



BLUETOOTH LOW ENERGY

THE DEVELOPER'S HANDBOOK

ROBIN HEYDON

FREE SAMPLE CHAPTER

SHARE WITH OTHERS



Bluetooth Low Energy

This page intentionally left blank

Bluetooth Low Energy

The Developer's Handbook

Robin Heydon



PRENTICE
HALL

Upper Saddle River, NJ • Boston • Indianapolis • San Francisco
New York • Toronto • Montreal • London • Munich • Paris • Madrid
Capetown • Sydney • Tokyo • Singapore • Mexico City

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 the publisher was aware of a trademark claim, the designations have been printed with initial capital letters or in all capitals.

The author and publisher have taken care in the preparation of this book, but make no expressed or implied warranty of any kind and assume no responsibility for errors or omissions. No liability is assumed for incidental or consequential damages in connection with or arising out of the use of the information or programs contained herein.

The publisher offers excellent discounts on this book when ordered in quantity for bulk purchases or special sales, which may include electronic versions and/or custom covers and content particular to your business, training goals, marketing focus, and branding interests. For more information, please contact:

U.S. Corporate and Government Sales
(800) 382-3419
corpsales@pearsontechgroup.com

For sales outside the United States please contact:

International Sales
international@pearson.com

Visit us on the Web: informit.com/ph

Cataloging-in-Publication Data is on file with the Library of Congress.

Copyright © 2013 Pearson Education, Inc.

All rights reserved. Printed in the United States of America. This publication is protected by copyright, and permission must be obtained from the publisher prior to any prohibited reproduction, storage in a retrieval system, or transmission in any form or by any means, electronic, mechanical, photocopying, recording, or likewise. To obtain permission to use material from this work, please submit a written request to Pearson Education, Inc., Permissions Department, One Lake Street, Upper Saddle River, New Jersey 07458, or you may fax your request to (201) 236-3290.

ISBN-13: 978-0-13-288836-3

ISBN-10: 0-13-288836-X

Text printed in the United States on recycled paper at RR Donnelley in Crawfordsville, Indiana.

First printing, October 2012

Executive Editor
Bernard Goodwin

Managing Editor
John Fuller

Project Editor
Elizabeth Ryan

Copy Editor
Bob Russell

Indexer
Jack Lewis

Proofreader
Christine Clark

Cover Designer
Gary Adair

Compositor
LaurelTech

This book is dedicated to Katherine.

—Robin xxx

This page intentionally left blank

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 3	Architecture	27
3.1	Controller	27
3.1.1	Physical Layer	28
3.1.2	Direct Test Mode	29
3.1.3	Link Layer	30
3.1.4	The Host/Controller Interface	31
3.2	The Host	32
3.2.1	Logical Link Control and Adaptation Protocol	32
3.2.2	The Security Manager Protocol	33
3.2.3	The Attribute Protocol	33
3.2.4	The Generic Attribute Profile	34
3.2.5	The Generic Access Profile	36
3.3	The Application Layer	36
3.3.1	Characteristics	36
3.3.2	Services	37
3.3.3	Profiles	37
3.4	Stack Splits	38
3.4.1	Single-Chip Solutions	38
3.4.2	Two-Chip Solutions	39
3.4.3	Three-Chip Solutions	40
Chapter 4	New Usage Models	41
4.1	Presence Detection	41
4.2	Broadcasting Data	42
4.3	Connectionless Model	43
4.4	Gateways	44
Part II	Controller	47
Chapter 5	The Physical Layer	49
5.1	Background	49
5.2	Analog Modulation	49
5.3	Digital Modulation	51
5.4	Frequency Band	54
5.5	Modulation	54
5.6	Radio Channels	55
5.7	Transmit Power	56
5.8	Tolerance	57

5.9	Receiver Sensitivity	57
5.10	Range	58
Chapter 6	Direct Test Mode	61
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	69
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	92
7.5.4	Discoverable Advertising	92
7.6	Broadcasting	92
7.7	Creating Connections	93
7.7.1	Access Address	95
7.7.2	CRC Initialization	95
7.7.3	Transmit Window	95
7.7.4	Connection Events	96
7.7.5	Channel Map	97
7.7.6	Sleep Clock Accuracy	98
7.8	Sending Data	98
7.8.1	Data Header	99
7.8.2	Logical Link Identifier	100
7.8.3	Sequence Numbers	101
7.8.4	Acknowledgement	101
7.8.5	More Data	101
7.8.6	Examples of the Use of Sequence Numbers and More Data	101
7.9	Encryption	104
7.9.1	AES	105
7.9.2	Encrypting Payload Data	106
7.9.3	Message Integrity Check	107
7.10	Managing Connections	109
7.10.1	Connection Parameter Update	109
7.10.2	Adaptive Frequency Hopping	111
7.10.3	Starting Encryption	112
7.10.4	Restarting Encryption	115
7.10.5	Version Exchange	117
7.10.6	Feature Exchange	118
7.10.7	Terminating Connections	118
7.11	Robustness	120
7.11.1	Adaptive Frequency Hopping	120
7.11.2	Strong CRCs	122
7.12	Optimizations for Low Power	123
7.12.1	Short Packets	124
7.12.2	High Bit Rate	125
7.12.3	Low Overhead	126
7.12.4	Acknowledgement Scheme	127
7.12.5	Single-Channel Connection Events	127

7.12.6	Subrating Connection Events	128
7.12.7	Offline Encryption	130
Chapter 8	The Host/Controller Interface	131
8.1	Introduction	131
8.2	Physical Interfaces	131
8.2.1	UART	132
8.2.2	3-Wire UART	132
8.2.3	USB	134
8.2.4	SDIO	134
8.3	Logical Interface	135
8.3.1	HCI Channels	135
8.3.2	Command Packets	135
8.3.3	Event Packets	137
8.3.4	Data Packets	138
8.3.5	Command Flow Control	139
8.3.6	Data Flow Control	140
8.4	Controller Setup	140
8.4.1	Reset the Controller to a Known State	141
8.4.2	Reading the Device Address	141
8.4.3	Set Event Masks	142
8.4.4	Read Buffer Sizes	142
8.4.5	Read Supported Features	143
8.4.6	Read Supported States	144
8.4.7	Random Numbers	145
8.4.8	Encrypting Data	145
8.4.9	Set Random Address	146
8.4.10	White Lists	147
8.5	Broadcasting and Observing	148
8.5.1	Advertising	148
8.5.2	Passive Scanning	150
8.5.3	Active Scanning	152
8.6	Initiating Connections	153
8.6.1	Initiating Connection to White List	154
8.6.2	Initiating a Connection to a Device	156
8.6.3	Canceling Initiating a Connection	156
8.7	Connection Management	158
8.7.1	Connection Update	158
8.7.2	Channel Map Update	159

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	244
11.1.7	Shared Secrets	244
11.2	Pairing and Bonding	248
11.2.1	Pairing	248
11.2.2	Exchange of Pairing Information	248
11.2.3	Authentication	250
11.2.4	Key Distribution	251
11.2.5	Bonding	252
11.3	Signing of Data	252
Chapter 12	The Generic Access Profile	255
12.1	Background	255
12.1.1	Initial Discovery	256
12.1.2	Establishing the Initial Connection	258
12.1.3	Service Characterization	258
12.1.4	Long-Term Relationships	259
12.1.5	Reconnections	260
12.1.6	Private Addresses	260
12.2	GAP Roles	261
12.3	Modes and Procedures	262
12.3.1	Broadcast Mode and Observation Procedure	263
12.3.2	Discoverability	263
12.3.3	Connectability	266
12.3.4	Bonding	270
12.4	Security Modes	270
12.4.1	Security Modes	271
12.5	Advertising Data	273
12.5.1	Flags	273
12.5.2	Service	274
12.5.3	Local Name	275
12.5.4	TX Power Level	275
12.5.5	Slave Connection Interval Range	275
12.5.6	Service Solicitation	275
12.5.7	Service Data	276
12.5.8	Manufacturer-Specific Data	276
12.6	GAP Service	276
12.6.1	The Device Name Characteristic	276
12.6.2	The Appearance Characteristic	276

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

14.8.4	Directed Advertising	307
14.8.5	Connected	307
14.8.6	Stay Connected or Disconnect	309
14.9	Optimizing Attributes	311
Chapter 15 Testing and Qualification		313
15.1	Starting a Project	313
15.2	Selecting Features	316
15.3	Consistency Check	316
15.4	Generating a Test Plan	317
15.5	Creating a Compliance Folder	317
15.6	Qualification Testing	318
15.7	Qualify Your Design	319
15.8	Declaring Compliance	320
15.9	Listing	321
15.10	Combining Components	321
Index		323

Preface

Sometimes, once in a lifetime, a new technology comes along that changes the world; for example, AM radio, television, and wireless Internet. Bluetooth low energy is at the cusp of the next revolution in wireless technology: a technology that can be embedded in products because it uses so little power that it can be designed around a small battery that lasts for years.

This book explains how this technology came about, why it was designed the way it has been designed, and how it works. It is written by one of the leading experts on Bluetooth low energy, Robin Heydon, who has been involved in creating the specifications, interoperability testing, and training.

This book is for anyone who is thinking about developing a product that incorporates Bluetooth low energy, whether you are an engineer, an application developer, a designer, or you're in marketing.

For engineers, the book covers the details of how the complete system works, from the physical radio waves up to the discovery of, connection with, and interface provided by that device.

For application developers, this book provides an understanding of the constraints imposed by Bluetooth low energy on applications. It also presents a thorough description of the design goals and implementation of these requirements.

For designers, the information contained herein will allow you to appreciate the particular problems with designing Bluetooth low energy wireless products, from how the product might need to work and how big a battery might be required to implement your ideas.

For everyone else, the book provides the background of why Bluetooth low energy was designed, the design goals it tried to achieve, and how you can take something that radically changes the way you can think of wireless technology and implement it in everything else.

The book is split into four parts:

Part I provides an overview of the technology, the basic concepts that guided the development of Bluetooth low energy, the architecture of the system from the radio through the various protocol layers up to the application layers, and finally, the new usage models that this new technology enables.

The second part goes into detail on how the radio chip—called a controller—functions. This is the silicon chip that product designers need to incorporate into

their end products. This part also covers the radio, Direct Test Mode, and the Link Layer. In addition, it shows how to interact with the controller from the upper-layer stack, called a host.

Part III goes into detail of how the host (the software stack) works. It covers the concepts and details behind the main protocol used to expose attributes of a device. It also covers the security models and how to make connections and bonds, or associate, two devices with one another.

In Part IV, you wrap up all the details by looking at the design considerations that a product or application developer needs to consider. It starts by looking at the issues involving central devices. Next, it looks at issues related to peripheral devices. Finally, it considers the entire problem surrounding testing and qualification, typically the final part of any product that will be taken to market.

If after reading the book you would like to learn more about Bluetooth low energy, there are a number of resources available. The specifications themselves are available on the Bluetooth SIG website at www.bluetooth.org. If you would like to find developer information about Bluetooth low energy, there is also a developer site available at developer.bluetooth.org that has detailed information about characteristics. The author also has a website at www.37channels.com, where you can view frequently asked questions raised by this book and Bluetooth low energy.

Acknowledgments

I would like to thank the following people for their invaluable help in making this book possible. Katherine Heydon, for reading the whole book cover to cover many times and providing constructive criticism on the contents. Jennifer Bray for her encouragement to write the book in the first place and allowing me the time and space to undertake such a task. All the production team at Addison-Wesley, especially Bernard Goodwin, Elizabeth Ryan, Michelle Housley and Gary Adair; my copy editor, Bob Russell; and all the others in the background who made this book happen. Nick Hunn for the many times spent discussing the best way to communicate the ideas behind the low energy technology. Zoë Hunn for the fantastic artwork on the front cover. Andy Glass for constantly asking (nagging?) about when the book would be done and providing excellent review comments. Steve Wenham, who suffered my constant ideas about how low energy could be made better. British Airways, for almost always giving me a front row bulkhead seat and allowing me to use my Bluetooth keyboard and mouse on the many long-haul flights. This book was probably written at an average height of 30,000 feet. For the Bluetooth SIG community in general, for the many questions that they asked at All Hands Meetings, UnPlugFests, and all the various working group meetings: these questions helped determine what were the hardest concepts to explain, and therefore the basic structure and contents of this book.

