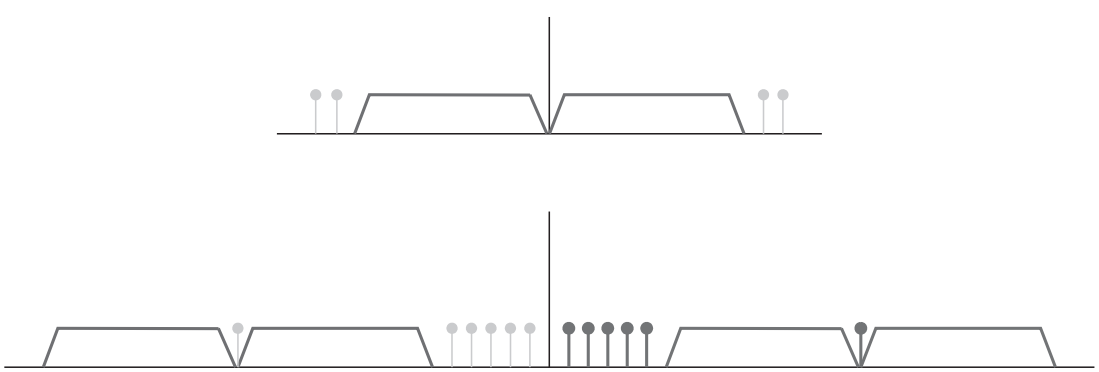

**Figure 29.8** 20-MHz and 40-MHz subcarriers.

## 29.3.5 Headers and Preambles

Another important point is the backward compatibility to 802.11a/g. Networks with either 11a/g or 11n access point, and a mixture of 11a/g and 11n client have to work. Many of the details of the 11n standard, in particular the design of preamble, can only be understood in the light of the requirement for backward compatibility.

There are three types of PLCP preambles (i.e., the part of the preamble that is used for synchronization and channel estimation, compare Section 29.2.4), see Figure 29.9. The first type is the legacy preamble, which is identical to the 802.11a preamble; this is to be used if only legacy (802.11a) devices are used at a given time.

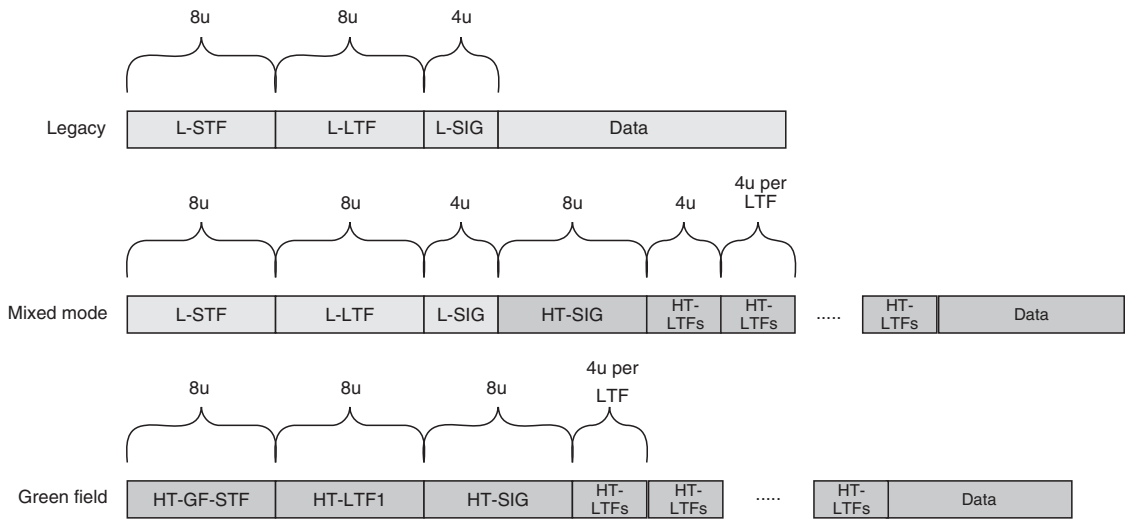


**Figure 29.9** Types of preambles in IEEE 802.11n. *In this figure:* HT-GF-STF, High Throughput – GreenField – Short Training Field; L-SIG, Legacy SIGnalling field; L-STF, Legacy Short Training Field.

