

IT 先锋系列丛书

(影印本)

蓝牙揭密

Bluetooth
Demystified

Nathan J. Muller 著

人民邮电出版社
www.pptph.com.cn

麦格劳-希尔国际公司
www.mhhe.com

MC
Graw
Hill



IT 先锋系列丛书

蓝 牙 揭 密

(影印本)

Bluetooth Demystified

Nathan J. Muller

 人民邮电出版社 McGraw - Hill 

Nathan J. Muller: Bluetooth Demystified.

Copyright © 2001 by The McGraw – Hill Companies, Inc.

Authorized Reprinting by the People's Posts and Telecommunications Publishing House.

All rights reserved. For sale in the People's Republic of China only.

ISBN 0 – 07 – 136323 – 8

IE ISBN: 0 – 07 – 118995 – 5

本书英文影印版由人民邮电出版社和美国麦格劳 – 希尔国际公司合作出版, 未经出版者书面许可, 不得以任何方式复制或抄袭本书的任何部分。

版权所有, 翻印必究。

IT 先锋系列丛书

蓝牙揭密(影印本)Bluetooth Demystified

- ◆ 著 Nathan J. Muller
责任编辑 陈万寿
- ◆ 人民邮电出版社出版发行 北京市崇文区夕照寺街 14 号
邮编 100061 电子函件 315@ pptph.com.cn
网址 <http://www.pptph.com.cn>
读者热线: 010 – 67129212 010 – 67129211(传真)
北京汉魂图文设计有限公司制作
北京顺义振华印刷厂印刷
新华书店总店北京发行所经销
- ◆ 开本: 800 × 1000 1/16
印张: 26 2001 年 4 月第 1 版
印数: 1 – 5 000 册 2001 年 4 月北京第 1 次印刷
著作权合同登记 图字: 01 – 2001 – 0966 号
ISBN 7-115-09140-4/TN·1699

定价: 49.00 元

35666/01

To a new friend, who seems like an old friend...

Genie Williams

PREFACE

Bluetooth™ wireless technology has become a global technology specification for “always on” wireless communication between portable devices and desktop machines and peripherals. Among the many things Bluetooth wireless technology enables users to do is swap data and synchronize files without having to cable devices together. Data exchange can be as simple as transferring business card and calendar information from a mobile phone to a hand-held computer, or synchronizing personal information between a palmtop and desktop computer, merely by having the devices come within range of each other. Even photos from a digital camera can be dropped off at a PC for editing or to a color printer for output—all without having to connect cables, load files, and open applications. And since the wireless link has a range of 30 feet (10 meters), users have more mobility than ever before. Without cables, the work environment also looks and feels more comfortable and inviting.

Bluetooth technology can also be used to make wireless data connections to conventional local area networks (LANs) via an access point equipped with a Bluetooth radio transceiver that is wired to the LAN. Once a wireless connection is established with one of these access points, a mobile device can access any of the resources on that LAN, including printers, database servers, and the Internet. If desired, a user might tap out an e-mail reply on a palmtop, tell it to make an Internet connection through a mobile phone, print a copy on a printer nearby, and archive the original on the desktop PC—all while walking down the hall to a meeting.

The Bluetooth baseband protocol is a combination of circuit- and packet-switching, making it suitable for voice as well as data. For example, instead of fumbling with a cell phone while driving, the user can wear a lightweight headset to answer a call and engage in a conversation without even taking the phone out of a briefcase or purse. Or the cell phone can be used to communicate through a base station in the home or office as if it were a cordless phone connected to the Public Switched Telephone Network (PSTN). Users can also connect to each other directly

Bluetooth is a trademark owned by Telefonaktiebolaget L M Ericsson, Sweden.

over a limited range through their telephones using Bluetooth wireless technology, without incurring usage charges from a service provider.