This page intentionally left blank

About the Author



Robin Heydon was educated as a software engineer, graduating with a degree in Computer Science from the University of Manchester, UK. He was employed in the computer entertainment industry for a decade working on networked flight simulators. He then moved into wireless communications in 2000, working for what was then a small company called CSR. There he moved from being a firmware engineer to working as a full-time standards architect. In this work, Robin has worked on fixing and improving all versions of the Bluetooth specification. In

early 2007, Robin started working on a project called Wibree, which later became the Bluetooth low energy specification. He cochaired the group, and drove through the specification to publication, and was recognized by the Bluetooth SIG as an inductee to the Bluetooth SIG Hall of Fame in 2010.

This page intentionally left blank

Chapter 1

What Is Bluetooth Low Energy?

*If I have seen a little further,
it is by standing on the shoulders of Giants.*
—Isaac Newton

Bluetooth low energy is a brand new technology that has been designed as both a complementary technology to classic Bluetooth as well as the lowest possible power wireless technology that can be designed and built. Although it uses the Bluetooth brand and borrows a lot of technology from its parent, Bluetooth low energy should be considered a different technology, addressing different design goals and different market segments.

Classic Bluetooth was designed to unite the separate worlds of computing and communications, linking cell phones to laptops. However its killer application has proved to be as an audio link from the cell phone to a headset placed on or around the ear. As the technology matured, more and more use cases were added, including stereo music streaming, phone book downloads from the phone to your car, wireless printing, and file transfer. Each of these new use cases required more bandwidth, and therefore, faster and faster radios have been constantly added to the Bluetooth ecosystem over time. Bluetooth started with Basic Rate (BR) with a maximum Physical Layer data rate of 1 megabit per second (Mbps). Enhanced Data Rate (EDR) was added in version 2.0 of Bluetooth to increase the Physical Layer data rates to 3Mbps; an Alternate MAC¹ PHY² (AMP) was added in version 3.0 of Bluetooth that used IEEE³ 802.11 to deliver Physical Layer data rates of up to hundreds of megabits per second.

Bluetooth low energy takes a completely different direction. Instead of just increasing the data rates available, it has been optimized for ultra-low power consumption. This means that you probably won't get high data rates, or even want to keep a connection up for many hours or days. This is an interesting move,

1. MAC stands for Medium Access Control. How a transceiver uses a Physical Layer to communicate with other transceivers.

2. PHY stands for Physical Layer.

3. IEEE stands for the Institute of Electrical and Electronics Engineers.

Table 1–1 Speeds Almost Always Increase

Modems	Ethernet
V.21: 0.3kbps	802.3i: 10Mbps
V.22: 1.2kbps	802.3u: 100Mbps
V.32: 9.6kbps	802.3ab: 1000Mbps
V.34: 28.8kbps	802.3an: 10000Mbps
Wi-Fi	Bluetooth
802.11: 2Mbps	v1.1: 1Mbps
802.11b: 11Mbps	v2.0: 3Mbps
802.11g: 54Mbps	v3.0: 54Mbps
802.11n: 135Mbps	v4.0: 0.3Mbps

as most wired and wireless communications technologies constantly increase speeds, as illustrated in Table 1–1.

This different direction has been achieved through the understanding that classic Bluetooth technology cannot achieve the low power requirements required for devices powered by button-cell batteries. However, to fully understand the requirements around low power, another consideration must be taken. Bluetooth low energy is also designed to be deployed in extremely high volumes, in devices that today do not have any wireless technology. One method to achieve very high volumes is to be extremely low cost. For example, Radio frequency identification (RFID) tags can be deployed in very high volumes because they are very low cost, ultimately because they work by scavenging power delivered by a more expensive scanner.

Therefore, it is crucial to also look at the Bluetooth low energy system design from the requirements of low cost. Three key elements within this design point to very low cost:

1. ISM Band

The 2.4GHz ISM band is a terrible place to design and use a wireless technology. It has poor propagation characteristics, with the radio energy readily being absorbed by everything, but especially by water; consider that the human body is made up primarily of water. These rather significant downsides are made up by the fact that the radio spectrum is available worldwide and there are no license requirements. Of course, this Free Rent sign means that other technologies are also going to use this space, including most Wi-Fi radios. But the lack of licensing doesn't mean that anything goes. There are still plenty of rules, mainly related to limiting the power output of devices that use the spectrum,

limiting the range. However, these limitations are still more attractive than paying heavily for licensed spectrum. Therefore, choosing to use the ISM band lowers the cost.

2. IP License

When the Wibree technology was mature enough to be merged into an established wireless standards group, Nokia could have taken the technology to any such group. For example, it could have taken it to the Wi-Fi Alliance, which also standardizes technology in the same 2.4GHz ISM band. But they chose the Bluetooth Special Interest Group (SIG) because of the excellent reputation and licensing policy that this organization has. These policies basically mean that the patent licensing costs are significantly reduced for a Bluetooth device when compared with a technology developed in another SIG or association that has a FRAND⁴ policy. Because Bluetooth has a very low license costs, the cost per device is also significantly reduced.

3. Low Power

The best way to design a low-cost device is to reduce the materials required to make such a device—materials such as batteries. The larger the battery, the larger the battery casing needs to be, again increasing the costs. Replacing a battery costs money, not just for a consumer who needs to purchase another battery, but replacement also includes the opportunity costs of not having that device available. If this device is maintained by a third party, perhaps because it is part of a managed home alarm system, there are additional labor costs to change this battery. Therefore, designing the technology around low power consumption also reduces the costs. As a thought experiment, how would things be different if a megawatt battery were available for a single penny?

Many devices could accommodate a larger battery. A keyboard or mouse can easily take AA batteries, yet the manufacturers want to use AAA batteries not because they are smaller, but because their use reduces the bill of materials and therefore the cost of the device.

Therefore, the fundamental design for low energy is to work with button-cell batteries—the smallest, cheapest, and most readily available type of battery available. This means that you cannot achieve high data rates or make low energy work for use cases that require large data transfers or the streaming of data. This single point

4. FRAND stands for Fair, Reasonable, and Non-Discriminatory. This means that if you license your technology, you must do it at a fair price, on the same terms for everybody, regardless of who the licensee is.

is probably the most important difference between classic and low-energy variants of Bluetooth. This is discussed further in the next section.

1.1 Device Types

Bluetooth low energy makes it possible to build two types of devices: dual-mode and single-mode devices. A dual-mode device is a Bluetooth device that has support for both Bluetooth classic as well as Bluetooth low energy. A single-mode device is a Bluetooth device that only supports Bluetooth low energy. There is a third type of device, which is a Bluetooth classic-only device.

Because it supports Bluetooth classic, a dual-mode device can talk with the billions of existing Bluetooth devices. Dual-mode devices are new. They require new hardware and firmware in the controller and software in the host. It is therefore not possible to take an existing Bluetooth classic controller or host and upgrade it to support low energy. However, most dual-mode controllers are simple replacement parts for existing Bluetooth classic controllers. This allows designers of cell phones, computers, and other device to replace their existing Bluetooth classic controllers with dual-mode controllers very quickly.

Because it does not support Bluetooth classic, a Bluetooth low energy single-mode device cannot talk with the existing Bluetooth devices, but it can still talk with other single-mode devices as well as dual-mode devices. These new single-mode devices are highly optimized for ultra-low power consumption, being designed to go into components that are powered by button-cell batteries. Single-mode devices will also not be able to be used in most of the use cases for which Bluetooth classic is used today because single-mode Bluetooth low energy does not support audio for headsets and stereo music or high data rates for file transfers.

Table 1–2 shows what device types can talk with other devices types and what Bluetooth radio technology would be used when they connect. Single-mode devices will talk with other single-mode devices using low energy. Single-mode devices will also talk with dual-mode devices using low energy. Dual-mode devices will talk with other dual-mode devices or classic devices using BR/EDR. A single-mode device cannot talk with a classic device.

Table 1–2 Single-Mode, Dual-Mode, and Classic Compatibility

	Single-Mode	Dual-Mode	Classic
Single-Mode	LE	LE	none
Dual-Mode	LE	Classic	Classic
Classic	none	Classic	Classic

1.2 Design Goals

When reviewing any technology, the first question to be asked is how did the designers optimize this technology? Most technologies have one or two things that they are very good at, and many things that they are not. By determining what these one or two things are, a greater understanding of that technology can be achieved.

With Bluetooth low energy, this is very simple. It was designed for ultra-low power consumption. The unique structure of the Bluetooth SIG is that the organization creates and controls everything from the Physical Layer up to the application. The SIG does this in a cooperative and open but commercially driven standards model, and over more than ten years, it has optimized the process of creating wireless specifications that not only work at the point of release but are also interoperable, robust, and of extremely high quality.

When the low energy work started, the goal was to create the lowest-power short-range wireless technology possible. To do this, each layer of the architecture has been optimized to reduce the power consumption required to perform a given task. For example, the Physical Layer's relaxation of the radio parameters, when compared with a Bluetooth classic radio, means that the radio can use less power when transmitting or receiving data. The link layer is optimized for very rapid reconnections and the efficient broadcast of data so that connections may not even be needed. The protocols in the host are optimized to reduce the time required once a link layer connection has been made until the application data can be sent. All of this is possible only when all parts of the system are designed at the same time by the same group of people.

The design goals for the original Bluetooth radio have not been forgotten. These include the following:

- Worldwide operation
- Low cost
- Robust
- Short range
- Low power

For global operation, a wireless band that is available worldwide is required. There is only one available band that can be implemented using low-cost and high-volume manufacturing technology today: the 2.45GHz band. This is available because it is of no interest to astronomers, cell phone operators, or other commercial interests. Unfortunately, just like everything that is free, everybody wants to be part of it,

causing congestion. Other wireless bands are available, for example, the 60GHz ISM band, but this is not practical from a low-cost point of view, or the 800/900MHz bands that have different frequencies and rules depending on where you are on the planet.

The design goal of low cost is interesting because it implies that the system should be kept as small and efficient as possible. Although it could be possible, for example, to add scatter net support or full-mesh networking into Bluetooth low energy, this would increase the cost because more memory and processing power would be required to maintain this network. The system has therefore been optimized for low cost above interesting research-based networking topologies.

The 2.45GHz band that Bluetooth low energy uses is already very crowded. Just taking into account standards-based technologies, it includes Bluetooth classic, Bluetooth low energy, IEEE 802.11, IEEE 802.11b, IEEE 802.11g, IEEE 802.11n, and IEEE 802.15.4. In addition, a number of proprietary radios are also using the band, including X10 video repeaters, wireless alarms, keyboards, and mice. A number of devices also emit noise in the band, such as street lights and microwave ovens.

It is therefore almost impossible to design a radio that will work at all times with all possible interferers, unless it uses *adaptive frequency hopping*, as pioneered by Bluetooth classic. Adaptive frequency hopping helps by not only detecting sources of interference quickly but also by adaptively avoiding them in the future. It also quickly recovers from the inevitable dropped packets caused by interference from other radios. It is this robustness that is absolutely key to the success of any wireless technology in the most congested radio spectrum available.

Robustness also covers the ability to detect and recover from bit errors caused by background noise. Most short-range wireless standards compromise by using a short cyclic redundancy check (CRC), although there are some that use very long checks. A good design will see compromise between the strength of the checks and the time taken to send this information.