If both 802.11a and 802.11n devices are present in a Local Area Network (LAN), then the mixed-mode preamble has to be used. It starts with the same fields as the legacy preamble, which are then followed by the High Throughput-SIGnal field (HT-SIG), see Figure 29.10. This contains information about a number of MIMO parameters, bandwidth allocations, etc., that are unique to 11n devices. In particular, it contains information about:

- modulation and coding scheme;
- bandwidth indication (20 or 40 MHz);
- *smoothing*: indicates whether frequency-domain smoothing is recommended as part of channel estimation;
- not-sounding (i.e., whether the current PPDU is a sounding PPDU, see Section 29.3.6);
- aggregation (whether the data portion of the packet participates is part of a data aggregation transmission);
- Space Time Block Code (STBC) (indication of space–time coding);
- FEC encoding (convolutional or LDPC);
- short GI: whether long or short cyclic prefix are used;
- number of extension spatial streams;
- Cyclic Redundancy Check (CRC): error detection for HT-SIG;
- tail bits for terminating convolutional code.

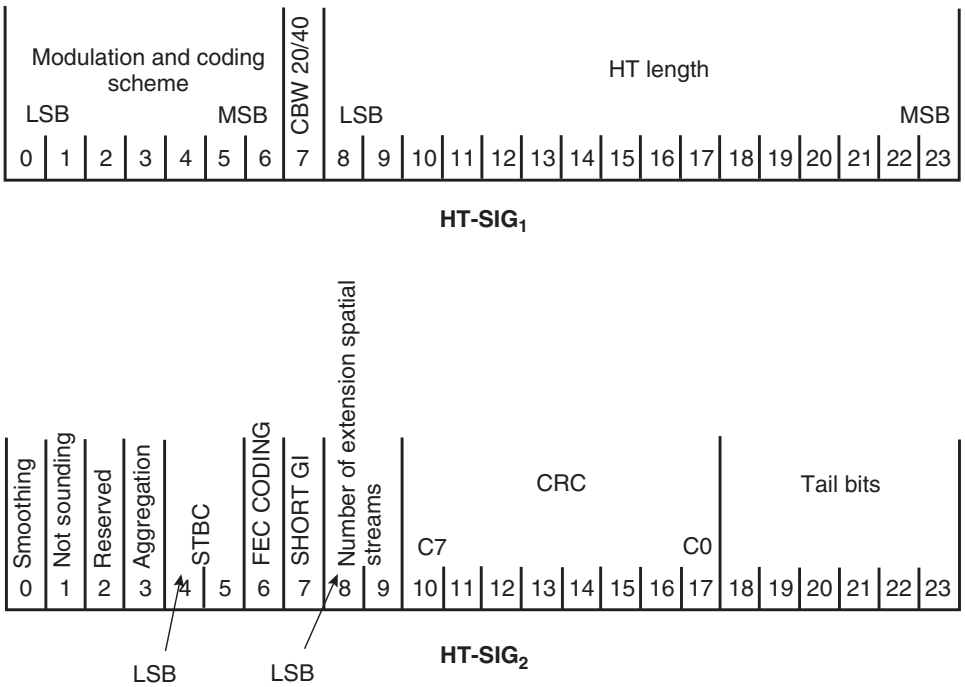


**Figure 29.10** High-throughput signaling field.
Reproduced with permission from [IEEE P802.11n] © IEEE

The HT-SIG is encoded with a rate 1/2 convolutional code, and BPSK modulated, to ensure high robustness in the transmission.

If there are only 11n devices in a LAN, then the greenfield preamble can be used, which omits all the "legacy" fields, and thus provides a shorter and more efficient preamble.

