# Contents

Preface xvii

Acknowledgments xix

About the Author xxi

Part I Overview 1

Chapter 1 What Is Bluetooth Low Energy? 3
   1.1 Device Types 6
   1.2 Design Goals 7
   1.3 Terminology 9

Chapter 2 Basic Concepts 11
   2.1 Button-Cell Batteries 11
   2.2 Time Is Energy 12
   2.3 Memory Is Expensive 13
   2.4 Asymmetric Design 14
   2.5 Design For Success 15
   2.6 Everything Has State 16
   2.7 Client-Server Architecture 17
   2.8 Modular Architecture 18
   2.9 One Billion Is a Small Number 19
   2.10 Connectionless Model 19
   2.11 Paradigms 20
      2.11.1 Client-Server Architecture 20
      2.11.2 Service-Oriented Architecture 21
Chapter 6  Direct Test Mode
6.1  Background 61
6.2  Transceiver Testing 62
  6.2.1  Test Packet Format 63
  6.2.2  Transmitter Tests 63
  6.2.3  Receiver Tests 64
6.3  Hardware Interface 65
  6.3.1  UART 65
  6.3.2  Commands and Events 65
6.4  Direct Testing by Using HCI 67

Chapter 7  The Link Layer
7.1  The Link Layer State Machine 69
  7.1.1  The Standby State 70
  7.1.2  The Advertising State 71
  7.1.3  The Scanning State 72
  7.1.4  The Initiating State 73
  7.1.5  The Connection State 73
  7.1.6  Multiple State Machines 74
7.2  Packets 76
  7.2.1  Advertising and Data Packets 76
  7.2.2  Whitening 77
7.3  Packet Structure 79
  7.3.1  Bit Order and Bytes 79
  7.3.2  The Preamble 79
  7.3.3  Access Address 80
  7.3.4  Header 81
  7.3.5  Length 82
  7.3.6  Payload 83
  7.3.7  Cyclic Redundancy Check 84
7.4  Channels 84
  7.4.1  Frequency Hopping 87
  7.4.2  Adaptive Frequency Hopping 88
7.5  Finding Devices 90
  7.5.1  General Advertising 91
  7.5.2  Direct Advertising 91
7.5.3 Nonconnectable Advertising
7.5.4 Discoverable Advertising
7.6 Broadcasting
7.7 Creating Connections
  7.7.1 Access Address
  7.7.2 CRC Initialization
  7.7.3 Transmit Window
  7.7.4 Connection Events
  7.7.5 Channel Map
  7.7.6 Sleep Clock Accuracy
7.8 Sending Data
  7.8.1 Data Header
  7.8.2 Logical Link Identifier
  7.8.3 Sequence Numbers
  7.8.4 Acknowledgement
  7.8.5 More Data
  7.8.6 Examples of the Use of Sequence Numbers and More Data
7.9 Encryption
  7.9.1 AES
  7.9.2 Encrypting Payload Data
  7.9.3 Message Integrity Check
7.10 Managing Connections
  7.10.1 Connection Parameter Update
  7.10.2 Adaptive Frequency Hopping
  7.10.3 Starting Encryption
  7.10.4 Restarting Encryption
  7.10.5 Version Exchange
  7.10.6 Feature Exchange
  7.10.7 Terminating Connections
7.11 Robustness
  7.11.1 Adaptive Frequency Hopping
  7.11.2 Strong CRCs
7.12 Optimizations for Low Power
  7.12.1 Short Packets
  7.12.2 High Bit Rate
  7.12.3 Low Overhead
  7.12.4 Acknowledgement Scheme
  7.12.5 Single-Channel Connection Events
7.12.6 Subrating Connection Events
7.12.7 Offline Encryption