Short range is actually a slight problem. If you want a low-power system, you must keep the transmitted power as low as possible to reduce the energy used to transmit the signal. Similarly, you must keep the receiver sensitivity fairly high to reduce the power required to pick up the radio signals of other devices from amongst the noise. What short range means in this context is really that it is not centered around a cellular base station system. Short range means that Bluetooth low energy should be a *personal area network*.

The original Bluetooth design goal of low power hasn't changed that much, except that the design goals for power consumption have been reduced by one or two orders of magnitude. Bluetooth classic had a design goal of a few days standby and a few hours talk time for a headset, whereas Bluetooth low energy has a design goal of a few years for a sensor measuring the temperature or measuring how far you've walked.

1.3 Terminology

Just like many high technology areas, the people working in Bluetooth low energy use their own language to describe the features and technology with the specification. This section enumerates each of the words that have special meaning and what they mean.

Adaptive Frequency Hopping (AFH) A technology whereby only a subset of frequencies is used. This allows devices to avoid the frequencies that other non-adaptive technologies are using (e.g., a Wi-Fi access point).

Architecture The design of the Bluetooth low energy is sometimes known as the Architecture.

Band See Radio Band.

Frequency Hopping The use of multiple frequencies to communicate between two devices. One frequency is used at a time, and each frequency is used in a defined sequence.

Layer A part of the system that fulfills a specific function. For example, the Physical Layer covers the operation of the radio. Each layer in a system is abstracted away from the layers above and below it. The Link Layer doesn't need to know all the details of how the radio functions; the Logical Link Control Layer and Adaptation Layer don't need to know all the details of how the Link Layer works. This abstraction is important to keep the complexity of the system at manageable levels.

Master A complex device that coordinates the activity of other devices within a piconet.

Piconet This is a contraction of the words pico and network. Pico is the SI⁵ prefix for 10^{-12} . This is derived from the Italian *piccolo*, meaning small.⁶ Therefore, a piconet is a very small network. A piconet has a single master device that coordinates the activity of all the other devices (slaves) in the piconet and one or more slaves.

Radio Band Radio waves are defined by their frequency or wavelength. Different radio waves are then allocated different rules and uses. When a range of radio

5. SI stands for *Système International* (or *International System* in English), which is a system of standardized unit designations, typically in relation to scientific, engineering, and technical measurements such as seconds, meters, kilograms, and so on.

6. <http://www.industrie.gouv.fr/metro/aquosert/etymol.htm>

frequencies are grouped together using the same rules, this group of frequencies is called a Radio Band.

Slave A simple device that works with a master. These devices are typically single-purpose devices.

Wi-Fi A complementary wireless technology that is designed for high data rates to connect computers and other very complex devices with the Internet.

Index

Numbers

- 2.4GHz ISM band
 - Bluetooth low energy using, 4–5
 - overview of, 54
 - at Physical Layer, 29
 - transmit power, 56–57
- 3-Wire UART, HCI physical interface, 132–134
- 24-bit CRC, Bluetooth low energy. *see* CRC (cyclic redundancy check)
- 32-bit MIC, Bluetooth low energy. *see* MIC (message integrity check)
- 128-bit UUIDs (Bluetooth Base UUIDs), 190–191
- 10101010 packet sequence, transmitter tests, 63–64
- 11110000 packet sequence, transmitter tests, 63–64

A

- Abstract state, 182–183
- Abstraction, service-oriented architecture, 23
- Access address
 - Link Layer connections, 95
 - packet structure, 30–31, 80–81
 - test packet format, 63
- Access permissions, attribute database, 194
- Acknowledgement
 - of data packet, 101
 - optimizing for low power, 127
- Action, requesting for command packets, 136
- Active scanning
 - in device discovery procedure, 257, 283–285
 - HCI, 152–153
 - Link Layer state machine, 72
 - overview of, 72
 - receiving broadcast data, 93
- Active state mode, 3-Wire UART, 63–64, 133
- Adaptive frequency hopping
 - Bluetooth low energy design, 8
 - channel map, 97–98
 - data channels used with, 30
 - defined, 9
 - Link Layer connection process, 93–94, 97–98, 111–112
 - Link Layer robustness, 120–122
 - managed by master, 14
 - optimizations for low power, 127
 - overview of, 88–89
- ADV_DIRECT_IND advertising packets, 81–82, 266–267
- ADV_IND advertising packets, 81–82, 267
- ADV_NONCONN_IND advertising packets, 82, 266
- ADV_SCAN_IND advertising packets, 82, 266
- Advanced Encryption System. *see* AES (Advanced Encryption System)
- Advertisers, defined, 14–15
- Advertising
 - access address, packet structure, 80–81
 - broadcasting data with, 42–43
 - data, 273
 - events, 90–92
 - formatting data when broadcasting, 263
 - Host/Controller Interface, 148–150
 - initial discovery using devices for, 256–257
 - interval, 90
 - presence detection using, 41–42
- Advertising channels
 - access addresses for, 80–81
 - advertising packets as transmitted on, 76
 - in connection state, 74
 - finding devices with, 90
 - in Link Layer, 30–31
 - overview of, 84–87
 - reducing number to reduce power
 - consumption, 70
 - in scanning state, 72
 - used by devices in broadcast mode, 263
- Advertising packets
 - broadcasting data with, 93, 148–150
 - finding devices, 90–92

- Advertising packets (*continued*)
 - GAP connection modes, 266–267
 - GAP connection procedures, 268–269
 - HCI connections to white lists, 155
 - header contents, 81–82
 - length field, 83
 - overview of, 76
 - peripheral connectability, 300–301
- Advertising state
 - entering connection state from, 73
 - entering slave substate from, 74
 - nonconnectable advertising device in, 92
 - optimizing peripherals for low power, 304–306
 - overview of, 71
- AES (Advanced Encryption System)
 - calculating MIC, 107–109
 - HCI controller setup, 145–146
 - overview of, 105–106
 - security features, 244
 - starting encryption for connections, 114
- AFH. *see* adaptive frequency hopping
- Alert Level characteristic, 288–290
- Algorithms, scheduling, 75
- Alternate MAC PHY (AMP), Bluetooth version 3.0, 3
- AM (amplitude modulation) radio, 50–51
- AMP (Alternate MAC PHY), Bluetooth version 3.0, 3
- Amplitude modulation (AM) radio, 50–51
- Amplitude-shift keying (ASK), digital modulation, 52
- Analog modulation, 49–51
- Appearance characteristic, GAP Service, 276–277, 284
- Application data rate, radio systems, 51
- Application Errors response, 231
- Application layer architecture
 - characteristics, 36–37
 - defined, 36
 - profiles, 37–38
 - services, 37
 - three-chip solution, 39–40
 - two-chip solution, 39–40
- Architectural paradigms, concepts, 20–25
- Architecture
 - application layer, 36–38
 - Bluetooth, 27–28
 - Bluetooth low energy design as, 9
 - controller, 27–31
 - host, 32–36
 - stack splits, 38–40
- ASK (amplitude-shift keying), digital modulation, 52
- Assembly, by multiplexing layers, 170
- Asymmetric design concept, 14–15
- ATM networks, as multiplexing layers, 170
- Atomic operations and transactions, 197–198
- Atomic services, 34
- Attribute database
 - accessing attributes, 196–197
 - exposing services to peripherals, 301–302
 - overview of, 192–193
 - permissions, 194–195
- Attribute handles
 - Find By Type Value Request/response, 222–223
 - Find Information Request/response, 221–222
 - Invalid Handle error, 228–229
 - overview of, 189–190
 - Read By Type Request/response, 223
 - Read Request including, 224
- Attribute Not Found error, 230
- Attribute Not Long error, 230
- Attribute Profile, 199
- Attribute Protocol
 - attribute client using, 192
 - Bluetooth low memory using only, 14
 - channel identifier for, 172
 - control points, 183
 - creation of, 179
 - error responses, 228–231
 - Exchange MTU Request, 221
 - exposing state with, 16–17
 - Find By Type Value Request, 222–223
 - Find Information Request, 221–222
 - Generic Attribute Profile vs., 231
 - Handle Value Indication, 228
 - Handle Value Notification, 227–228
 - host architecture, 33–34
 - overview of, 217–219
 - Prepare Write Request and Execute Write Request, 226–227
 - protocol messages, 219–220
 - Read Blob Request, 224
 - Read By Group Type Request, 225
 - Read By Type Request, 223
 - Read Multiple Request, 224
 - Read Request, 224
 - in service-oriented architecture, 25

- Signed Write Command, 225–226
- state machines, 183–185
- Write Command, 225
- Write Request, 225
- Attribute Protocol Layer
 - asymmetric design at, 14–15
 - security protection at, 16
- Attribute types
 - Find By Type Value Request/response, 222–223
 - Find Information Request/response, 221–222
 - fundamental, 192
 - overview of, 190–191
 - Unsupported Group Type error, 231
- Attribute value(s)
 - attribute permissions applying to, 194
 - Characteristic Descriptor, 192
 - Characteristic Type UUID, 192
 - Find By Type Value Request/response, 222–223
 - Handle Value Indication, 228
 - Handle Value Notification, 227–228
 - Invalid Attribute Value Length error, 230
 - overview of, 191
 - Prepare Write Request and Execute Write Request, 226–227
 - Read Blob Request, 224
 - Read By Type Request/response, 223
 - Read Multiple Request, 224
 - service UUIDs, 191
 - units, 191
- Attributes
 - accessing, 196–197
 - atomic operations and transactions, 197–198
 - attribute handle, 189–190
 - Attribute Protocol. *see* Attribute Protocol
 - attribute type, 190–191
 - attribute value, 191–193
 - characteristics, 210–217
 - grouping, 199
 - overview of, 179
 - peripheral design optimizing, 311–312
 - permissions, 194–195
 - structure of, 189
- Attributes, background to
 - data, data, everywhere. and, 180–181
 - data and state, 181–182
 - kinds of state, 182–183
 - protocol proliferation is wrong, 180

- services and profiles, 185–189
- state machines, 183–185
- Attributes, services
 - combining services, 204–205
 - extending services, 201–203
 - including services, 209–210
 - overview of, 199–201
 - plug-and-play client applications, 207–208
 - primary or secondary, 205–207
 - reusing another service, 203–204
 - service declaration, 208–209
- Authentication
 - attribute database permissions as, 194–195
 - authorization vs., 195
 - Bluetooth low energy and, 115
 - in bonding process, 259
 - central devices initiating bonding via, 292–293
 - concept of, 241–242
 - data channel, 30
 - encrypted packet, 104
 - Insufficient Authentication error, 229
 - integrity via, 243
 - pairing procedure, 250–251
 - resolving signatures for, 225–226, 247
- Authorization
 - Insufficient Authorization error, 229
 - security and, 242–243
- Authorization permissions, attribute
 - database, 195
- Auto-connection establishment procedure,
 - GAP, 267–268
- Autonomy, service-oriented architecture, 24
- Ax encryption blocks, encrypting payload
 - data, 106

B

- Bandwidth, classic Bluetooth and, 3
- Basic Rate (BR), original Bluetooth, 3
- Batteries
 - lowering cost with button-cell, 5–6
 - monitoring in connectionless model, 44
- Behavior
 - application layer services and, 37
 - combining services, 204–205
 - extending services, 201–203
 - primary vs. secondary services and, 205–207
 - profiles and, 37–38, 185
 - reusing another service and, 203–204
 - service characteristics and, 200–201
 - services and, 34–36