## *29.3.6 Channel Estimation*

The MIMO channel between TX and RX is estimated from the High Throughput – Long Training Field (HT-LTFs). If the TX provides training for the exactly available spatial streams, then the preamble uses exactly $N_{SS}$ training symbols (except for the case of three spatial streams, which requires four training symbols). If the TX is providing more training fields than is required for the current number of spatial streams, more spatial dimensions can be estimated, which enables, e.g., beamforming for eigenvalue decomposition. In this case, the PPDU is called a *sounding PPDU*. Thus, the HT long training field portion has one or two parts. The first part consists of $N_{SS}$ Long Training Fields (LTFs) (known as Data-HT-LTFs) that are necessary for demodulation of the HT-Data portion of the PPDU. The optional second part (the one occurring only in sounding PPDUs) consists of the HT-LTFs that may be used to sound extra spatial dimensions. Figure 29.11 shows an example.

Another way of sounding all spatial dimensions is to use a PPDU that contains no payload data. The preamble of such a *Null Data Packet* then contains only data-HT-LTFs, but the (nominal) $N_{SS}$ is chosen such that all required spatial dimensions can be sounded.

The HT-LTFs provide the Channel State Information (CSI) that is required for the reception of the signals, but can also be used at the TX to enable an appropriate precoding (i.e., creation of a suitable matrix **Q** for each subcarrier). The CSI at the TX can either be obtained through explicit feedback, or from the principle of reciprocity.

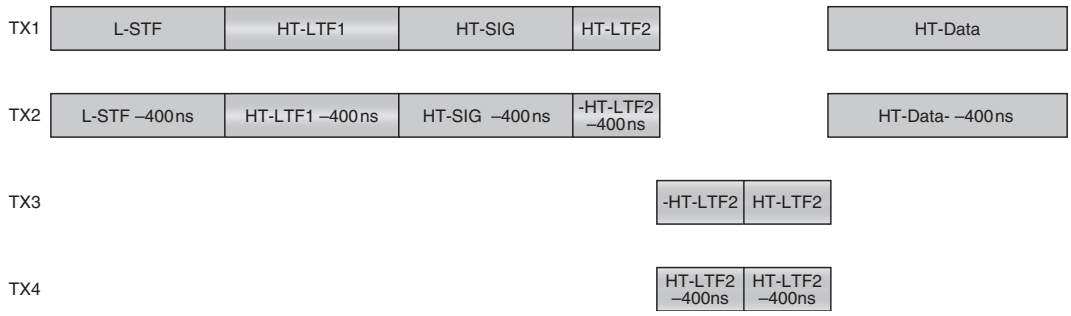


**Figure 29.11** Example for sounding PPDU with extension HT-LTFs.

- In the case of explicit feedback, the RX determines either the effective channel matrix $\mathbf{H}_{\text{eff}}$ (which is the product of the matrix $\mathbf{Q}$ with the channel matrix $\mathbf{H}$) or the beamforming matrix. The real and imaginary parts of the channel matrix coefficients are quantized to 4, 5, 6, or 8 bits. This can result in rather large channel matrices that need to be fed back; therefore, a compressed feedback is foreseen as well.
- In implicit feedback, the TX employs the channel reciprocity to obtain knowledge about the channel. Since all transmissions are at the same frequency, and the channels are changing only slowly, the channel matrix is approximately the same for uplink and the downlink. However, this is true only for the actual propagation channel (from TX antenna connector to RX antenna connector), while the upconversion/downconversion RF chains are *not* necessarily reciprocal. The 802.11n standard thus foresees a procedure for calculating a set of calibration matrices that can be applied at the transmit side of a STAtion (STA i.e., an access point or client), to correct the amplitude and phase differences between the transmit and receive chains in the STA. The procedure, which has to be performed only at very large intervals, involves essentially determining channel coefficients implicitly as well as explicitly; the difference between the results can then be used to establish the calibration matrices.