No matter what the application, data or voice, Bluetooth wireless technology is intended to replace cable connections between computers, peripherals, and other electronic devices. With Bluetooth technology, making connections is as easy as powering up the device. There is no need for the user to open an application or press a button to initiate a process. In fact, one of the main advantages of Bluetooth wireless technology is that it does not need to be set up—it is always on, running in the background. The Bluetooth protocols scan for other Bluetooth devices and when they come within range of each other, start to exchange messages so they can become aware of each other's capabilities, establish connections and, if needed, arrange for security to protect sensitive data during transmission. The devices do not even require a line of sight to communicate with each other.

Bluetooth technology can be used for a variety of purposes, eliminating the need for multiple types of cable connections. With a radio link, users can think about what they are working on, rather than how to cable everything together to achieve connectivity between the various devices. Within a few years, about 80 percent of mobile phones are expected to carry a Bluetooth chip that can provide a wireless connection to similarly equipped notebook computers, printers and, potentially, any other digital device.

The Bluetooth radio transceivers operate in the globally available unlicensed ISM radio band of 2.4 GHz. The ISM (industrial, scientific, and medical) bands include the frequency ranges at 902 MHz to 928 MHz and 2.4 GHz to 2.484 GHz, which do not require an operator's license from a regulatory agency, such as the Federal Communications Commission (FCC) in the US. The use of a generally available frequency band means that devices using Bluetooth wireless technology can be used virtually anywhere in the world and link up with other such devices for ad hoc networking when they come within range of each other.

There will be points of convergence between Bluetooth and other wireless technologies. Infrared and Bluetooth technologies, for example, provide complementary implementations for data exchange and voice applications. Bluetooth complements infrared's point-and-shoot ease of use with omni-directional signaling, longer distance communications, and capacity to penetrate through walls. For some devices, having both Bluetooth and infrared will provide the optimal short-range wireless solution. For other devices, the choice of adding Bluetooth or infrared wireless technology will be based on the applications and intended usage models.

As the number and types of computer and communications devices continue to proliferate, establishing the connectivity between them becomes the critical issue. What everyone needs is an economical wireless solution that is convenient, reliable, easy to use, and operates over a longer distance than infrared without requiring a clear line of sight. Of the many emerging wireless solutions that attempt to address one or more of these needs, there is only one promising enough to elicit the support of a broad base of vendors representing all segments of the computer and communications markets—Bluetooth.

Since its initial development in 1994 by the Swedish telecommunications firm, Ericsson, over 1800 companies worldwide have signed on as members of the Bluetooth Special Interest Group (SIG) to build products to the wireless specification and promote the new technology in the marketplace. The sheer number and diversity of companies involved in the Bluetooth SIG is indicative of where the computer and communications industries are headed: Bluetooth wireless technology enables seamless voice and data transmission via short-range radio, allowing users to connect a wide range of devices easily and quickly, without the need for cables, thus expanding communications capabilities for mobile phones and handheld computing devices.

Bluetooth wireless technology has been greeted with unparalleled enthusiasm throughout the computer and communications industries. It is widely anticipated that soon people all over the world will enjoy the convenience, speed and security of instant wireless connections. To meet these expectations, Bluetooth wireless technology is expected to be embedded in hundreds of millions of mobile phones, PCs, laptops and a whole range of other electronic devices in the next few years. This book explains the advantages that Bluetooth wireless technology provides to users for a variety of applications and discusses the key operational details of the technology and its relationship to the emerging third-generation global wireless infrastructure.

The information contained in this book, especially as it relates to specific vendors and products, is believed to be accurate at the time it was written and is, of course, subject to change with continued advancements in technology and shifts in market forces. Mention of specific products and services is for illustration purposes only and does not constitute an endorsement of any kind by either the author or the publisher.

