PRENTICE HALL

BLUETOOTH LOW ENERGY

THE DEVELOPER'S HANDBOOK

ROBIN HEYDON

Bluetooth Low Energy

This page intentionally left blank

Bluetooth Low Energy

The Developer's Handbook

Robin Heydon

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

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

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

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 MAC[1] PHY[2] (AMP) was added in version 3.0 of Bluetooth that used IEEE[3] 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 FRAND[4] 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 SI[5] 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/aquoisert/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

A

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

V

W

X