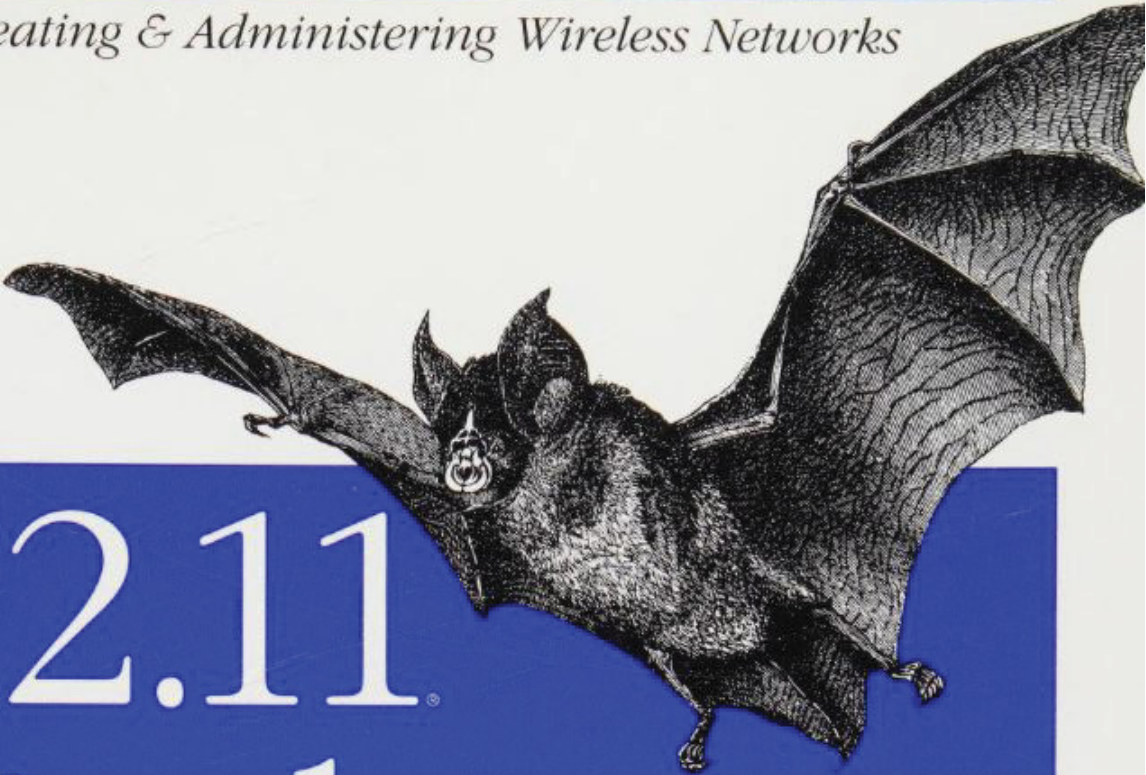


2nd Edition
Covers 802.11a, g, n & i

Creating & Administering Wireless Networks



802.11[®] Wireless Networks



The Definitive Guide

O'REILLY[®]

Matthew S. Gast

OZMO Ex. 2001, Page 1

IPR2023-00193

SECOND EDITION

802.11® Wireless Networks

The Definitive Guide

Matthew S. Gast

O'REILLY®

Beijing • Cambridge • Farnham • Köln • Paris • Sebastopol • Taipei • Tokyo

OZMO Ex. 2001, Page 3
IPR2023-00193

802.11® Wireless Networks: The Definitive Guide, Second Edition

by Matthew S. Gast

Copyright © 2005 Matthew S. Gast. All rights reserved.
Printed in the United States of America.

Published by O'Reilly Media, Inc., 1005 Gravenstein Highway North, Sebastopol, CA 95472.

O'Reilly books may be purchased for educational, business, or sales promotional use. Online editions are also available for most titles (safari.oreilly.com). For more information, contact our corporate/institutional sales department: (800) 998-9938 or corporate@oreilly.com.