Nathan J. Muller

CONTENTS

Preface	xv
1 The Case for Bluetooth	1
What About Infrared?	2
Infrared and Bluetooth?	3
Speed Differential	4
Wireless to Wireline	4
Dialup to the Internet	5
How About Wireless LANs?	6
HomeRF Networks	8
Bluetooth Advantage	13
Origin of Bluetooth	14
What's With the Name?	15
Bluetooth Technology	16
Types of Links	17
Ad Hoc Networking	17
Voice over Bluetooth	18
Video over Bluetooth	19
Radio Link	21
Interference	21
Safety	22
Personal Area Networks	22
Bluetooth Topology	23
Security	25
What Can You Do With Bluetooth?	26
Presentations	26
Card Scanning	27
Collaboration	27
Synchronizing Data	27
Remote Synchronization	28

Printing	28
In-Car Systems	29
Communicator Platforms	29
Electronic Books	30
Travel	31
Home Entertainment	32
Payment Systems	32
Scanners	33
Behavior Enforcement	34
Mobile E-commerce	34
Java and Bluetooth	37
Jini and Bluetooth	38
Other Connectivity Solutions	40
JetSend	40
HAVi	41
Global 3G Wireless Framework	42
Problems with Bluetooth	44
Bluetooth Qualification Program	45
Market for Bluetooth	45
Summary	46
2 Basic Concepts	49
Serial versus Parallel	50
Serial Transmission	51
Parallel Transmission	51
Asynchronous versus Synchronous	53
Asynchronous	54
Synchronous	57
Spread Spectrum	60
Spreading	62
Direct Sequence	64
Frequency Hopping	65
Circuit and Packet Switching	66
Time Division Duplexing	68
Physical Links	74
SCO Links	74
ACL Links	75
Peeking into Packets	75

Bluetooth Packets	77
Access Code	77
Header	79
Payload	81
Logical Channels	82
Client-Server Architecture	83
Architectural Model	83
Service Discovery	86
Summary	88
3 Bluetooth Protocol Architecture	89
What Are Protocols?	90
Open Systems Interconnection	91
Application Layer	92
Presentation Layer	94
Session Layer	95
Transport Layer	96
Network Layer	97
Data-Link Layer	98
Physical Layer	99
Bluetooth Protocol Stack	101
Bluetooth Core Protocols	103
Baseband	104
Link Manager Protocol (LMP)	104
Logical Link Control and Adaptation Protocol	105
Service Discovery Protocol (SDP)	105
Cable Replacement Protocols	105
RFCOMM	105
Telephony Control Protocols	107
Adopted Protocols	107
PPP	107
TCP/UDP/IP	108
OBEX Protocol	110
Wireless Application Protocol (WAP)	111
WAP Applications Environment (WAE)	113
Content Formats	116
Usage Models and Profiles	118
Summary	120

4 Link Management	121
Types of PDUs	123
General Response Messages	127
Authentication	127
Pairing	128
Changing the Link Key	129
Changing the Current Link Key	130
Changing a Temporary Link Key	130
Encryption	131
Clock Offset Request	133
Slot Offset Information	133
Timing Accuracy Information Request	134
LMP Version	134
Supported Features	136
Switching of Master-Slave Role	136
Name Request	137
Detach	137
Hold Mode	137
Sniff Mode	138
Park Mode	139
Power Control	140
Channel Quality-Driven Change of Data Rate	141
Quality of Service (QoS)	142
SCO Links	143
Control of Multi-Slot Packets	144
Paging Scheme	145
Link Supervision	146
Connection Establishment	146
Test Modes	147
Error Handling	147
Summary	148
5 Logical Link Control	149
L2CAP Functions	151
Basic Operation	152
Channel Identifiers	153
Segmentation and Reassembly	154

State Machine	155
Events	157
Actions	161
Channel Operational States	163
Mapping Events to Actions	164
Data Packet Format	168
Connection-Oriented Channel	168
Connectionless Data Channel	169
Signaling	170
Packet Structure	170
Signaling Commands	171
Configuration Parameter Options	173
Packet Structure	173
Options	174
Configuration Process	175
Service Primitives	176
Event Indication	176
Connect	176
Connect Response	177
Configure	177
Configuration Response	177
Disconnect	177
Write	177
Read	178
Group Create	178
Group Close	178
Group Add Member	178
Group Remove Member	178
Get Group Membership	179
Ping	179
Get Info	179
Disable Connectionless Traffic	179
Enable Connectionless Traffic	179
Summary	179
6 Bluetooth General Profiles	181
Generic Access Profile	182
Common Parameters	184