Chapter 8 The Host/Controller Interface
8.1 Introduction
8.2 Physical Interfaces
  8.2.1 UART
  8.2.2 3-Wire UART
  8.2.3 USB
  8.2.4 SDIO
8.3 Logical Interface
  8.3.1 HCI Channels
  8.3.2 Command Packets
  8.3.3 Event Packets
  8.3.4 Data Packets
  8.3.5 Command Flow Control
  8.3.6 Data Flow Control
8.4 Controller Setup
  8.4.1 Reset the Controller to a Known State
  8.4.2 Reading the Device Address
  8.4.3 Set Event Masks
  8.4.4 Read Buffer Sizes
  8.4.5 Read Supported Features
  8.4.6 Read Supported States
  8.4.7 Random Numbers
  8.4.8 Encrypting Data
  8.4.9 Set Random Address
  8.4.10 White Lists
8.5 Broadcasting and Observing
  8.5.1 Advertising
  8.5.2 Passive Scanning
  8.5.3 Active Scanning
8.6 Initiating Connections
  8.6.1 Initiating Connection to White List
  8.6.2 Initiating a Connection to a Device
  8.6.3 Canceling Initiating a Connection
8.7 Connection Management
  8.7.1 Connection Update
  8.7.2 Channel Map Update
8.7.3 Feature Exchange 160
8.7.4 Version Exchange 160
8.7.5 Starting Encryption 161
8.7.6 Restarting Encryption 163
8.7.7 Terminating a Connection 164

Part III Host 167

Chapter 9 Logical Link Control and Adaptation Protocol 169
9.1 Background 169
9.2 L2CAP Channels 171
9.3 The L2CAP Packet Structure 172
9.4 The LE Signaling Channel 173
  9.4.1 Command Reject 174
  9.4.2 Connection Parameter Update Request and Response 175

Chapter 10 Attributes 179
10.1 Background 179
  10.1.1 Protocol Proliferation Is Wrong 180
  10.1.2 Data, Data, Everywhere... 180
  10.1.3 Data and State 181
  10.1.4 Kinds of State 182
  10.1.5 State Machines 183
  10.1.6 Services and Profiles 185
10.2 Attributes 189
  10.2.1 Attribute 189
  10.2.2 The Attribute Handle 189
  10.2.3 Attribute Type 190
  10.2.4 Attribute Value 191
  10.2.5 Databases, Servers, and Clients 192
  10.2.6 Attribute Permissions 194
  10.2.7 Accessing Attributes 196
  10.2.8 Atomic Operations and Transactions 197
10.3 Grouping 199
10.4 Services 199
  10.4.1 Extending Services 201
  10.4.2 Reusing Another Service 203
  10.4.3 Combining Services 204
  10.4.4 Primary or Secondary 205
10.4.5 Plug-and-Play Client Applications 207
10.4.6 Service Declaration 208
10.4.7 Including Services 209

10.5 Characteristics 210
10.5.1 Characteristic Declaration 211
10.5.2 Characteristic Value 213
10.5.3 Descriptors 214

10.6 The Attribute Protocol 217
10.6.1 Protocol Messages 219
10.6.2 The Exchange MTU Request 221
10.6.3 The Find Information Request 221
10.6.4 The Find By Type Value Request 222
10.6.5 The Read By Type Request 223
10.6.6 The Read Request 224
10.6.7 The Read Blob Request 224
10.6.8 The Read Multiple Request 224
10.6.9 The Read By Group Type Request 225
10.6.10 The Write Request 225
10.6.11 The Write Command 225
10.6.12 The Signed Write Command 225
10.6.13 The Prepare Write Request and Execute Write Request 226
10.6.14 The Handle Value Notification 227
10.6.15 The Handle Value Indication 228
10.6.16 Error Response 228

10.7 The Generic Attribute Profile 231
10.7.1 The Discovery Procedures 232
10.7.2 The Discovering Services 232
10.7.3 Characteristic Discovery 234
10.7.4 Client-Initiated Procedures 235
10.7.5 Server-Initiated Procedures 238
10.7.6 Mapping ATT PDUs to GATT Procedures 239

Chapter 11 Security 241

11.1 Security Concepts 241
11.1.1 Authentication 241
11.1.2 Authorization 242
11.1.3 Integrity 243
11.1.4 Confidentiality 243
11.1.5 Privacy 243
11.1.6 Encryption Engine
11.1.7 Shared Secrets