Editor: Mike Loukides
Production Editor: Colleen Gorman
Cover Designer: Ellie Volckhausen
Interior Designer: David Futato

Printing History:

April 2002: First Edition.
April 2005: Second Edition.

Nutshell Handbook, the Nutshell Handbook logo, and the O'Reilly logo are registered trademarks of O'Reilly Media, Inc. 802.11® *Wireless Networks: The Definitive Guide*, Second Edition, the image of a horseshoe bat, and related trade dress are trademarks of O'Reilly Media, Inc.

802.11® and all 802.11-based trademarks and logos are trademarks or registered trademarks of IEEE, Inc. in the United States and other countries. O'Reilly Media, Inc. is independent of IEEE.

Many of the designations used by manufacturers and sellers to distinguish their products are claimed as trademarks. Where those designations appear in this book, and O'Reilly Media, Inc. was aware of a trademark claim, the designations have been printed in caps or initial caps.

While every precaution has been taken in the preparation of this book, the publisher and author assume no responsibility for errors or omissions, or for damages resulting from the use of the information contained herein.



This book uses RepKover™, a durable and flexible lay-flat binding.

ISBN: 0-596-10052-3

[M]

Table of Contents

Foreword	xi
Preface	xiii
1. Introduction to Wireless Networking	1
Why Wireless?	1
What Makes Wireless Networks Different	5
A Network by Any Other Name...	8
2. Overview of 802.11 Networks	12
IEEE 802 Network Technology Family Tree	13
802.11 Nomenclature and Design	14
802.11 Network Operations	23
Mobility Support	28
3. 802.11 MAC Fundamentals	32
Challenges for the MAC	34
MAC Access Modes and Timing	37
Contention-Based Access Using the DCF	41
Fragmentation and Reassembly	44
Frame Format	46
Encapsulation of Higher-Layer Protocols Within 802.11	54
Contention-Based Data Service	55
Frame Processing and Bridging	63

4. 802.11 Framing in Detail	67
Data Frames	67
Control Frames	76
Management Frames	82
Frame Transmission and Association and Authentication States	111
5. Wired Equivalent Privacy (WEP)	114
Cryptographic Background to WEP	114
WEP Cryptographic Operations	117
Problems with WEP	123
Dynamic WEP	127
6. User Authentication with 802.1X	129
The Extensible Authentication Protocol	130
EAP Methods	135
802.1X: Network Port Authentication	141
802.1X on Wireless LANs	145
7. 802.11i: Robust Security Networks, TKIP, and CCMP	149
The Temporal Key Integrity Protocol (TKIP)	149
Counter Mode with CBC-MAC (CCMP)	159
Robust Security Network (RSN) Operations	163
8. Management Operations	170
Management Architecture	170
Scanning	171
Authentication	176
Preauthentication	180
Association	184
Power Conservation	188
Timer Synchronization	197
Spectrum Management	199
9. Contention-Free Service with the PCF	214
Contention-Free Access Using the PCF	214
Detailed PCF Framing	218
Power Management and the PCF	223

802.11 MAC Fundamentals

This chapter begins our exploration of the 802.11 standard in depth. Chapter 2 provided a high-level overview of the standard and discussed some of its fundamental attributes. You are now at a fork in the book. Straight ahead lies a great deal of information on the 802.11 specification and the various related standards that it uses liberally. It is possible, however, to build a wired network without a thorough and detailed understanding of the protocols, and the same is true for wireless networks. However, there are a number of situations in which you may need a deeper knowledge of the machinery under the hood:

- Although 802.11 has been widely and rapidly adopted, security issues have continued to grab headlines. Network managers will undoubtedly be asked to comment on security issues, especially in any wireless LAN proposals. To understand and participate in these discussions, read Chapters 5 and 6. WEP with static keys should be considered fully broken. Solutions based on 802.1X and dynamic WEP keying are significantly stronger, with the full complement of protocols in 802.11i described in Chapter 7 stronger still.
- Troubleshooting wireless networks is similar to troubleshooting wired networks but can be much more complex. As always, a trusty packet sniffer can be an invaluable aid. To take full advantage of a packet sniffer, though, you need to understand what the packets mean to interpret your network's behavior.
- Tuning a wireless network is tied intimately to a number of parameters in the specification, as well as the behavior of the underlying radio technology. To understand the behavior of your network and what effect the optimizations will have requires a knowledge of what those parameters really do and how radio waves travel throughout your environment.
- Device drivers may expose low-level knobs and dials for you to play with. Most drivers provide good defaults for all of the parameters, but some give you freedom to experiment. Open source software users have the source code and are free to experiment with any and all settings.

