ZigBee Wireless Networking
ZigBee Wireless Networking

Drew Gislason
Contents

Foreword ........................................................................................................ ix
Preface ........................................................................................................... xi
Acknowledgments ............................................................................................ xv

Chapter 1 Hello ZigBee ..................................................................................... 1
1.1 What’s a ZigBee? .......................................................................................... 3
1.2 The ZigBee Alliance ..................................................................................... 14
1.3 ZigBee in the Marketplace ............................................................................ 20
1.4 Hello ZigBee (A First ZigBee Network) ....................................................... 24
1.5 ZigBee Home Automation ............................................................................ 34
1.6 ZigBee Speak ................................................................................................ 38
1.7 ZigBee Architecture ..................................................................................... 42

Chapter 2 Deciding on ZigBee ......................................................................... 45
2.1 Deciding on the Right Technology .............................................................. 46
2.2 Deciding on a ZigBee Solution ..................................................................... 50
2.3 ZigBee Modules ........................................................................................... 57
2.4 A ZigBee Checklist ...................................................................................... 59

Chapter 3 The ZigBee Development Environment ......................................... 65
3.1 Development Hardware .............................................................................. 66
3.2 The ZigBee Stack ........................................................................................ 74
3.3 The Embedded Compiler and Debugger .................................................... 88
3.4 Debugging the Network .............................................................................. 91
3.5 Example Development Sessions .................................................................. 95

Chapter 4 ZigBee Applications ......................................................................... 111
4.1 Sending and Receiving Data ....................................................................... 112
4.2 No Common C API .................................................................................... 125
4.3 ZigBee PANs ............................................................................................... 135
Contents

4.4 ZigBee Addressing ................................................................. 149
4.5 Addressing Within the Node .................................................. 169
4.6 Profiles ................................................................................... 181
4.7 ZigBee Application Support Sublayer (APS) ............................. 193
4.8 ZigBee AES 128-Bit Security .................................................. 200

Chapter 5 ZigBee, ZDO, and ZDP .............................................. 207
5.1 Device Discovery .................................................................... 211
5.2 Service Discovery ................................................................. 222
5.3 Binding .................................................................................. 226
5.4 ZDP Management Services ................................................... 229
5.5 Starting and Stopping ZigBee with ZDO ................................... 233
5.6 ZDO, ZigBee, and Low Power ................................................ 234

Chapter 6 The ZigBee Cluster Library ........................................ 239
6.1 ZCL Foundation ................................................................. 243
6.2 ZCL General Clusters .......................................................... 251
6.3 ZCL and Public Profiles ....................................................... 262
6.4 When to Use ZCL ................................................................. 267

Chapter 7 The ZigBee Networking Layer .................................... 273
7.1 ZigBee and IEEE 802.15.4 .................................................... 274
7.2 Forming, Joining, and Rejoining ZigBee Networks .................. 278
7.3 ZigBee Address Assignment .................................................. 297
7.4 ZigBee Packet Routing .......................................................... 302
7.5 ZigBee Over-the-Air Frames .................................................. 318
7.6 ZigBee Stack Profiles ............................................................ 327

Chapter 8 Commissioning ZigBee Networks ................................ 331
8.1 Commissioning Overview ..................................................... 332
8.2 The Commissioning Cluster ................................................... 336
8.3 Example 1: Simple Commissioning ........................................ 340
8.4 Example 2: Commercial Commissioning ................................. 344
8.5 Example 3: Custom Commissioning ........................................ 347

Chapter 9 ZigBee Gateways ......................................................... 351
9.1 A UART ZigBee Gateway ...................................................... 356
9.2 The Data Concentrator Problem .............................................. 363
9.3 Bandwidth and the Gateway .................................................. 377
9.4 Custom Gateways ............................................................ 383
Appendix A  ZigBee 2007 and ZigBee Pro ................................. 389
A.1  ZigBee 2006, 2007, and ZigBee Pro................................. 389
A.2  Stochastic Addressing .................................................... 391
A.3  Source Routing .............................................................. 392
A.4  Multicast ................................................................. 394
A.5  Frequency Agility ......................................................... 396
A.6  Fragmentation ............................................................ 398
A.7  Symmetric Routes and Link Status ................................. 400
A.8  Link Keys, SKKE, and High Security ............................... 401

Appendix B  ZigBee Quick Reference ................................. 405
B.1  The ZigBee Architecture .............................................. 405
B.2  APS Commands .......................................................... 405
B.3  ZDP Commands .......................................................... 405

Appendix C  ZigBee Cluster Library Quick Reference ............... 415
C.1  ZCL Foundation .......................................................... 415
C.2  ZCL General Clusters ................................................... 415

Index .............................................................................. 419
Foreword

Back in 1999, we saw the need for an organization with a mission to define a complete, open, global standard for reliable, cost-effective, low-power, wirelessly networked products addressing monitoring and control. While there were other standards that addressed higher data rates or battery-powered networks for a very small number of devices, none of these truly met the needs of this market. Instead, what we needed was something focused on:

- Large networks (a large number of devices and a large coverage area) that could form autonomously, and operate very reliably and securely for years without operator intervention
- Very long battery life (years of use from a pair of AA cells), very low infrastructure cost (low device and setup costs), very low complexity, and small size
- A relatively low data rate
- A standardized protocol, allowing multiple-vendor, interoperable products for the global market

Thus, in 2002, the ZigBee Alliance was born.