- BER (bit error rate), receiver sensitivity, 58
- B-frame format, 32
- Binary FSK (frequency-shift keying), digital modulation, 52
- Bit error rate (BER), receiver sensitivity, 58
- Bit errors
 - CRC detecting odd numbers of, 84
 - protection against, 16
- Bit order
 - access address and, 80–81
 - packet structure and, 79
 - preamble and, 79–80
- Bit rate, optimizing for low power, 125–126
- Bits, defined, 51
- Block counter, encrypting payload data, 106–107
- Bluetooth classic, fixed and
 - connection-oriented channels, 170–171
- Bluetooth classic vs. low energy
 - compatibility with device types, 6
 - connectionless model, 43–44
 - overview of, 3–4
 - power consumption, 8
 - services and profiles, 185–189
- Bluetooth low energy, overview
 - concepts. *see* concepts
 - design goals, 4, 7–8
 - device types, 6
 - low cost of, 4–5
 - single-mode devices, 3–4
 - terminology, 9–10
- Bluetooth Qualification Administrator (BQA), 317
- Bondable mode, GAP, 270
- Bondable procedure, GAP, 270
- Bonding
 - central devices using, 292–293
 - controlling connectability of peripherals, 301
 - GAP defining device, 36
 - long-term relationships and, 259
 - modes and procedures for, 270
 - optimizing peripherals for low power, 304–306
 - profile security, 296–297
- BQA (Bluetooth Qualification Administrator), 317
- BR (Basic Rate), original Bluetooth, 3
- BR/EDR Not Supported flag, advertising data, 274

- Broadcast Flag, HCI data packets, 138–139
- Broadcaster role, GAP, 261
- Broadcasting data
 - advertising state for, 71
 - HCI, 148–153
 - new wireless model for, 42–43
 - overview of, 92–93
 - Server Characteristic Configuration
 - Descriptor for, 214–215
- Broadcasting model
 - active scanning, 152–153
 - advertising, 148–150
 - defined, 148
 - passive scanning, 150–152
 - peripherals that only broadcast, 299–300
- Brute-force checking, private addresses, 261
- Buffer sizes, HCI controller setup, 142–143
- Bulk data USB packets, HCI, 134
- Button-cell batteries
 - concept of, 11–12
 - lowering cost of Bluetooth low energy, 5–6
 - short duration bursts of, 13
 - single-mode devices designed for, 6
- Bytes, packet structure, 79

C

- Calibration, of controller in Direct Test Mode, 62
- Categories, of qualification tests, 318–319
- CCM (Counter with Cipher Block Chaining-Message Authentication Code Mode), 106
- Cell phones
 - dual-mode controllers for, 6
 - marketing concept for, 19
 - two-chip solutions on, 39–40
- Central devices
 - background of, 283
 - bonding, 292–293
 - building generic clients, 287–288
 - changing services, 293–294
 - connecting to devices, 285–286
 - controlling connectability of peripherals, 301
 - discoverability of peripherals, 283–285, 301
 - implementing profiles, 294–297
 - interacting with services, 288–292
 - understanding, 286
- Central role, GAP, 262
- Changed services, central devices, 293–294
- Channel identifiers, L2CAP, 172–173

- Channel map
 - HCI advertising, 150
 - HCI connection management, 159–160
 - Link Layer, 85
 - Link Layer connection process, 97–98
- Channel map, adaptive frequency hopping
 - Link Layer connections, 94, 97–98, 111–112
 - Link Layer robustness, 120–122
 - overview of, 88–89
- Channels
 - Bluetooth classic using narrow, 55
 - Bluetooth low energy using radio, 56
 - HCI interface, 135
 - L2CAP. *see* L2CAP (Logical Link Control and Adaptation Protocol)
 - UART transport, 132–133
- Channels, Link Layer
 - adaptive frequency hopping, 88–89
 - determining advertising vs. data packets, 76
 - frequency hopping, 87
 - overview of, 30–31, 84–85
 - understanding, 84–87
- Characteristic Aggregation Format
 - Descriptor, 217
- Characteristic Descriptors, attribute value, 192
- Characteristic Extended Properties
 - Descriptor, 214
- Characteristic Presentation Format
 - Descriptor, 215–217, 287
- Characteristic Type UUID, 192
- Characteristic User Description descriptor, 214
- Characteristic Value Reliable Writes
 - procedure, 237
- Characteristic(s)
 - application layer, 36–37
 - central device discovery, 286
 - central device interaction with services, 288–289
 - combining services, 204–205
 - declaration of, 211–213
 - descriptors on, 214–217
 - discovering with Read By Type Request, 223
 - discovery and configuration of services, 258–259
 - discovery on initial connection, 258
 - exposing services to peripherals, 302–303
 - extending services, 201–203
 - GATT client-initiated procedures for, 235–238
 - GATT discovery procedures for, 234–235
 - grouping, 199
 - optimizing peripheral attributes, 310–311
 - overview of, 210–211
 - peripheral devices, 302–303
 - primary vs. secondary services, 205–207
 - profiles discovering and using, 296
 - reusing another service, 203–204
 - services as grouping of, 37, 199–200
 - value of, 213
- Chips, defined, 51
- Ciphertext, encryption text, 105
- Classes, object-oriented programming, 199–200
- Clear to send (CTS), 5-wire UART transport, 132
- Client Characteristic Configuration
 - Descriptor
 - notifications and indications, 292
 - overview of, 214
 - profiles, 296
- Client Preferred Connection Parameters
 - characteristic, 285–286
- Client-initiated procedures, GATT
 - overview of, 235
 - reading characteristic values, 235–236
 - reading/writing characteristic descriptors, 238
 - writing characteristic values, 236–238
- Clients, building generic, 287–288
- Client-server architecture
 - asymmetric design of, 14–15
 - attribute database and, 192–193
 - attribute permissions, 194–195
 - Attribute Protocol messages, 33
 - concept of, 17–18
 - data concept, 181–182
 - as paradigm for Bluetooth low energy, 20–21
 - profiles and services in, 186–189
 - state-based model for, 17
- Clock accuracy, Link Layer connection process, 98
- CMAC algorithm, signing of data, 252
- CMOS (Complimentary Metal on Silicon), 124–125
- Command Complete event, HCI
 - channel map update, 159
 - command flow control, 139–140
 - encryption, 145–146
 - event packets, 137–138

- Command Complete event, HCI (*continued*)
 - reading device address, 141–142
 - reading supported features, 143–144
 - reading supported states, 144–145
 - resetting controller to known state, 141
 - setting random address, 147
 - white lists, 147
- Command flow control, HCI, 139–140
- Command not understood reason code,
 - command reject command, 174–175
- Command packets, HCI, 135–137
- Command reject command, LE signaling
 - channel, 174–175
- Command Status event
 - enabling command flow control, 139–140
 - encrypting data packets while connected, 161–162
 - HCI event packets, 138
 - HCI feature exchange, 160
- Commands
 - Attribute Protocol, 218–219
 - connection, 137
 - controller state, 136
 - Direct Test Mode, 65–68
 - as exceptions to transaction rules, 197
 - requesting specific action, 136
- Company identifier, version information, 118
- Compliance folder, testing and qualification, 317–318
- Complimentary Metal on Silicon (CMOS), 124–125
- Component subsystem product type, 315–316
- Composability, service-oriented architecture, 24
- Concepts
 - architectural paradigms, 20–25
 - asymmetric design, 14–15
 - button-cell batteries, 11–12
 - client-server architecture, 17–18
 - connectionless model, 19–20
 - design for success, 15–16
 - everything has state, 16–17
 - memory is expensive, 13–14
 - modular architecture, 18–19
 - one billion is a small number, 19
 - targeting new market segments, 11
 - time is energy, 12–13
- Confidentiality
 - ensuring with encryption, 104
 - security concept of, 243
- CONNECT_REQ, advertising packet, 82
- Connectable advertising state, peripherals, 304–307
- Connectable directed advertising, 149
- Connectable modes, GAP
 - direct-connectable, 266–267
 - nonconnectable, 266
 - overview of, 266
 - undirected-connectable, 267
- Connectable undirected advertising, 148
- Connection events
 - determining instant by counting, 112
 - Link Layer connection process, 96–97
 - optimizing for low power by subrating, 128–130
 - optimizing for low power with single-channel, 127–128
 - sleep clock accuracy in connection process, 98
- Connection handle
 - controlling connections with, 137
 - HCI interface, 135
 - labeling HCI data packets with, 138–139
 - LE Connection Complete event, 155
- Connection interval, optimizing peripherals, 308–309
- Connection management. *see* HCI connection management
- Connection parameter update request
 - command, LE signaling channel, 175–177
- Connection parameter updates, Link Layer, 109–111
- Connection Signature Resolving Key. *see* CSRK (Connection Signature Resolving Key)
- Connection state, Link Layer state machine, 73–74
- Connectionless model
 - achieving with L2CAP layer for. *see* L2CAP (Logical Link Control and Adaptation Protocol)
 - new wireless model enabling, 43–44
 - overview of, 19–20
- Connection-oriented model
 - channel identifiers for, 172
 - connectionless model vs., 43–44
 - Internet built around, 45
- Connections
 - controlling, 137
 - establishing initial device, 258

- initiating from central devices, 285–286
 - peripheral devices, 301
 - reconnected, 260
 - Connections, creating at Link Layer
 - access address, 95
 - channel map, 97–98
 - connection events, 96–97
 - CRC initialization, 95
 - initiating state for, 72
 - overview of, 30–31
 - sleep clock accuracy, 98
 - transmit window, 95–96
 - understanding, 93–94
 - Connections, initiating in HCI
 - canceling, 156–157
 - HCI initiating connections to devices, 156
 - overview of, 153–154
 - to white list, 154–155
 - Connections, managing Link Layer
 - adaptive frequency hopping, 111–112
 - connection parameter update, 109–111
 - feature exchange, 118
 - offline encryption, 130
 - overview of, 109
 - restarting encryption, 115–116
 - starting encryption, 112–115
 - terminate procedure, 118–119
 - version exchange, 117–118
 - Connections, optimizing peripherals for low power
 - bonding, 306
 - connectable advertising, 306–307
 - connected, 307–309
 - directed advertising, 307
 - discoverable advertising, 305
 - overview of, 303–305
 - stay connected or disconnect, 309–310
 - Consistency check, starting new project, 316–317
 - Continuation messages, LLID, 100–101
 - Control endpoint, USB interface in HCI, 134
 - Control points, Attribute Protocol
 - central devices interacting with services, 289–290
 - characteristics, 303
 - defined, 183
 - state machine, 183–185, 290–291
 - Controller
 - configuring state of, 136
 - device density design, 16
 - Direct Test Mode, 29–30
 - dual-mode, 6
 - HCI. *see* HCI (Host/Controller Interface)
 - Link Layer. *see* Link Layer
 - overview of, 27–28
 - Physical Layer. *see* Physical Layer
 - three-chip solution, 39–40
 - two-chip solution, 39–40
 - Controller subsystem product type, 315–316
 - Correlation of access address, 80–81
 - Cost
 - design goal of low, 7–8
 - designing Bluetooth low energy for low, 4–6
 - memory is expensive concept, 13–14
 - one billion is a small number concept, 19
 - Counter with Cipher Block Chaining-Message Authentication Code Mode (CCM), 106
 - CR2032 button-cell batteries, 11–12
 - CRC (cyclic redundancy check)
 - 3-Wire UARTs in HCI, 133
 - bit errors and, 16
 - calculating MIC, 107–109
 - Link Layer connection process, 95
 - Link Layer robustness with strong, 122–123
 - overview of, 84
 - packet structure, 30–31, 84
 - Prepare/Execute Writes and, 198
 - Prepare Write Request and, 227
 - short range wireless standards, 8
 - too weak to be security measure, 243
 - Create New Project page, bluetooth.org, 315
 - CSRK (Connection Signature Resolving Key)
 - key distribution during pairing, 251
 - long-term relationships, 259
 - message authentication code, 226
 - overview of, 247
 - private addresses, 261
 - signing of data, 252
 - CTS (clear to send), 5-wire UART transport, 132
 - Current time, peripherals that only broadcast, 300
- ## D
- Data
 - packet structure, 30–31
 - state vs., 181–182
 - text packets transmitting, 63–64
 - types in Bluetooth low energy devices, 180–181