## 29.4 Packet Transmission in 802.11 Wireless Local Area Networks

There are nine MAC services specified by IEEE 802.11. These include distribution, integration, association, reassociation, disassociation, authentication, deauthentication, privacy, and MSDU delivery. Six of the services are used to support MSDU delivery between STAs (used as a generic expression for 802.11 devices, both access points and clients). Three of the services are used to control 802.11 WLAN access and confidentiality. Each of the services is supported by one or more MAC frame types. The IEEE 802.11 MAC uses three types of messages: *data, management*, and *control*. Some of the services are supported by MAC management messages and some by MAC data messages. All messages gain access to the WM (Wireless Medium) via the IEEE 802.11 MAC medium access method which includes both contention-based and contention-free channel access methods: *Distributed Coordination Function* (DCF) and *Point Coordination Function* (PCF). In the following, the 802.11 MAC functions and services will be described.

### *29.4.1 General Medium Access Control Structure*

The 802.11 MAC uses a temporal superframe structure with *Contention Period* (CP)[4] and *Contention Free Period* (CFP) alternately as shown in Figure 29.12. Superframes are separated by

[4] Note that it is only in this section that we use the abbreviation CP for contention period (and not for cyclic prefix). Since we are talking about the MAC layer only, no confusion can arise.

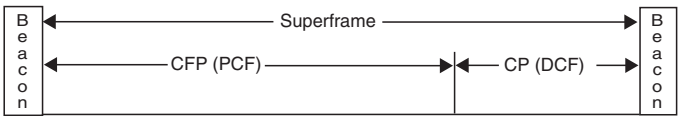


**Figure 29.12** Superframe structure of 802.11.
Reproduced with permission from IEEE 802.11 © IEEE.

periodic management frames, the so-called "beacon frames." During the CP, DCF is used for channel access, while PCF is used for channel access during the CFP.

The 802.11 MAC uses different interframe gaps, denoted as *Inter Frame Spaces* (IFSs), in order to control medium access – i.e., to give STAs in specific cases a higher or lower priority. These IFSs are (in the order shortest to longest):

- *Short Inter Frame Space* (SIFS);
- *Priority Inter Frame Space* (PIFS);
- *Distributed Inter Frame Space* (DIFS);
- *Extended Inter Frame Space* (EIFS).

Their actual values depend on PHY parameters.

## 29.4.2 Frame Formats

The MAC frame format comprises a set of fields that contain various types of control information as well as the actual frame body, all of which occur in a fixed order in all frames. Figure 29.13 depicts the general MAC frame format. The fields Address 2, Address 3, Sequence Control, Address 4, and Frame Body are only present in certain frame types.

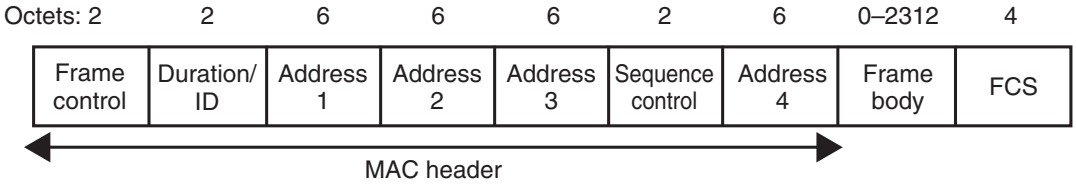


**Figure 29.13** Medium-access-control frame format (a typical MPDU).
Reproduced with permission from O'Hara and Petrick [2005] © IEEE.

When the MSDUs handed down to the MAC become too large, it becomes difficult to transmit them in one block: obviously, the probability of a block error – i.e., that one of the bits in the block is in error – increases with duration of the block.[5] As each block error might lead to the necessity of retransmission, this is highly undesirable. Thus, MSDUs have to be fragmented in order to increase transmission reliability. This fragmentation is done when an MSDU size exceeds the fragmentation threshold. In this case, the MSDU will be broken into multiple fragments with an MPDU size equal to a fragmentation threshold, and a special field (the "more_fragments" field) is set to 1 in all but the last fragment. The receiving STA acknowledges each fragment individually. The channel is not released until the complete MSDU has been transmitted successfully or until

[5] Note that, in general, this effect may be offset by the fact that larger blocks allow the use of better codes, like highly efficient LDPC codes. However, for convolutional codes this is not relevant.

a nonacknowledgment has been received for a fragment. In the latter case, the source STA will recontend for the channel following the normal rules and retransmit the nonacknowledged fragment, as well as all the subsequent ones.