Idle Mode Procedures	186
Bonding	187
Establishment Procedures	188
Serial Port Profile	190
Application-Level Procedures	191
Power Mode and Link Loss Handling	193
RS-232 Control Signals	193
L2CAP Interoperability Requirements	194
SDP Interoperability Requirements	195
Link Manager Interoperability Requirements	195
Service Discovery Application Profile	196
Client and Server Roles	197
Pairing	199
Service Discovery Application	200
Message Sequence	202
Service Discovery	202
Signaling	203
Configuration Options	204
SDP Transactions and L2CAP Connections	204
Link Manager	206
Link Control	208
Generic Object Exchange Profile (GOEP)	210
Profile Stack	211
Server and Client	211
Profile Basics	212
Features	213
OBEX Operations	213
Summary	214
7 Bluetooth Profiles for Usage Models	217
Intercom Profile	218
Call Procedures	221
Message Summary	223
Call Failure	223
Cordless Telephony Profile	225
Device Roles	226
Typical Call Scenarios	227
Features	229

Contents

Terminal-to-Gateway Connection	230
Terminal-to-Terminal Connection	231
Call Control	232
Group Management	234
Periodic Key Update	235
Inter-Piconet Capability	236
Service Discovery Procedures	236
LMP Procedures	237
Link Control Features	238
GAP Compliance	239
Headset Profile	241
Profile Restrictions	243
Basic Operation	243
Features	244
Link Control Features	246
GAP Compliance	247
Dialup Networking Profile	248
Profile Restrictions	250
Basic Operation	250
Services	251
Gateway Commands	251
Audio Feedback	253
Service Discovery Procedures	254
Link Control Features	254
GAP Compliance	254
Fax Profile	256
Profile Restrictions	257
Basic Operation	258
Services	259
Gateway Commands	259
Audio Feedback	260
Service Discovery Procedures	260
Link Control Features	260
GAP Compliance	260
LAN Access Profile	261
Profile Restrictions	263
Basic Operation	264
Security	265

GAP Compliance	265
Service Discovery Procedures	266
Link Control	267
Management Entity Procedures	267
File Transfer Profile	268
Basic Operation	270
Functions	270
Features	271
OBEX Operations	272
Service Discovery Procedures	273
Object Push Profile	273
Functions	275
Basic Operation	276
Features	277
Content Formats	277
OBEX Operations	278
Service Discovery Procedures	278
Synchronization Profile	279
Basic Operation	281
Features	283
OBEX Operations	284
Service Discovery Procedures	284
Summary	286
8 Bluetooth Security	289
Security Modes	290
Link-level Security	291
A Matter of Trust	292
Flexible Access	293
Implementation	293
Architecture Overview	294
Security Level of Services	296
Connection Setup	296
Authentication on Baseband Link Setup	297
Protocol Stack Handling	298
Registration Procedures	299
External Key Management	301
Access Control Procedures	301

Connectionless L2CAP	301
Security Manager	301
Interface to L2CAP	305
Interface to Other Multiplexing Protocols	306
Interface to ESCE	306
Registration Procedures	306
Interface to HCI/Link Manager	307
Summary	308
9 Bluetooth in the Global Scheme of 3G Wireless	309
The IMT-2000 Vision	311
Spanning the Generations	311
Current 2G Networks	314
Time Division Multiple Access	314
Code Division Multiple Access	316
CDMA versus TDMA	317
GSM	318
Global 3G Initiative	326
Standards Development	326
Goals of IMT-2000	328
Universal Mobile Telecommunications System	329
U.S. Participation in 3G	334
CDMA Proposals	334
TDMA Proposal	338
Role of Bluetooth	339
Summary	341
Appendix A	343
Contributors to the Bluetooth Specification	343
Appendix B	347
Terms and Definitions	347
Appendix C	371
Acronyms	371
Index	381

CHAPTER

1

The Case for Bluetooth