- Data access address, packet structure, 80–81
- Data channels
 - adaptive frequency hopping, 88–89
 - frequency hopping over time, 87
 - Link Layer and, 30–31
 - placing, 84–87
- Data flow control, HCI interface, 140
- Data packets
 - HCI interface, 138–139
 - header contents, 82–83
 - length field, 83
 - overview of, 76
 - starting encryption when connected, 161–162
- Data packets, sending
 - acknowledgement, 101
 - example of, 101–104
 - header, 99
 - logical link identifier, 100–101
 - more data, 101
 - overview of, 98–99
 - sequence numbers, 101
- Data rates
 - in classic Bluetooth vs. low energy, 3–4
 - optimizing for low power, 125–126
 - radio systems vs. application, 51
- Data types, advertising, 273–276
- DBm
 - calculating range, 58–60
 - measuring receiver sensitivity, 57–58
- Debugging
 - HCI version exchange, 160–161
 - version information for, 117
- Declaration, characteristic, 211–213
- Declaration of Compliance (DoC), 313, 320–321
- Description field, Characteristic Presentation Format Descriptor, 216–217
- Descriptors, characteristic
 - discovering all, 234–235
 - discovery, central device, 286
 - overview of, 214–217
 - reading/writing, 238
- Design
 - asymmetric, 14–15
 - compliance folder containing information on, 318
 - goals, 7–8
 - lowering cost, 4–6
 - service-oriented architecture goals, 21–25
 - for success, 15–16
- Development tool product type, 315–316
- Device address
 - HCI advertising parameters, 149–150
 - HCI controller setup, 141–142
- Device density, designing controller, 15–16
- Device Name characteristic, GAP Service, 276, 284
- Device Under Test. *see* DUT (Device Under Test)
- Devices
 - asymmetric design concept, 14–15
 - Direct Test Mode requirements, 61–62
 - finding, 90–92
 - Generic Access Profile for, 36
 - given tolerance of, 57
 - initial connection to, 156, 258
 - initial discovery procedure, 256–257
 - new usage models for. *see* new usage models
 - profiles describing two or more, 37–38
 - time is energy concept, 12–13
 - types of, 6
 - types of data in Bluetooth low energy, 180–181
- Digital modulation, 51–54
- Digital radio, phase modulation in, 51
- Digital television, 51
- Direct advertising, 91–92
- Direct Test Mode
 - background of, 61–62
 - controller architecture, 29–30
 - hardware interface, 65–67
 - transceiver testing, 62–65
 - using HCI, 67–68
- Direct-connectable mode, GAP, 266–267
- Direct-connection establishment procedure, GAP, 269
- Directed advertising, optimizing peripherals, 307
- Discoverability
 - advertising state used for, 71
 - central device, 283–285
 - Generic Access Profile defining device, 36
 - initial discovery, 256–257
 - modes, 264–265
 - overview of, 263–264
 - peripheral devices, 300–301
 - procedures, 265–266
 - in service-oriented architecture, 24–25

- Discoverable advertising events, 82, 93
- Discoverable advertising state, peripherals, 304–306
- Discovery procedures, GATT, 232–235
- DoC (Declaration of Compliance), 313, 320–321
- Documentation, authorization via, 242–243
- Dual-mode devices, 6
- DUT (Device Under Test)
 - Direct Test Mode, 61–62
 - hardware interface, 65–67
 - receiver tests, 64–65
 - transceiver tests, 62
 - transmitter tests for, 63–64
- Duty cycle, short packets optimizing, 125
- Dynamic refreshing, memory, 13–14

E

- EDR (Enhanced Data Rate), Bluetooth
 - version 2.0, 3
- Encapsulation of services, 34
- Encryption
 - AES, 105–106
 - authentication via, 242
 - central device bonding using, 292–293
 - data channel, 30
 - ensuring confidentiality, 243
 - HCI controller setup, 145–146
 - HCI restarting, 163–164
 - HCI starting, 161–162
 - Insufficient Encryption error, 230
 - Insufficient Encryption Key Size error, 230
 - Link Layer restarting, 115–116
 - Link Layer starting, 112–115
 - Long-Term Key, 246
 - lowering overhead with, 126
 - message integrity check, 107–109
 - offline, 130
 - overview of, 104–105
 - payload data, 106–107
 - security design and, 16
 - Short-Term Key, 246
- Encryption Change event, HCI, 161, 163
- Encryption engine, security, 244
- Encryption Key Refresh Complete, HCI, 163–164
- End product type, 315–316
- Energy
 - life of button-cell batteries, 12

- memory is expensive concept, 13–14
- time is, 12–13
- Enhanced Data Rate (EDR), Bluetooth
 - version 2.0, 3
- Error Response, Attribute Protocol, 228–231
- Errors
 - bit, 16, 58, 84
 - SDIO interface with low rates of, 135
 - types of responses, 228–231
- Ethernet, technologies increasing speeds of, 4
- Event masks, HCI controller setup, 142
- Event packets, HCI interface, 137–138
- Events, Direct Test Mode, 65–68
- Everything has state concept, 16–17
- Exchange MTU procedure, GATT, 232
- Exchange MTU Request and Response, Attribute Protocol, 221
- Execute Write Request, Attribute Protocol
 - characteristic descriptors procedure, 238
 - characteristic values procedure, 236
 - as exception to transaction rules, 198
 - overview of, 226
 - reliable writes procedure, 237
- Extending services, 201–203
- External state, 182

F

- Features
 - consistency check for new product, 316–317
 - HCI connection management, 160
 - HCI controller setup, 143–144
 - Link Layer control, 118
 - selecting for new product, 316
- Filter policy, HCI, 150, 152
- Filters
 - Bluetooth low energy vs. classic, 29
 - determining device discoverability, 257
- Find By Type Value Request, Attribute Protocol, 222–223, 230, 233
- Find Information Request, Attribute Protocol, 221–222, 230, 234–235
- Find Requests, accessing attributes, 196
- Finite state machines, Attribute Protocol, 184–185
- Fixed channels, Bluetooth low energy
 - supporting only, 171
- Flags
 - advertising data, 273–274
 - HCI data packets, 138–139

Flags AD information
 advertising data, 273–274
 discoverable modes and, 264–265
 discoverable procedures and, 265–266

Flow control wires, 5-wire UART transport, 132

FM (frequency modulation) radio, analog,
 51–52

Formal contracts, service-oriented
 architecture, 22

Format
 Bluetooth low energy requiring one frame,
 32–33
 characteristic specification, 37–38
 test packet, 63

Format field
 Characteristic Aggregation Format
 Descriptor, 217
 Characteristic Presentation Format
 Descriptor, 215–216

Frame rate, 51

Frequency
 device tolerance and accuracy of, 57
 optimizing drift with short packets, 124–125
 peripherals that only broadcast, 300
 radio signal at Physical Layer, 28–29

Frequency bands
 agreements on allocation of, 51
 Bluetooth low energy using radio channels,
 55–56
 overview of, 54

Frequency hopping
 adaptive. *see* adaptive frequency hopping
 Bluetooth classic using, 55
 data channels at Link Layer, 30
 defined, 9
 Link Layer connection process, 97–98
 overview of, 87
 spread spectrum radio regulations vs., 29

Frequency modulation (FM) radio, analog,
 51–52

FSK (frequency-shift keying)
 Bluetooth low energy using GFSK, 54–55
 in digital modulation, 52
 MSK variant of, 53
 using whitener with, 77–79

Future-proof design, 18–19

G

attribute database including, 193

background, 255–256

bonding and pairing process, 252

defined, 255

establishing initial connection, 258

exposing services to peripherals, 301–302

generating private addresses, 106

host architecture, 36

initial discovery procedure, 256–257

long-term relationships, 259

private addresses, 260–261

reconnections, 260

roles, 261–262

security modes, 270–273

service characterization, 258–259

GAP (Generic Access Profile), modes and
 procedures
 bonding, 270
 broadcast mode and observation, 263
 connectability, 266–269
 discoverability, 263–266
 overview of, 262–263

GAP Service, 276–279, 284

Gateways
 client-server architecture, 17–18
 device interaction with Internet, 44–46
 modular service architecture and, 19

GATT (Generic Attribute Profile)
 characteristic discovery, 234–235
 client-initiated procedures, 235–239
 creation of, 179
 defining flat structure of attributes, 199
 discovering services, 232–233
 discovery procedures, 232
 ensuring future-proof design, 18
 forms of grouping, 200
 as GAP Service, 276–279
 host architecture, 34–36
 mapping ATT PDUs to, 239
 overview of, 231–232

Gaussian Frequency Shift Keying (GFSK),
 28–29, 54–55

General advertising, 91, 93

General-connection establishment procedure,
 GAP, 268–269

General-discoverable mode, 256–257, 265–266

Generic Access Profile. *see* GAP (Generic
 Access Profile)

Generic Attribute Profile. *see* GATT (Generic
 Attribute Profile)

Generic clients

- building for central devices, 287–288

- Characteristic Presentation Format

- Descriptor and, 215–217

- defined, 215

- enabling with GATT, 215

- GFSK (Gaussian Frequency Shift Keying), 28–29, 54–55

- Global operations, 7–8, 54

- Ground, 3-Wire UART transport, 132

Grouping

- Read By Group Type Request, 225

- services and characteristics, 199

- services using service declaration, 208–209

- Unsupported Group Type error, 231

H

- Handle Value Indication, Attribute Protocol, 228, 239

- Handle Value Notification, Attribute Protocol, 227–228, 238

- Hardware interface, Direct Test Mode, 65–67

- Hash values, Identity Resolving Key, 246–247

HCI (Host/Controller Interface)

- active scanning, 152–153

- advertising, 148–150

- defined, 131

- Device Under Test requirements, 61

- Direct Test Mode using, 67–68

- initiating connections, 153–157

- overview of, 31

- passive scanning, 150–152

- segmentation and reassembly, 170

HCI connection management

- channel map update, 159–160

- connection update, 158

- feature exchange, 160

- initiating connections, 153–157

- restarting encryption, 163–164

- starting encryption, 161–163

- termination, 164–165

- version exchange, 160–161

HCI controller setup

- encrypting data, 145–146

- overview of, 140–141

- random numbers, 145

- reading buffer sizes, 142–143

- reading device address, 141–142

- reading supported features, 143–144

- reading supported states, 144–145

- resetting to known state, 141

- setting event masks, 142–143

- setting random address, 146–147

- white lists, 147–148

- HCI Encrypt command, private addresses, 261

HCI logical interface

- command flow control, 139–140

- command packets, 135–136

- data flow control, 140

- data packets, 138–139

- defined, 135

- event packets, 137

- HCI channels, 135

HCI physical interfaces

- 3-Wire UART, 132–134

- overview of, 131

- SDIO, 134–135

- UART, 132

- USB, 134

Header

- data packet, 99

- framed packet, 133

- L2CAP packet, 173

- packet structure, 30–31, 81–83

- Hop value, frequency hopping, 87

- Host, enabling presence detection, 41–42

Host architecture

- Attribute Protocol, 33–34

- attributes. *see* attributes

- Generic Access Profile. *see* GAP (Generic Access Profile)

- Generic Attribute Profile. *see* GATT (Generic Attribute Profile)

- L2CAP. *see* L2CAP (Logical Link Control and Adaptation Protocol)