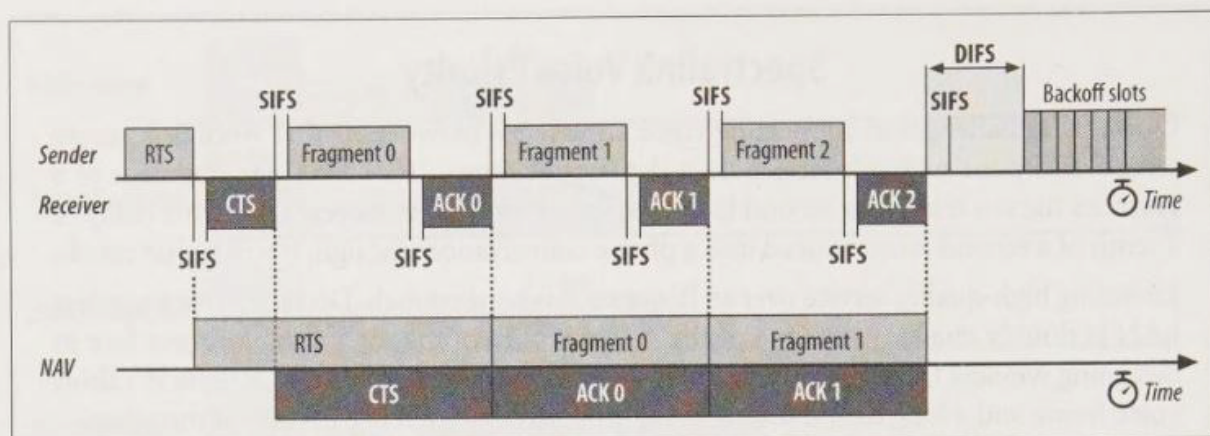


Figure 3-8. Fragmentation burst

Fragments and their acknowledgments are separated by the SIFS, so a station retains control of the channel during a fragmentation burst. The NAV is also used to ensure that other stations do not use the channel during the fragmentation burst. As with any RTS/CTS exchange, the RTS and CTS both set the NAV from the expected time to the end of the first fragments in the air. Subsequent fragments then form a chain. Each fragment sets the NAV to hold the medium until the end of the acknowledgment for the next frame. Fragment 0 sets the NAV to hold the medium until ACK 1, fragment 1 sets the NAV to hold the medium until ACK 2, and so on. After the last fragment and its acknowledgment have been sent, the NAV is set to 0, indicating that the medium will be released after the fragmentation burst completes.

Frame Format

To meet the challenges posed by a wireless data link, the MAC was forced to adopt several unique features, not the least of which was the use of four address fields. Not all frames use all the address fields, and the values assigned to the address fields may change depending on the type of MAC frame being transmitted. Details on the use of address fields in different frame types are presented in Chapter 4. Figure 3-9 shows the generic 802.11 MAC frame. All diagrams in this section follow the IEEE conventions in 802.11. Fields are transmitted from left to right.

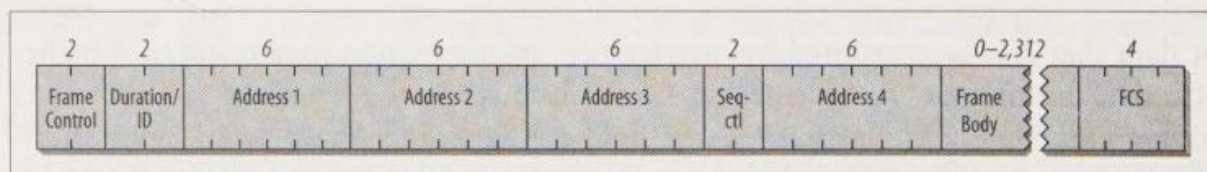


Figure 3-9. Generic 802.11 MAC frame

802.11 MAC frames do not include some of the classic Ethernet frame features, most notably the type/length field and the preamble. The preamble is part of the physical layer, and encapsulation details such as type and length are present in the header on the data carried in the 802.11 frame.