## 29.4.3 Packet Radio Multiple Access

### Carrier Sense Multiple Access

The DCF employs *Carrier Sense Multiple Access with Collision Avoidance* (CSMA/CA), as described in Chapter 17, plus a random backoff mechanism. Support for DCF is mandatory for all STAs. In DCF mode, each STA checks whether the channel is idle before attempting to transmit. If the channel has been sensed idle for a DIFS period, transmission can begin immediately. If the channel is determined to be busy, the STA will defer until the end of the current transmission. After the end of the current transmission, the STA will select a random number called a "backoff timer," in the range between 0 and a *Contention Window* (CW). This is the time the WM has to be free before the STA might try to transmit again. The size of the CW increases (up to a limit) every time a transmission has to be deferred. If transmission is not successful, the STA thinks that a collision has occurred. Also in this case, the CW is doubled, and a new backoff procedure starts again. The process will continue until transmission is not successful (or discarded). The basic access method and backoff procedure are shown in Figures 29.14 and 29.15, respectively.

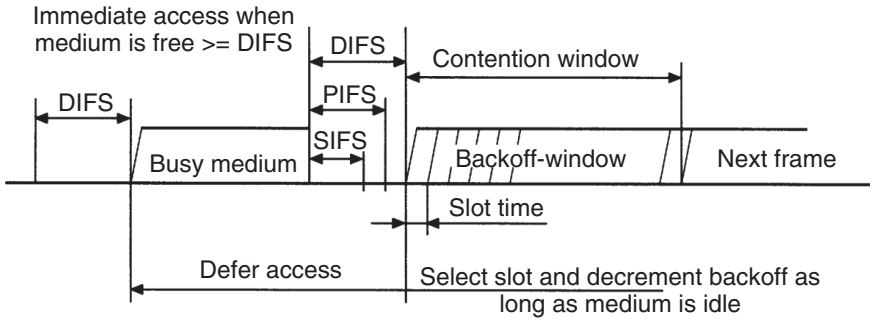


**Figure 29.14** Basic access method.

Reproduced with permission from IEEE 802.11 © IEEE.

Physical and virtual carrier-sense functions are used to determine the state of the channel. When either function indicates a busy channel, the channel should be considered busy; otherwise, it should be considered idle. A physical carrier-sense mechanism is provided by the PHY. A virtual carrier-sense mechanism is 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 the DURATION field in the transmitted frames.

### Polling

PCF is an optional medium access mode for 802.11. It provides contention-free frame transfer, based on polling (see Chapter 17). The *Point Coordinator* (PC) resides in the BS (access point). All STAs inherently obey the medium access rules of the PCF and set their NAV at the beginning of each CFP. The PCF relies on the PC to perform polling, and enables polled STAs to transmit without contending for the channel. When polled by the PC, an STA transmits only one MPDU, which can be to any destination. If the transmitted dataframe is not in turn acknowledged, the STA