11.2 Pairing and Bonding
11.2.1 Pairing
11.2.2 Exchange of Pairing Information
11.2.3 Authentication
11.2.4 Key Distribution
11.2.5 Bonding

11.3 Signing of Data

Chapter 12 The Generic Access Profile

12.1 Background
12.1.1 Initial Discovery
12.1.2 Establishing the Initial Connection
12.1.3 Service Characterization
12.1.4 Long-Term Relationships
12.1.5 Reconnections
12.1.6 Private Addresses

12.2 GAP Roles

12.3 Modes and Procedures
12.3.1 Broadcast Mode and Observation Procedure
12.3.2 Discoverability
12.3.3 Connectability
12.3.4 Bonding

12.4 Security Modes
12.4.1 Security Modes

12.5 Advertising Data
12.5.1 Flags
12.5.2 Service
12.5.3 Local Name
12.5.4 TX Power Level
12.5.5 Slave Connection Interval Range
12.5.6 Service Solicitation
12.5.7 Service Data
12.5.8 Manufacturer-Specific Data

12.6 GAP Service
12.6.1 The Device Name Characteristic
12.6.2 The Appearance Characteristic
12.6.3 The Peripheral Privacy Flag 277
12.6.4 Reconnection Address 278
12.6.5 Peripheral Preferred Connection Parameters 278

Part IV Application 281

Chapter 13 Central 283
13.1 Background 283
13.2 Discovering Devices 283
13.3 Connecting to Devices 285
13.4 What Does This Device Do? 286
13.5 Generic Clients 287
13.6 Interacting with Services 288
  13.6.1 Readable Characteristics 288
  13.6.2 Control Points 289
  13.6.3 State Machines 290
  13.6.4 Notifications and Indications 291
13.7 Bonding 292
13.8 Changed Services 293
13.9 Implementing Profiles 294
  13.9.1 Defining a Profile 294
  13.9.2 Finding Services 295
  13.9.3 Finding Characteristics 296
  13.9.4 Using Characteristics 296
  13.9.5 Profile Security 296

Chapter 14 Peripherals 299
14.1 Background 299
14.2 Broadcast Only 299
14.3 Being Discoverable 300
14.4 Being Connectable 301
14.5 Exposing Services 301
14.6 Characteristics 302
14.7 Security Matters 303
14.8 Optimizing for Low Power 303
  14.8.1 Discoverable Advertising 305
  14.8.2 Bonding 306
  14.8.3 Connectable Advertising 306
<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.8.4</td>
<td>Directed Advertising</td>
<td>307</td>
</tr>
<tr>
<td>14.8.5</td>
<td>Connected</td>
<td>307</td>
</tr>
<tr>
<td>14.8.6</td>
<td>Stay Connected or Disconnect</td>
<td>309</td>
</tr>
<tr>
<td>14.9</td>
<td>Optimizing Attributes</td>
<td>311</td>
</tr>
</tbody>
</table>

## Chapter 15 Testing and Qualification

<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.1</td>
<td>Starting a Project</td>
<td>313</td>
</tr>
<tr>
<td>15.2</td>
<td>Selecting Features</td>
<td>316</td>
</tr>
<tr>
<td>15.3</td>
<td>Consistency Check</td>
<td>316</td>
</tr>
<tr>
<td>15.4</td>
<td>Generating a Test Plan</td>
<td>317</td>
</tr>
<tr>
<td>15.5</td>
<td>Creating a Compliance Folder</td>
<td>317</td>
</tr>
<tr>
<td>15.6</td>
<td>Qualification Testing</td>
<td>318</td>
</tr>
<tr>
<td>15.7</td>
<td>Qualify Your Design</td>
<td>319</td>
</tr>
<tr>
<td>15.8</td>
<td>Declaring Compliance</td>
<td>320</td>
</tr>
<tr>
<td>15.9</td>
<td>Listing</td>
<td>321</td>
</tr>
<tr>
<td>15.10</td>
<td>Combining Components</td>
<td>321</td>
</tr>
</tbody>
</table>

Index

323