Frame Control

Each frame starts with a two-byte Frame Control subfield, shown in Figure 3-10. The components of the Frame Control subfield are:

Protocol version

Two bits indicate which version of the 802.11 MAC is contained in the rest of the frame. At present, only one version of the 802.11 MAC has been developed; it is assigned the protocol number 0. Other values will appear when the IEEE standardizes changes to the MAC that render it incompatible with the initial specification. So far, none of the revisions to 802.11 have required incrementing the protocol number.

Type and subtype fields

Type and subtype fields identify the type of frame used. To cope with noise and unreliability, a number of management functions are incorporated into the 802.11 MAC. Some, such as the RTS/CTS operations and the acknowledgments, have already been discussed. Table 3-1 shows how the type and subtype identifiers are used to create the different classes of frames.

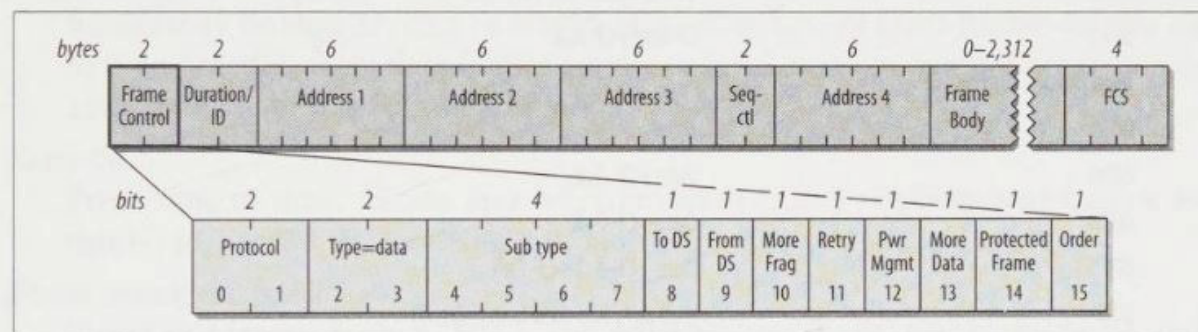


Figure 3-10. Frame control field

In Table 3-1, bit strings are written most-significant bit first, which is the reverse of the order used in Figure 3-10. Therefore, the frame type is the third bit in the frame control field followed by the second bit (b3 b2), and the subtype is the seventh bit, followed by the sixth, fifth, and fourth bits (b7 b6 b5 b4).

Table 3-1. Type and subtype identifiers

Subtype value	Subtype name
Management frames (type=00) ^a	
0000	Association request
0001	Association response
0010	Reassociation request
0011	Reassociation response
0100	Probe request
0101	Probe response

Table 3-1. Type and subtype identifiers (continued)

Subtype value	Subtype name
1000	Beacon
1001	Announcement traffic indication message (ATIM)
1010	Disassociation
1011	Authentication
1100	Deauthentication
1101	Action (for spectrum management with 802.11h, also for QoS)
Control frames (type=01) ^b	
1000	Block Acknowledgment Request (QoS)
1001	Block Acknowledgment (QoS)
1010	Power Save (PS)-Poll
1011	RTS
1100	CTS
1101	Acknowledgment (ACK)
1110	Contention-Free (CF)-End
1111	CF-End+CF-Ack
Data frames (type=10)	
0000	Data
0001	Data+CF-Ack
0010	Data+CF-Poll
0011	Data+CF-Ack+CF-Poll
0100	Null data (no data transmitted)
0101	CF-Ack (no data transmitted)
0110	CF-Poll (no data transmitted)
0111	CF-Ack+CF-Poll (no data transmitted)
1000	QoS Data ^c
1001	QoS Data + CF-Ack ^c
1010	QoS Data + CF-Poll ^c
1011	QoS Data + CF-Ack + CF-Poll ^c
1100	QoS Null (no data transmitted) ^c
1101	QoS CF-Ack (no data transmitted) ^c
1110	QoS CF-Poll (no data transmitted) ^c
1111	QoS CF-Ack+CF-Poll (no data transmitted) ^c
(Frame type 11 is reserved)	

^a Management subtypes 0110–0111 and 1110–1111 are reserved and not currently used.