Now, with over 225 member companies, we are able to draw on a wealth of experience in every aspect of the business. Allowing so many companies the opportunity to have input is not as fast-paced as adopting a single proprietary system and declaring it a standard. Even so, the combined wisdom and the vetting process enable a much better solution to be built, one which meets all of the needs mentioned above. Getting it right is extremely important if a standard is to have a long track record of success.
Foreword

The ZigBee Alliance slogan, “Wireless Control That Simply Works,” is clearly what is needed for end users and implementers, but achieving that result places a heavy burden on the developers and OEMs. Drew Gislason has the ability to take complex topics and present them in a manner that is cogent and easily digestible to OEMs and developers. This book goes a long way in helping to explain ZigBee concepts, and in explaining how to implement ZigBee in a wide variety of products.

Many people do not realize that a quiet revolution is already under way in business, and in our homes. Great emphasis is being placed on reducing natural resource waste and in becoming exponentially more efficient. To achieve global efficiency goals, we must have an extensive, intelligent, easy-to-deploy, low-cost infrastructure to monitor and manage our surroundings. ZigBee is a solid technological solution for this monumental task, and brings with it other benefits and lifestyle improvements, such as increased security and convenience.

The momentum is gathering, and we are about to take a leap that brings remarkable savings, not only of resources, but of money and time. History repeatedly demonstrates that companies at the forefront set the mark for their industries. Indeed, many current industry leaders who take a “wait and see” approach are likely to be supplanted by new leaders willing to make an early investment in learning and implementing solutions such as ZigBee into their product lines. This book will help companies move up the learning curve rapidly.

Bob Heile, Ph.D.
Chairman, ZigBee Alliance
Preface

Intended Audience

ZigBee Wireless Networking is for developers who are interested in learning more about ZigBee. The developer who actually has a project at hand may benefit the most from the text and examples, but managers considering using ZigBee on a project will also benefit, especially from Chapter 1, “Hello ZigBee,” and Chapter 2, “Deciding on ZigBee.”

No prior experience with embedded programming, 802.15.4, or networking is required, but a working knowledge of the C programming language is helpful.

Most of the examples use the Freescale ZigBee platform, but the ideas apply to all ZigBee platform vendors. Occasionally, an example or solution is specific to the Freescale platform. Where this occurs, the text makes it clear that the solution is Freescale-specific, and not a ZigBee requirement, in general.

Formatting Conventions

Various elements in this book are specially formatted for easier identification while reading. Code samples are printed in a different style on a light gray background. Variables in the text are printed in bold. Each section ends in a brief summary, indicating the key points. For example, Code samples look like this:

```c
void BeeAppDataIndication(void)
{
    apsdeToAfMessage_t *pMsg;
    zbApsdeDataIndication_t *pIndication;
    zbStatus_t status = gZclMfgSpecific_c;
    while(MSG_Pending(&gAppDataIndicationQueue)
```

The Book’s Structure

This book is designed to be read from cover-to-cover, tutorial style. Each chapter introduces concepts that are used in later chapters. However, the reader is encouraged to
skip ahead if the concepts of any section are already familiar. To keep the reader oriented in each section, some overlap is necessary.

While it is not required, it is helpful to have the ZigBee and IEEE 802.15.4 specifications available when reading this book. I’ll sometimes refer to a section or a concept in those specifications for further reading.

To obtain the ZigBee specification, go to http://www.zigbee.org and click on “Download the Specification.” It is free, and comes in PDF format.

Go to http://standards.ieee.org/getieee802/802.15.html and select “IEEE 802.15.2-2003” to obtain the 802.15.4 standard in PDF format. There is a new draft standard, IEEE 802.15.2-2006, but ZigBee does not currently use that specification.

The chapters are organized as follows.

Chapter 1, “Hello ZigBee,” lays out the basics of ZigBee and its intended use. It describes the ZigBee Alliance, which is the standards body which defines and promotes the ZigBee standard worldwide. This chapter also provides the developer with several ZigBee networking examples, complete with source code.

Chapter 2, “Deciding on ZigBee,” helps the developer make technical and marketing choices about ZigBee, and even helps determine whether ZigBee is the right solution for any given problem. It provides a concise checklist, with all of the ZigBee factors that must be considered throughout the entire product life cycle, from inception through development, deployment, and maintenance.