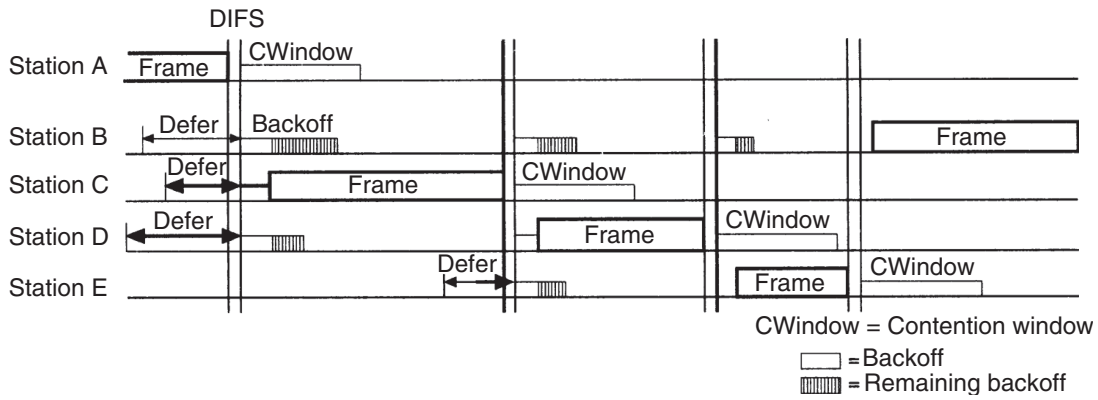


**Figure 29.15** Timing backoff procedure.

Reproduced with permission from IEEE 802.11 © IEEE.

does not retransmit the frame unless it is polled again by the PC, or it decides to retransmit during the CP. An example of PCF frame transfer is given in Figure 29.16. At the beginning of each CFP, the PC senses and makes sure the channel is idle for one PIFS before sending the beacon frame. All STAs adjust their NAVs according to the broadcast CFP duration value in the beacon. After one SIFS time of the beacon, the PC may send out a *Contention-free Poll* (CF-Poll), data, or data plus a CF-Poll. Each polled STA can get a chance to transmit to another STA or respond to the PC after one SIFS with an acknowledgment (plus possibly data).

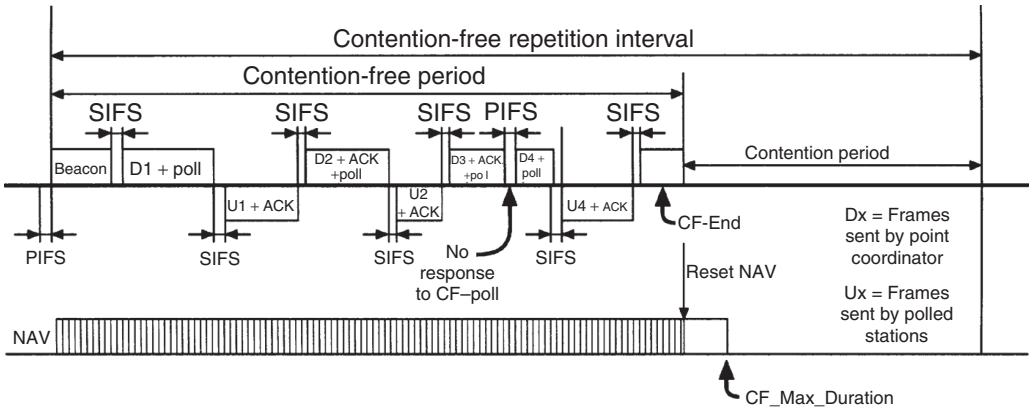


**Figure 29.16** Point-coordination-function frame transfer.

Reproduced with permission from IEEE 802.11 © IEEE.

As discussed above, the DCF and PCF coexist in a manner that permits both to operate concurrently.[6] The two access methods alternate, with a CFP followed by a CP. Since the PCF is built on top of the DCF, there are no conflicts between DCF and PCF when they coexist in the system. All STAs will inherently obey the medium access rules of the PCF. STAs will stay silent during CFP unless they are polled.

[6] Within the same Basic Service Set (BSS).

## 29.5 Alternative Wireless Local Area Networks and Future Developments

As we mentioned in the introduction, there is a multitude of "802.11-named" standards, most of which have not gained widespread popularity. Among these standards, the original 802.11 standard with its 1-Mbit/s direct-sequence spreading mode is a typical example. Furthermore, the frequency-hopping mode of this standard never gained popularity. Finally, the standard also defined a mode for infrared communications between computers; this application never gained significant popularity as well. While the 802.11b standard was enormously popular in the mid-2000s, it has in the meantime lost much ground to the 802.11g standard.