^b Control subtypes 0000–0111 are reserved and not currently used.

^c Proposed by the 802.11e task group, but not yet standardized. Note that these frames all have a leading one, which has caused some to refer to the first bit as the QoS bit.

802.11 Framing in Detail

Chapter 3 presented the basic frame structure and the fields that comprise it, but it did not go into detail about the different frame types. Ethernet framing is a simple matter: add a preamble, some addressing information, and tack on a frame check at the end. 802.11 framing is much more involved because the wireless medium requires several management features and corresponding frame types not found in wired networks.

Three major frame types exist. *Data frames* are the pack horses of 802.11, hauling data from station to station. Several different data frame flavors can occur, depending on the network. *Control frames* are used in conjunction with data frames to perform area-clearing operations, channel acquisition and carrier-sensing maintenance functions, and positive acknowledgment of received data. Control and data frames work in conjunction to deliver data reliably from station to station. *Management frames* perform supervisory functions; they are used to join and leave wireless networks and move associations from access point to access point.

This chapter is intended to be a reference. There is only so much life any author can breathe into framing details, no matter how much effort is expended to make the details interesting. Please feel free to skip this chapter in its entirety and flip back when you need in-depth information about frame structure. With rare exception, detailed framing relationships generally do not fall into the category of “something a network administrator needs to know.” This chapter tends to be a bit acronym-heavy as well, so refer to the glossary at the back of the book if you do not recognize an acronym.

Data Frames

Data frames carry higher-level protocol data in the frame body. Figure 4-1 shows a generic data frame. Depending on the particular type of data frame, some of the fields in the figure may not be used.

- The element ID is 221, not 48.
- A WPA-specific tag of 00:50:F2:01 is inserted before the version field.
- Microsoft's OUI (00:50:F2) is used instead of the 802.11 working group's OUI.
- Only one cipher suite and one authentication suite are supported in the information element. However, many WPA implementations do not follow this restriction.
- TKIP is the default cipher, rather than CCMP.
- Preauthentication is not supported in WPA, so the preauthentication capabilities bit is always zero.

Types of Management Frames

The fixed fields and information elements are used in the body of management frames to convey information. Several types of management frames exist and are used for various link-layer maintenance functions.

Beacon

Beacon frames announce the existence of a network and are an important part of many network maintenance tasks. They are transmitted at regular intervals to allow mobile stations to find and identify a network, as well as match parameters for joining the network. In an infrastructure network, the access point is responsible for transmitting Beacon frames. The area in which Beacon frames appear defines the basic service area. All communication in an infrastructure network is done through an access point, so stations on the network must be close enough to hear the Beacons.

Figure 4-51 shows most the fields that can be used in a Beacon frame in the order in which they appear. Not all of the elements are present in all Beacons. Optional fields are present only when there is a reason for them to be used. The FH and DS Parameter Sets are used only when the underlying physical layer is based on frequency hopping or direct-sequence techniques. Only one physical layer can be in use at any point, so the FH and DS Parameter Sets are mutually exclusive.

The CF Parameter Set is used only in frames generated by access points that support the PCF, which is optional. The TIM element is used only in Beacons generated by access points, because only access points perform frame buffering. If the Country-specific frequency hopping extensions were to be present, they would follow the Country information element. Frequency hopping networks are much less common now, though, so I omit the frequency hopping extensions for simplicity. Likewise, the IBSS DFS element occur between the Quiet and TPC Report elements, were it to appear.