- Logical Link Control and Adaptation Protocol, 32–33

- overview of, 32

- security. *see* security

- Security Manager, 33

- three-chip solution, 39–40

- two-chip solution, 39–40

- Host subsystem product type, 315–316

- Host/Controller Interface. *see* HCI (Host/Controller Interface)

- I**
- ICS (Implementation Conformance Statements), 316–317
 - Identifiers, L2CAP channel, 171–172
 - Identity
 - central devices discovering other device, 284
 - Identity Resolving Key and, 246–247
 - Identity Resolving Key. *see* IRK (Identity Resolving Key)
 - IEEE 802.11, Bluetooth version 3.0, 3
 - IETF RFC 3610, encrypting payload data, 106
 - Immediate Alert Service, central devices, 290
 - Immutability, 200
 - Immutable encapsulation of services, 34
 - Imperial units, SI, 191
 - Implementation Conformance Statements (ICS), 316–317
 - Include attributes, services, 209–210
 - Include declaration, 233
 - Included services
 - discovering, 233
 - overview of, 209–210
 - Read By Type Request searching for, 223
 - Indications
 - accessing attributes, 196–197
 - Attribute Protocol, 218–219
 - central devices interacting with services, 291–292
 - Client Characteristic Configuration
 - Descriptor for, 214
 - Handle Value Indication, 228
 - optimizing peripheral attributes, 310–311
 - server-initiated GATT procedure for, 239
 - in service characterization, 259
 - Industrial, Scientific, and Medical (ISM)
 - band. *see* 2.4GHz ISM band
 - Inheritance, enabling changes to interfaces, 200
 - Initial connection procedure, 258
 - Initial discovery procedure, GAP, 256–257
 - Initialization vector (IV), encryption, 114
 - Initiating connections
 - from central devices, 285–286
 - HCI, 153–157
 - Initiating state, Link Layer state machine, 73
 - Instant parameter, connection updates, 110–111
 - Insufficient Authentication error, 229
 - Insufficient Authorization error, 229
 - Insufficient Encryption error, 230
 - Insufficient Encryption Key Size error, 230
 - Insufficient Resources error, 231
 - Integrity, security concept of, 243
 - Interfaces, object-oriented programming, 199
 - Internal state, 182–185
 - International System of Units (SI), 191
 - Internet
 - client-server architecture, 17–18
 - gateways. *see* gateways
 - Interoperability
 - Bluetooth classic/Bluetooth low energy, 6
 - connection-oriented problems, 43–44
 - profile/service architecture and, 185–189
 - Interpacket gap, optimizing for low power, 125
 - Invalid Attribute Value Length error, 230
 - Invalid CID in request reason code, 175
 - Invalid Handle error, attributes, 228–229
 - Invalid Offset error, 229
 - Invalid PDU error, 229
 - IP (Internet Protocol) license, 4–5
 - IPv6 (Internet Protocol), 46
 - IRK (Identity Resolving Key)
 - key distribution during pairing, 251
 - long-term relationships, 259
 - overview of, 246–247
 - saving during bonding for private addresses, 260–261
 - ISM (Industrial, Scientific, and Medical)
 - band. *see* 2.4GHz ISM band
 - IV (initialization vector), encryption, 114
- J**
- Just Works mode, TK value in, 245
- K**
- Key distribution
 - pairing procedure, 251
 - security architecture, 15
 - Security Manager protocol for, 33
 - Keys
 - Connection Signature Resolving Key, 247
 - encrypting text with, 105
 - Identity Resolving Key, 246–247
 - Long-Term Key, 246
 - as shared secrets, 245
 - Short-Term Key, 246
 - Temporary Key, 245–246

- L**
- L2CAP (Logical Link Control and Adaptation Protocol)
 - background to, 169–171
 - Bluetooth low energy using, 179–180
 - channels, 171–172
 - defined, 169
 - host architecture and, 32–33
 - LE signaling channel, 173–177
 - optimizing peripherals for low power, 307–309
 - packet structure, 172–173
 - solving connection-oriented problems, 43–44
 - LANs (local area networks), 2.4GHz ISM band rules, 54
 - Latency, resolving low, 129–130
 - Layers
 - defined, 9
 - low power as design goal for, 7–8
 - LE Add Device To White List command, HCI, 147–148, 154–156
 - LE Advertising Report event, HCI, 152
 - LE Clear White List Size command, HCI, 147–148
 - LE Connection Complete event, HCI, 155–157
 - LE Connection Update command, HCI, 158
 - LE Connection Update Complete event, HCI, 158
 - LE Create Connection Cancel command, HCI, 157
 - LE Create Connection command, HCI, 154–157
 - LE Long Term Key Request event, 162–163
 - LE Rand command, HCI, 147
 - LE Read Advertising Channel Tx Power command, HCI, 150
 - LE Read Buffer Size command, HCI, 142–143
 - LE Read Channel Map command, HCI, 159
 - LE Read Remote Used Features command, HCI, 160
 - LE Read Remote Used Features Complete event, HCI, 160
 - LE Read Remote Version Information command, HCI, 160–161
 - LE Read Supported Features command, HCI, 143–144
 - LE Read Supported States command, HCI, 144–145
 - LE Read White List Size command, HCI, 147–148
 - LE Remove Device From White List command, HCI, 147–148
 - LE Set Advertising Data command, HCI, 150
 - LE Set Advertising Enable command, HCI, 150
 - LE Set Advertising Parameters command, HCI, 148–150
 - LE Set Host Channel Classification command, HCI, 159
 - LE Set Random Address command, HCI, 147
 - LE Set Scan Enable command, HCI, 152
 - LE Set Scan Parameters command, HCI, 150
 - LE Set Scan Response Data command, HCI, 150
 - LE signaling channel, L2CAP
 - command reject command, 174–175
 - connection parameter update request command, 175–177
 - overview of, 173–174
 - LE Start Encryption command, 161–162
 - Leakage current, button-cell batteries, 12
 - Length field
 - advertising data, 273
 - packet structure, 30–31, 82–83
 - Licensing
 - 2.4GHz ISM band free of, 54
 - Bluetooth low energy IP, 5
 - Bluetooth low energy ISM band, 4–5
 - Limited-discoverable mode, devices
 - discoverable procedures, 265–266
 - initial discovery, 256
 - overview of, 264–265
 - peripherals, 300–301
 - Link budget, calculating range, 58–60
 - Link establishment mode, 3-Wire UART, 133
 - Link Layer
 - advertising mode in, 41
 - asymmetric design at, 14
 - broadcasting, 92–93
 - channels, 84–89
 - controller architecture, 30–31
 - creating connections, 93–98
 - encryption, 104–109
 - finding devices, 90–92
 - function of, 69
 - HCI. *see* HCI (Host/Controller Interface)
 - low power as design goal for, 7
 - managing connections, 109–119
 - optimizing for low power. *see* optimization for low power
 - packet structure, 79–84

- Link Layer (*continued*)
 - packets, 76–79
 - robustness, 120–123
 - sending data, 98–104
 - Link Layer state machine
 - advertising, 71
 - connection, 73–74
 - multiple state machines, 74–75
 - overview of, 69–70
 - scanning, 72
 - standby, 70–71
 - Link Loss Service, 288–289
 - Link Power Management, 134
 - LL_CHANNEL_MAP_REQ, 111–112
 - LL_CONNECTION_UPDATE_REQ, 109–111
 - LL_ENC_REQ, 112–113, 116
 - LL_ENC_RSP, 112–113
 - LL_FEATURE_REQ, 118
 - LL_FEATURE_RSP, 118
 - LL_PAUSE_ENC_REQ, 115
 - LL_PAUSE_ENC_RSP, 115–116
 - LL_START_ENC_REQ, 114
 - LL_START_RSP, 114–115
 - LL_TERMINATE_IND, 119
 - LLID (logical link identifier), data packet
 - header, 100–101
 - Load balancing, client-server architecture, 21
 - Local area networks (LANs), 2.4GHz ISM band rules, 54
 - Local name advertising data type, 275
 - Logical interface. *see* HCI logical interface
 - Logical Link Control and Adaptation Protocol. *see* L2CAP (Logical Link Control and Adaptation Protocol)
 - Logical Link Control protocol, 180
 - Logical link identifier (LLID), data packet
 - header, 100–101
 - Long-term relationships, bonding, 259
 - Loose coupling, service-oriented architecture, 22–23
 - Low power
 - button-cell batteries for, 11–12
 - as design goal, 7–8
 - lowering cost of Bluetooth low energy with, 5–6
 - optimizing for. *see* optimization for low power
 - Low power state mode, 3-Wire UART, 133
 - Lower-host controller interface, 31
 - LT (Lower Tester)
 - Direct Test Mode, 61–62
 - receiver tests, 64–65
 - transceiver tests, 62
 - transmitter tests, 64
 - LTK (Long-Term Key)
 - key distribution during pairing, 251
 - long-term relationships, 259
 - overview of, 246
 - private addresses, 261
 - starting encryption for connections, 112–114
- ## M
- Man-in-the-middle attacks, 245–246, 249–250
 - Manufacturer-specific advertising data type, 276
 - Mapping
 - ATT PDUs to GATT procedures, 239
 - data broadcasting helping with, 42–43
 - profiles to services, 37–38
 - Market segments
 - one billion is a small number concept, 19
 - targeted by Bluetooth low energy, 11
 - Master connection substate, 73–74
 - Masters
 - asymmetric design concept of, 15
 - defined, 9
 - Link Layer connection process, 95–98
 - multiple state machine restrictions, 74–75
 - Maximum transmission unit (MTU), Attribute Protocol, 221
 - Mbps (million bits per second), Bluetooth low energy transmission, 54–55
 - MD (more data) bit, 101–104
 - Memory
 - Attribute Protocol requiring very little, 34
 - cost of, 13–14
 - Prepare Queue Full error and, 229–230
 - single-chip solutions and, 39
 - Message authentication code, authentication signature, 226
 - Message integrity check. *see* MIC (message integrity check)
 - Metric units, SI, 191
 - MIC (message integrity check)
 - AES calculating, 105
 - encrypted packets including, 107–109
 - encrypting payload data, 106–107
 - Prepare/Execute Writes and, 198, 227

Million bits per second (Mbps), Bluetooth
 low energy transmission, 54–55
 Minimum-shift keying (MSK), 53, 55
 Modems, technologies increasing speeds of, 4
 Modes, GAP
 bonding, 270
 broadcast, 263
 connectable, 266–267
 discoverability, 263–265
 overview of, 262
 security levels and, 270–273
 Modular architecture concept, 18–19
 Modular service architecture, 18–19
 Modulation
 analog, 49–51
 digital, 51–54
 overview of, 54–55
 Modulation index
 Bluetooth low energy, 54–55
 digital modulation, 52–53
 radio signal, 29
 More data (MD) bit, 101–104
 MSK (minimum-shift keying), 53, 55
 MTU (maximum transmission unit),
 Attribute Protocol, 221
 Multiple state machines, 74–75
 Multiplexing layer. *see* L2CAP (Logical Link
 Control and Adaptation Protocol)

N

Name, discovery of device, 257
 NAT (network address translation), gateways,
 45
 NESN (next expected sequence number), 99,
 101–104
 Network address translation (NAT),
 gateways, 45
 New usage models
 broadcasting data, 42–43
 connectionless model, 43–44
 gateways, 44–46
 presence detection, 41–42
 Next expected sequence number (NESN), 99,
 101–104
 Next expected sequence numbers, 101–104
 NIST FIPS-197. *see* AES (Advanced
 Encryption System)
 NIST Special Publication 800-38B, 247
 Nokia, 5