In all the discussions above, we have concentrated on WLANs that have one access point, plus a number of clients that connect to this access point. The 802.11 group of standards also establishes modes for peer-to-peer communications. This approach has not gathered widespread popularity either.

We have also mentioned the HIPERLAN standards developed by ETSI. The HIPERLAN II standard, in particular, bears considerable similarity to the 802.11a PHY, though the MAC is based on Time Division Multiple Access (TDMA) instead of CSMA. While a number of research papers have been published on this standard, it has not gained practical relevance, and even its previous proponents have switched to using 802.11a.

802.11 has also started activities on standards that can provide even higher throughput than the 11n standard. One of these envisioned high-throughput standards works at carrier frequencies around 60 GHz, where a very large bandwidth (approximately 7 GHz) is available. Due to the high carrier frequency, attenuation is strong, and the scheme works best in line-of-sight situations, or at least for TX and RX being in the same room. Another scheme, which works in the usual microwave regime, exploits multiple-antenna techniques that are more advanced than those in 11n and/or have more antenna elements, to achieve a higher throughput.

## 29.6 Glossary for WLAN

| | |
|---|---|
| AC | Access Category |
| AIFS | Arbitration Inter Frame Spacing |
| AP | Access Point |
| CAP | Controlled Access Period |
| CCK | Complementary Code Keying |
| CFB | Contention Free Burst |
| CFP | Contention Free Period |
| CF-Poll | Contention-free Poll |
| CP | Contention Period |
| CSMA/CA | Carrier Sense Multiple Access with Collision Avoidance |
| CW | Contention Window |
| DCF | Distributed Coordination Function |
| DIFS | Distributed Inter Frame Space |
| DLP | Direct Link Protocol |
| EDCA | Enhanced Distributed Channel Access |
| EIFS | Extended Inter Frame Space |
| FCS | Frame Check Sequence |
| HCCA HCF | (Hybrid Coordination Function) Controlled Channel Access |
| HC | Hybrid Coordinator |
| HCF | Hybrid Coordination Function |

| | |
|---|---|
| HIPERLAN | High PERformance Local Area Network |
| IEEE | Institute of Electrical and Electronic Engineers |
| IFS | Inter Frame Space |
| ISM | Industrial, Scientific, and Medical |
| MBOA | Multi Band OFDM Alliance |
| MPDU | MAC Protocol Data Unit |
| MSDU | MAC Service Data Unit |
| NAV | Network Allocation Vector |
| PAN | Personal Area Network |
| PC | Point Coordinator |
| PCF | Point Coordination Function |
| PIFS | Priority Inter Frame Space |
| PLCP | Physical Layer Convergence Procedure |
| PPDU | Physical Layer Protocol Data Unit |
| PSDU | Physical Layer Service Data Unit |
| QAP | QoS Access Point |
| QoS | Quality of Service |
| QSTA | QoS STAtion |
| SIFS | Short Infer Frame Space |
| STA | STAtion |
| TC | Traffic Category |
| TS | Traffic Stream |
| TXOP | Transmission Opportunity |
| TSPEC | Traffic SPECifications |
| U-NII | Unlicensed National Information Structure |
| UP | User Priority |

## Further Reading

The official standards documents for the 802.11 standard can be found online at *www.802wirelessworld.com* Excellent summaries of the older 802.11 versions (802.11, 11b, 11a/g) and the recent 802.11n standard are given in O'Hara and Petrick [2005], and Perahia and Stacey [2008], respectively. A historically interesting comparison of IEEE 802 and HIPERLAN is found in Doufexi et al. [2002]. The principles of the WiMedia–MBOA (Multi Band OFDM Alliance) specifications are described in Siriwongpairat and Liu [2007]. A comparison between WLAN and Wireless Personal Area Network (WPAN) standards is given in Cooklev [2004].

For updates and errata for this chapter, see wides.usc.edu/teaching/textbook