Chapter 3, “The ZigBee Development Environment,” covers the basics of the ZigBee development environment, and walks the reader through an example, step-by-step, to help gain a full understanding of what’s involved in the development and debug phase. This chapter contains information necessary if the reader plans to follow along with the examples using actual hardware.

Chapter 4, “ZigBee Applications,” goes in-depth into application development, including the fundamentals of ZigBee networks, nodes, addressing, Application Profiles, and the features provided to the application by the Application Framework (AF) and Application Support Sub-layer (APS).

Chapter 5, “ZigBee, ZDO, and ZDP,” describes the ZigBee Device Object (ZDO) and how it interacts with and is used by applications, including how to achieve maximum battery life from ZigBee nodes.
Chapter 6, “The ZigBee Cluster Library,” covers the library of common clusters used for profile and device development. It describes Home Automation in some detail.

Chapter 7, “The ZigBee Networking Layer,” goes in-depth into how ZigBee actually delivers packets from one node to another, including mesh and tree networking. It also discusses some of the table management that must occur for ZigBee nodes to last for years (and decades) in the field with no required maintenance. This chapter also describes security in detail.

Chapter 8, “Commissioning ZigBee Networks,” describes the commissioning process with ZigBee. This topic is critical to the successful deployment and maintenance of ZigBee networks.

Chapter 9, “ZigBee Gateways,” introduces gateways and describes techniques for retrieving information from a ZigBee network, as well as controlling and configuring sensors and actuators from outside the ZigBee network.

Appendix A, “ZigBee 2007 and ZigBee Pro,” is a quick reference to the ZigBee application API.

Appendix B, “ZigBee Quick Reference,” is a quick reference to ZigBee architecture and commands.

Appendix C, “ZigBee Cluster Library Quick Reference,” covers some of the new features in ZigBee to be found in the upcoming ZigBee 2007, a specification that was not quite ready for publication at the time of this writing.

Example Source Code

Each chapter contains examples designed to enhance understanding of the ZigBee concepts introduced. Only partial source code is included in the text of this book.

For full source code, including Freescale CodeWarrior project files, go to the web site:

http://www.zigbookexamples.com/code

The home page of this site is just an advertisement for the book, so remember to type in /code after the site name. The sample code may be freely used in applications. A standard author's disclaimer applies:

No warrantee is implied or expressed and it's probably not suitable for anything other than instructional purposes, and maybe not even that. If you use the source code, keep the copyright text intact.
The code on the Web site is organized by chapters. Each example, except for the two in Chapter 1, contain only the application source code, and assume that you use Freescale’s BeeKit to generate the project. The whole process of taking small source code samples and incorporating them into the Freescale solution is described, step-by-step, in Chapter 3, “The ZigBee Development Environment.”
Acknowledgments

There are so many people that contributed to this book. First of all, I’d like to thank my wife, Alicia. Without her countless hours of encouragement and solid support of this arduous process called writing a book, this would not have been possible. And to my daughters, Lita, Genevieve, and Elanor, I love you.

To Rachel, my editor at Elsevier, a big thank you, especially for your patience. There is a White Chocolate Frappuccino® waiting for you at Starbucks®, my treat.

I’d like to thank all the staff at Freescale, in what’s now called Wireless Commercial Operations (WCO), especially Brett Black for believing in and championing this technology, Darrel Simms for introducing me to Freescale, Mark Williams for always supporting his partners, Walter Young whose command of the English language is greater than Strunk and White, Mads Westergreen—a Danish man who knows more about ZigBee than just about anybody on the planet, Matt Maupin, Ryan Kelly, Shannon Reid, and so many others as well.

Also, ZigBee Alliance members deserve many thanks for this book: Bob Heile, Zachary Smith, Ian Marsden, Don Sturek, Phil Jamieson, and Skip Ashton, all of whom have made the ZigBee standard possible. I really appreciate all the time you’ve spent explaining the concepts to me, and discussing the edge cases. You have taught me so much. And to others within the Alliance who have patiently answered my questions: Spiro Sacre, Monique Brown, Wally Burnham, Claudio Borean, Rudi Belliardi, Greg Henry, Silviu Chiricescu, and Bill Wood, thank you.

To my good friends and colleagues, Masaru and Blanca Natsu, Christian Garcia, and Dalila Pinedo, thank you for all your help, suggestions, corrections, and insight. And to
xvi  Acknowledgments

Tim Gillman who was the idea man behind many of the stories which open each chapter. Tim, you are a funny guy.

Special thanks to Mads Westergreen and Allan McDaniel for the iPod example. I think the readers will love this one.

Any mistakes, inaccuracies, or omissions in this text are purely my own.