Nonbondable mode, GAP, 270
 Nonce, 106, 112–113
 Nonconnectable advertising events, 82, 93
 Nonconnectable mode, GAP, 266
 Nonconnectable undirected advertising, 149
 Nondiscoverable mode, 264
 Nonresolvable private addresses, 278
 Notifications
 accessing attributes, 196–197
 Attribute Protocol, 219
 central devices interacting with services,
 291–292
 Client Characteristic Configuration
 Descriptor for, 214
 as exception to transaction rules, 197
 Handle Value Notification, 227–228
 optimizing peripheral attributes, 310–311
 server-initiated GATT procedure for, 238
 in service characterization, 259
 Null modem, UART configuration, 132
 Num HCI Command Packets parameter,
 command flow control, 139–140

O

Object-oriented programming, 199
 Objects, in object-oriented programming, 199
 Observer role, GAP, 262
 Offline encryption, 130
 Offset, Invalid Offset error, 229
 One billion is a small number concept, 19
 Online resources, starting new project, 313
 OOK (on-off keying), digital modulation,
 51–52
 Optimization for low power
 acknowledgement scheme, 127
 high bit rate, 125–126
 low overhead, 126
 overview of, 123–124
 peripheral design for attributes, 311–312
 peripheral devices, 303–310
 short packets, 124–125
 single-channel connection events, 127–128
 subrating connection events, 128–130
 Out Of Band algorithm, TK value in, 245
 Overhead, optimizing for low power, 126

P

Packet Boundary Flag, HCI, 138–139
 Packet counter, encrypting payload data, 106

- Packet overhead, application data rate and, 51
- Packet reporting event, Direct Test Mode, 67–68
- Packet structure, Link Layer
 - access address, 80–81
 - bit order and bytes, 79–80
 - CRC, 84
 - header, 81–83
 - length, 82–83
 - overview of, 30–31, 76
 - payload, 83–84
 - preamble, 79–80
- Packets
 - advertising and data, 76
 - as building block of Link Layer, 76
 - CRC protecting against bit errors, 16
 - initiating, 73
 - optimizing with short, 124–125
 - reducing memory requirements with small, 14
 - restricting devices to short, 13
 - structure of L2CAP, 172–173
 - testing. *see* Direct Test Mode
 - whitening, 77–79
- Pairing
 - authentication of link, 242, 250–251
 - and bonding, 252
 - central devices initiating bonding, 292–293
 - exchange of information, 248–250
 - key distribution, 251
 - overview of, 248
 - Security Manager protocol for, 33
 - Short-Term Key for encrypting during, 246
 - Temporary Key in, 245–246
- Pairing Failed message, 249, 251
- Pairing Request message, 249–250, 270
- Pairing Response message, 249–250
- PAL (Protocol Adaptation Layer), Bluetooth
 - low energy, 169–170
- PANs (personal area networks), 2.4GHz ISM
 - band rules, 54
- Parameters
 - configuring advertising, 148–150
 - HCI connection management by updating, 158
 - HCI connections to white lists, 155
 - HCI passive scanning, 150–152
 - initiating connections from central devices, 285–286
- Parity bit, UART, 132
- Passive scanning
 - central devices discovering devices with, 283–285
 - HCI, 150–152
 - Link Layer state machine, 72
 - overview of, 72
 - receiving broadcast data, 93
- Passkey Entry mode, TK value, 245
- Pathloss
 - calculating link budget to determine range, 58–60
 - central devices discovering devices, 284
- Payload data
 - 3-Wire UARTs in HCI, 133
 - AES encrypting, 105
 - encrypting, 106–107
 - L2CAP packet structure, 172–173
 - packet structure, 83–84
- PDUs, Attribute Protocol
 - Invalid PDU error, 229
 - mapping ATT PDUs to GATT procedures, 239
 - overview of, 219–220
- Peak current, button-cell batteries and, 12
- Peripheral design
 - background of, 299
 - being connectable, 301
 - being discoverable, 300–301
 - broadcast only, 299–300
 - characteristics, 302–303
 - exposing services, 301–302
 - optimizing attributes, 311–312
 - optimizing for low power, 303–310
 - security, 303
- Peripheral Preferred Connection Parameters
 - characteristic, GAP Service, 279
- Peripheral Privacy Flag, GAP Service, 277–278
- Peripheral role devices, GAP
 - connectable modes, 266–269
 - discoverability in, 263–264
 - discoverability modes, 264–265
- Permissions
 - attribute database, 194–195
 - Attribute Protocol, 34
 - authorization via, 242–243
 - profile security, 296
 - security for peripherals, 303
- Personal area networks (PANs), 2.4GHz ISM
 - band rules, 54

- Phase modulation, 51
- Physical bit rate, 51
- Physical interfaces. *see* HCI physical interfaces
- Physical Layer
 - asymmetric design at, 14
 - evolution of Bluetooth data rates, 3
 - low power design goal for, 7
- Physical Layer, controller
 - analog modulation, 49–51
 - architecture, 28–29
 - background, 49
 - digital modulation, 51–54
 - frequency band, 54
 - modulation, 54–55
 - radio channels, 55–56
 - range, 58–60
 - receiver sensitivity, 57–58
 - testing with Direct Test Mode, 29–30
 - tolerance, 57
 - transmit power, 56–57
- Physical measurement, external state, 182
- Piconet, 9
- PIN (personal identification number), 104, 242, 244–245
- Plan, test, 317
- Plug-and-play client applications, 207–208
- Power sensitivity, USB interface, 134
- PRBS9 packet sequence, transmitter tests, 63–64
- PRD (Qualification Program Reference Document), compliance, 320
- Preamble, packet structure, 30–31, 79–80
- Prepare Queue Full error, 229–230
- Prepare Write Request, Attribute Protocol
 - overview of, 198
 - Prepare Queue Full error, 229–230
 - reliable writes procedure, 237
 - working with, 226–227
 - writing characteristic descriptors procedure, 238
 - writing characteristic values procedure, 236
- Presence detection, new wireless model
 - enabling, 41–42
- Primary services
 - defined, 37
 - discovering all, 232–233
 - discovering with service UUID, 233
 - discovery, central device, 286
- Find By Type Value Request, 223
 - grouping using service declaration, 208–209
 - overview of, 35–36
 - plug-and-play client applications, 207–208
 - profile discovering for peer device, 295
 - secondary vs., 205–207
- Privacy
 - creating with resolvable private addresses, 36
 - Identity Resolving Key and, 246–247
 - Peripheral Privacy Flag, 277–278
 - primary goal of, 16
 - security concept of, 243–244
- Private addresses
 - AES generating, 105–106
 - complications of advertising using, 260
 - defined, 260
 - GAP connection procedures, 268–269
 - for privacy, 16
 - reconnection addresses as nonresolvable, 278
- Procedures, GAP
 - bonding, 270
 - connectable, 267–269
 - defined, 263
 - discoverable, 265–266
 - observation, 263
 - types of, 263
- Procedures, GATT
 - characteristic discovery, 234–235
 - client-initiated, 235–238
 - Exchange MTU, 232
 - mapping ATT PDUs to, 239
 - overview of, 231–232
 - server-initiated, 238–239
 - service discovery, 232–233
- Product information
 - compliance folder contents, 318
 - including in Declaration of Compliance, 320
- Product types
 - combining components, 321
 - selecting features for new, 316
 - selecting for Bluetooth low energy projects, 315–316
- Profile subsystem product type, 315–316
- Profile Tuning Suite (PTS) testers,
 - qualification testing, 318
- Profiles
 - application layer, 37–38
 - finding and using characteristics, 296
 - finding services, 295
 - generating test plan for, 317

Profiles (*continued*)

- modular service architecture for, 18–19
- security, 296–297
- selecting for new product, 316
- understanding, 294–295

Profile/service architecture

- in Bluetooth classic, 185–186
- in Bluetooth low energy, 186–189

Properties, characteristic, 211–214

Protocol Adaptation Layer (PAL), Bluetooth low energy, 169–170

Protocol messages, Attribute Protocol, 219–220

Protocol testers, qualification testing, 318

Protocols

- Bluetooth low energy, 179–180
 - Bluetooth using Attribute Protocol. *see* Attribute Protocol
 - memory burdened with multiple, 14
- PTS (Profile Tuning Suite) testers, qualification testing, 318

Q

QDID (Qualified Design Identifier)

- combining components, 321
- declaring compliance, 320
- listing product, 321
- qualifying design, 319–320

Quadrature amplitude modulation, 51

Qualification program. *see* testing and qualification

Qualification Program Reference Document (PRD), compliance, 320

R

Race conditions, HCI, 157

Radio Band, 9–10

Radio channels

- overview of, 55–56
- starting receiver tests, 64
- starting transmitter tests, 63–64

Radio signals

- analog modulation and, 50–51
- controllers transmitting and receiving, 27
- enabling presence detection, 41–42
- high bit rate for low power, 125
- measuring path loss in, 58
- at Physical Layer, 28–29
- short range issues, 8
- widening of low energy, 29, 41

Radio-Frequency Identification (RFID) tags, 4

Random addresses

- HCI advertising parameters, 149–150
- HCI controller setup, 146–147
- Identity Resolving Key and, 246–247
- private addresses as, 260

Random numbers

- authentication during pairing, 250–251
- HCI controller setup, 145
- Long-Term Key using, 246
- Short-Term Key generated with, 246
- whiteners as, 77–79

Range, calculating, 58–60

Read BD_ADDR command, device address, 141–142

Read Blob Request, Attribute Protocol

- Attribute Not Long error, 230
- characteristic descriptors procedure, 238
- multiple characteristic values procedure, 235–236
- overview of, 224

Read Buffer Size command, HCI controller, 142–143

Read By Group Type Request, Attribute Protocol, 225, 230, 232–233

Read By Type Request, Attribute Protocol

- Attribute Not Found error, 230
- discovering all characteristics of service, 234
- discovering included services, 233
- multiple characteristic values procedure, 236
- overview of, 223

Read Characteristic Value by UUID

- procedure, central devices, 284

Read Multiple Request, Attribute Protocol, 224, 236

Read Not Permitted error, 229

Read only memory (ROM), single-chip solutions, 39

Read Request, Attribute Protocol

- accessing attributes, 196
- characteristic descriptors procedure, 238
- multiple characteristic values procedure, 235–236
- overview of, 224

Read Supported Features command, HCI controller, 143–144

Readable, access permission, 194

- Readable and Writable, access permission, 194
 - Readable characteristics, 288
 - Readable state, 16–17
 - Reason codes, command reject command, 174–175
 - Receive data (RXD), UART/3-Wire UART transport, 132
 - Received signal strength (RSSI), central devices, 284
 - Receiver sensitivity, 57–58
 - Receiver test command, Direct Test Mode, 66, 68
 - Receivers
 - in advertising state, 71
 - analog modulation and, 49–51
 - asymmetric design of, 14
 - calculating range, 58–60
 - time is energy concept of, 12–13
 - transceiver tests, 62–65
 - using whitener with FSK, 77–79
 - Reconnected connections, 260
 - Reconnection Address, GAP Service, 278
 - References
 - combining services, 204–205
 - extending services, 201–203
 - reusing another service, 203–204
 - services referencing other services, 200–201
 - Relationships
 - accommodating between services, 35
 - central device discovery of, 286
 - central devices initiating bonding, 292–293
 - creating permanently with Generic Access Profile, 36
 - profile service, 37–38
 - Remapping process, adaptive frequency hopping, 88–89
 - Replay attack protection
 - authentication via signatures, 242
 - encrypted packets, 105
 - Request Not Supported error, 229
 - Request to send (RTS), 5-wire UART transport, 132
 - Requests
 - Attribute Protocol, 218–219
 - error responses to, 228–231
 - Reset command, Direct Test Mode, 66, 68
 - Reset command, HCI controller, 141
 - Resolvable private addresses, 260–261, 268–269
 - Restarting encryption, HCI connections, 163–164
 - Reusability
 - behaviors limiting, 37
 - of characteristics, 37–38
 - in service-oriented architecture, 23
 - RF testers, qualification testing, 318
 - RFID (Radio-Frequency Identification) tags, 4
 - Robustness, Link Layer, 120–123
 - Roles
 - GAP, 261–262
 - profile, 294–295
 - ROM (read only memory), single-chip solutions, 39
 - RSSI (received signal strength), central devices, 284
 - RTS (request to send), 5-wire UART transport, 132
 - Rules
 - 2.4 GHz ISM band, 54
 - access address, 81
 - Attribute Protocol, 33–34
 - RXD (receive data), UART/3-Wire UART transport, 132
- ## S
- Scale, client-server architecture, 21
 - Scan Parameters Service, peripheral optimization, 309–310
 - SCAN_REQ, advertising packet, 82
 - SCAN_REQ packets, HCI active scanning, 152
 - SCAN_RSP, advertising packet, 82
 - SCAN_RSP packets, HCI active scanning, 152
 - Scannable undirected advertising, 149
 - Scanners
 - asymmetric design of, 14–15
 - enabling presence detection, 41–42
 - initial discovery process, 256–257
 - at Link Layer, 30–31
 - receiving advertising events via, 91
 - Scanning state, Link Layer state machine, 72
 - Scatternets, 75
 - SDIO interface, HCI, 134–135
 - Secondary services
 - defined, 37
 - grouping using service declaration, 208–209
 - including services, 209–210
 - overview of, 35–36
 - primary vs., 205–207