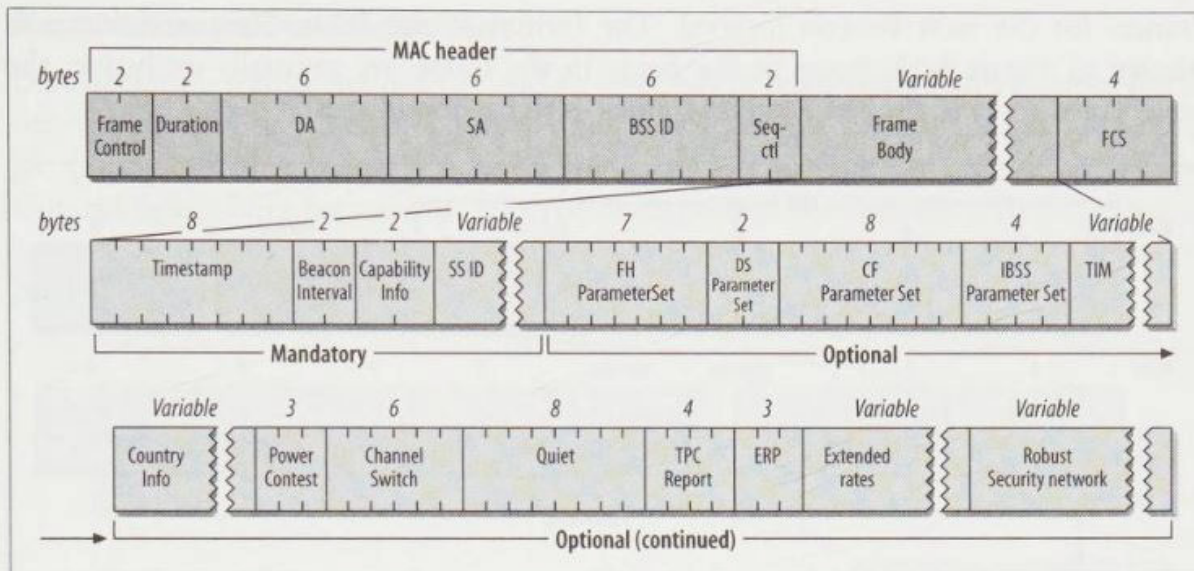


Figure 4-51. Beacon frame

Probe Request

Mobile stations use Probe Request frames to scan an area for existing 802.11 networks. The format of the Probe Request frame is shown in Figure 4-52. All fields are mandatory.

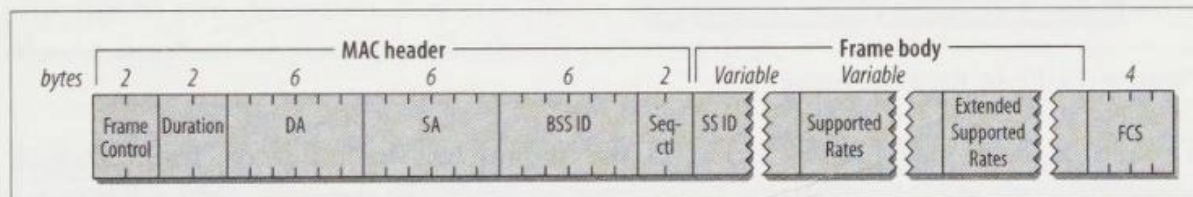


Figure 4-52. Probe Request frame

A Probe Request frame contains two fields: the SSID and the rates supported by the mobile station. Stations that receive Probe Requests use the information to determine whether the mobile station can join the network. To make a happy union, the mobile station must support all the data rates required by the network and must want to join the network identified by the SSID. This may be set to the SSID of a specific network or set to join any compatible network. Drivers that allow cards to join any network use the broadcast SSID in Probe Requests.

Probe Response

If a Probe Request encounters a network with compatible parameters, the network sends a Probe Response frame. The station that sent the last Beacon is responsible for responding to incoming probes. In infrastructure networks, this station is the access point. In an IBSS, responsibility for Beacon transmission is distributed. After a station transmits a Beacon, it assumes responsibility for sending Probe Response