Secure Simple Pairing feature, 248–250

Security

- asymmetric design of, 15
- authentication, 241–242
- authorization, 242–243
- bonding, 252
- client-server gateway model of, 18
- confidentiality, 243
- Connection Signature Resolving Key, 247
- designing for success, 16
- encryption engine, 244
- Identity Resolving Key, 246–247
- integrity, 243
- Long-Term Key, 246
- overview of, 241
- pairing, 248–251
- peripheral devices, 303
- privacy, 243–244
- profile, 296–297
- shared secrets, 244–245
- Short-Term Key, 246
- signing of data, 252–253
- Temporary Key, 245–246

Security Manager

- Bluetooth low energy using, 179–180
- channel identifier for, 172
- host architecture, 33
- signing of data, 106

Segmentation, by multiplexing layers, 170

Selective-connection establishment procedure,
GAP, 269

Sequence numbers (SNs), 101–104

Server Characteristic Configuration

Descriptor, 214–215

Server-initiated procedures, GATT, 238–239

Service Changed characteristic, 294

Service data advertising data type, 276

Service solicitation advertising data type, 275

Service UUIDs

- discovering primary service, 233
- Include attributes, 209–210
- overview of, 191
- service advertising data types and, 274–275
- service declaration, 209

Service-oriented architecture

- abstraction, 23
- autonomy, 24
- composability, 24
- discoverability, 24–25
- formal contract, 22

loose coupling, 22–23

as paradigm for Bluetooth low energy,
21–22

reusability, 23

statelessness, 23–24

Services

- advertising data types for, 274
 - application layer, 37
 - central device changing, 293–294
 - central device interaction with, 288–292
 - central device's client remembering/caching
between connections, 293–294
 - combining, 204–205
 - defining with profile roles, 294–295
 - discovery at initial connect, 258
 - extending, 201–203
 - filtering advertising data based on, 257
 - GATT characteristic discovery procedures
for, 234–235
 - GATT discovery procedures for, 232–233
 - generating test plan for, 317
 - Generic Attribute Profile and, 34–36
 - grouping, 199, 208–209
 - mapping profiles to, 37–38
 - modular architecture for, 18–19
 - optimizing peripheral
attributes, 310–311
 - peripheral design for exposing, 301–302
 - plug-and-play client applications, 207–208
 - primary or secondary, 205–206
 - profiles discovering, 185–189, 295–296
 - reusing, 203–204
 - security for peripherals, 303
 - selecting for new product, 316
- Session based, connection-oriented model of
Internet, 45
- Session key diversifiers (SKD), 114
- Session key (SK), 112–115
- Shared secrets
- authentication via, 241–242
 - in bonding process, 259
 - Connection Signature Resolving Key, 247
 - encrypting data packets while connected
using, 161–162
 - Identity Resolving Key, 246–247
 - keys as, 245
 - Long-Term Key, 246
 - overview of, 244–245
 - Security Manager for key distribution, 33
 - Short-Term Key, 246
 - Temporary Key, 245–246

- Shift register, 77
 - Short packets, for low power, 124–125
 - Short range wireless standards, 8
 - Short-Term Key (ST), 245–246
 - Short-wave radio, 51
 - SI (International System of Units), 191
 - SIG (Special Interest Group), Bluetooth
 - testing and qualification requirements, 313–316
 - UnPlugFest testing events, 15
 - Signaling channel, channel identifier for, 172
 - Signaling MTU exceeded reason code,
 - command reject command, 175
 - SignCounter
 - authentication signature, 226
 - Connection Signature Resolving Key, 247
 - signing of data, 252–253
 - Signed Write Command, Attribute Protocol, 225–226, 237–238
 - Signing of data
 - AES, 105
 - authentication via, 242
 - Connection Signature Resolving Key, 247
 - security and, 252–253
 - Silicon manufacturing processes, short packets
 - optimizing, 124–125
 - Simultaneous LE And BR/EDR To Same Device Capable, 274
 - Single-channel connection events, 127–128
 - Single-chip solutions, stack split, 38–39
 - Single-mode devices, 6
 - SK (session key), 112–115
 - SKD (session key diversifiers), 114
 - Slave connection interval range, 275
 - Slave connection substate, 73–74
 - Slave latency
 - connecting to devices, 285
 - connection events and, 96–97, 129–130
 - connection parameter update request and, 175–176
 - connection update request, 111
 - controlling in peripherals, 308–309
 - defined, 129
 - optimizing peripherals for low power, 308–309
 - Slaves
 - in asymmetric design, 14–15
 - connection parameter update request and, 109–111
 - defined, 10
 - Link Layer connection process, 95–98
 - multiple state machine restrictions, 74–75
 - Sleep clock accuracy, Link Layer connection
 - process, 98
 - Sleep message, 3-Wire UARTs in HCI, 133–134
 - SLIP, framing packets in 3-Wire UART, 133
 - SNs (sequence numbers), 101–104
 - Spark-gap radios, 49–50, 51
 - Special Interest Group. *see* SIG (Special Interest Group), Bluetooth
 - Speeds, technology almost always increasing, 3–4
 - Spread spectrum radio regulations, 29
 - ST (Short-Term Key), 245–246
 - Stack splits architecture, 38–40
 - Standby state, Link Layer, 70–71
 - Start messages, LLID, 100
 - Starting encryption, HCI connection
 - management, 161–163
 - Starting new project, qualification program, 313–316
 - State
 - configuring controller, 136
 - in connectionless model, 44
 - in connection-oriented systems, 43–44
 - data vs., 181–182
 - HCI advertising filter policy, 150
 - HCI controller setup, 141, 144–145
 - kinds of, 182
 - Link Layer. *see* Link Layer state machine
 - optimizing peripherals for low power, 304–305
 - State machines
 - Attribute Protocol, 183–185
 - central devices interacting with services, 290–291
 - Link Layer. *see* Link Layer state machine
 - representing current internal state, 182
 - Statelessness
 - of Attribute Protocol, 34
 - in service-oriented architecture, 23–24
 - Stop bit, UART, 132
 - Subrated connection events, 128–130
 - Sub-version number, version information, 118
 - Symbols, 51
- T**
- TCP connection, as session-based, 45
 - Temperature, button-cell batteries, 12
 - Temporary Key (TK), 245–246, 250

Termination

- error response resulting in request, 231
- HCI connections, 164–165
- Link Layer connections, 118–119

Test end command, Direct Test Mode, 66, 68

Test equipment product type, 315–316

Test Plan Generator (TPG) project, 313–315, 317

Test status event, Direct Test Mode, 67–68

Testing and qualification

- Bluetooth process for, 314
- combining components, 321
- consistency check, 316–317
- creating compliance folder, 317–318
- declaring compliance, 320
- generating test plan, 317
- listing, 321
- overview of, 313
- qualification testing, 318–319
- qualify your design, 319–320
- selecting features, 316
- standardizing, *see* Direct Test Mode
- starting project, 313–316

Testing information, compliance folder contents, 318

Text strings, associating with characteristics, 214

Third-party attackers, compromising integrity, 243

Three-chip solutions, stack split, 40

Three-way handshake, encryption for connections, 113, 115

Time is energy concept, 12–13

TK (Temporary Key), 245–246, 250

Toggle command, state machines, 184–185

Tolerance, 57

TPG (Test Plan Generator) project, 313–315, 317

Transactions, atomic operations and, 197–198

Transceiver testing, Direct Test Mode, 62–65

Transmit (TX) power level advertising data type, 275, 284

Transmit power, 56–57

Transmit window, Link Layer connections, 95–96, 110–111

Transmitter test command, Direct Test Mode, 66, 68

Transmitters

- in advertising state, 71
- analog modulation and, 49–51

asymmetric design of, 14

calculating range, 58–60

time is energy concept of, 12–13

transceiver tests, 62–65

Two-chip solutions, stack split, 39–40

TX (transmit) power level advertising data type, 275, 284

TXD (transmit data), UART/3-Wire UART transport, 132

U

UART (Universal Asynchronous Receiver Transmitter), HCI

3-Wire, 132–134

Direct Test Mode, 61, 65

physical interface, 132

Undirected-connectable mode, GAP, 267

Unit UUIDs, 191

Units

Characteristic Presentation Format Descriptor, 216–217

generic client, 287

Unlikely Error response, 230

UnPlugFest testing events, 15

Unsupported Group Type error, 231

Updates

adaptive frequency hopping, 111–112

connection parameter, 109–111

Upper-host controller interface, 31

URLs, client-server architecture, 20–21

Usage models. *see* new usage models

USB physical interface, HCI, 134

UT (Upper Tester)

Direct Test Mode, 61–62

receiver tests, 64–65

transceiver tests, 62

UUIDs (Universally Unique Identifiers)

attribute types, 192

Bluetooth Base, 190–191

characteristic, 212–213, 236

characteristics at application layer labeled with, 37–38

discovering all primary services, 233

Find Information Response and, 222

generic clients and, 287

identifying attribute type, 190

service declaration, 209

service UUIDs. *see* service UUIDs

unit UUIDs, 191

V

- Validated testers, qualification testing, 318
- Value handle, characteristic, 212
- Values, characteristic
 - overview of, 213
 - reading, 235–236
 - writing, 236–238
- Version exchange
 - HCI connection management, 160–161
 - Link Layer connections, 117–118

W

- White lists
 - auto-connection establishment procedure, 267–268
 - connectability of peripherals, 301
 - HCI advertising filter policy, 150
 - HCI controller setup, 147–148
 - HCI initiating connection to device(s) in, 154–156
 - HCI passive scanning filter policy, 152
- Whitening, 77–79, 81
- Wibree technology, 5
- Wi-Fi
 - adaptive frequency hopping remapping, 88–89
 - defined, 10

- Link Layer channels and, 84–85
- technologies increasing speeds of, 4
- Window widening, 309
- Wired infrastructure, problem of Internet design, 45
- Wireless band, global operation design goals, 7–8
- Woken message, 3-Wire UARTs in HCI, 134
- Writable, access permission, 194
- Writable characteristics, 288–289
- Writable state, 17
- Write Command, Attribute Protocol
 - accessing attributes, 196
 - Signed Write Command, 225–226
 - writing without response procedure, 237–238
- Write Request, Attribute Protocol
 - accessing attributes, 196
 - characteristic descriptors procedure, 238
 - characteristic values procedure, 236
 - overview of, 225

X

- XML files
 - characteristic specifications, 302–303
 - generic clients and, 287–288