

# Contents

## Foreword

xxv

## Chapter 1

### Introducing Bluetooth Applications

1

Introduction	2
Why Throw Away Wires?	3
Adding Usability to Products	6
Allowing for Interference	7
Considering Connection Times	8
Coping with Limited Bandwidth	9
Considering Power and Range	9
Deciding on Acceptable Range	10
Recognizing Candidate Bluetooth Products	10
Considering Product Design	11
Are You Adding End User Value?	11
Investigating Convenience	12
Enhancing Functionality	15
Do You Have Time?	17
Investigating Product Performance	18
Evaluating Connection Times	19
Discovering Devices	20
Connecting Devices	21
Quantifying Connection Times	22
Performing Service Discovery	24
Quality of Service in Connections	25
Data Rate	25
Latency	27
Delivering Voice Communications	28

#### Connecting Devices

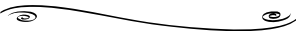
The page scanning device's Bluetooth Device Address can be obtained in several ways:

- From an inquiry response via FHS
- From user input
- By preprogramming at manufacture

Investigating Interference	29
Interfering with Other Technologies	31
Coexisting Piconets	32
Using Power Control	34
Aircraft Safety	35
Assessing Required Features	36
Enabling Security	36
Using Low Power Modes	37
Hold Mode	37
Sniff Mode	38
Park Mode	38
Unparking	39
Which Devices Need Low Power Modes?	39
Providing Channel Quality Driven Data Rate	40
Deciding How to Implement	40
Choosing a System Software Architecture	40
Constraining Implementation Options	
with Profiles	43
Choosing a Hardware Implementation Option	43
Design Bluetooth Directly Onto the PCB	45
Design Verification	49
Manufacturing	50
Using a Prequalified Complete Bluetooth	
Module	51
Firmware Versions	53
Dependant for Functionality	53
Considering Battery Limitations	55
Adding Batteries	56
Using Power Saving Modes to Extend	
Battery Life	57
Assessing Battery Life	58
Summary	64
Solutions Fast Track	65
Frequently Asked Questions	67

<b>Chapter 2</b>	
<b>Exploring the Foundations of Bluetooth</b>	<b>69</b>
Introduction	70
Reviewing the Protocol Stack	70
L2CAP	71
RFCOMM	72
OBEX	73
PPP	73
TCS Binary	73
SDP	74
Management Entities	74
HCI	74
Lower Layers	74
Why Unconnected Devices Need to Talk	75
Discovering Neighboring Devices	77
Inquiring and Inquiry Scanning	77
Timing	80
When to Stop	81
Connecting to a Device	82
Paging and Page Scanning	82
Timing	86
Who Calls Who?	88
Finding Information on Services a Device Offers	88
Connecting to and Using Bluetooth Services	91
Summary	98
Solutions Fast Track	99
Frequently Asked Questions	101

**Relationship between SP Mode and Mandatory Page Scan Period**



Scan Period Mode	T <sub>mandatory_pscan</sub>
P0	>20 seconds
P1	>40 seconds
P2	>60 seconds

## Chapter 3 Power Management 103

Introduction	104
Using Power Management: When and Why Is It Necessary?	104
Investigating Bluetooth Power Modes	106
Active Mode	106
Hold Mode	107
Sniff Mode	110
Park Mode	113
Evaluating Consumption Levels	117
Summary	120
Solutions Fast Track	121
Frequently Asked Questions	122

### Using Power Management: When and Why Is It Necessary?

- Consider whether your application is suitable for power-managed operation.
- Consider the constraints imposed by the application (e.g., maximum response times, characteristics of the data traffic, and so on).

## Chapter 4 Security Management 125

Introduction	126
Deciding When to Secure	126
Outfitting Your Security Toolbox	127
Authentication	128
Pairing	129
Link Keys	130
Bonding	130
Application Involvement	132
Authorization: How and Why?	132
Using the Trust Attribute	133
Enabling Encryption	133
Point-to-Point Encryption	134
Broadcasting	134
Application Involvement	135
Understanding Security Architecture	135
The Role of the Security Manager	135
Mode 1 Role	138
Mode 2 Role	138
Mode 3 Role	141
Mode Unknown	142

	The Role of Security Databases	143
	Service Database Content	143
	Service Database Operations	144
	Role of Device Databases	146
	Device Database Content	146
	Device Database Operations	147
	Managing the Device Database for Your Applications	147
	Working with Protocols and Security Interfaces	148
	Mode 2 Operation	148
	Mode 3 Operation	150
	Application—API Structure	150
	Exploring Other Routes to Extra Security	153
	Invisibility	154
	Application Level Security	154
	Implementing Security Profiles	155
	SDP	155
	Cordless Telephony and Intercom	156
	Serial Port Profile	156
	Headset Profile	157
	Dial-Up Network and FAX	157
	LAN Access	158
	OBEX	159
	Case Study	161
	Summary	162
	Solutions Fast Track	162
	Frequently Asked Questions	164
<b>Security Modes</b>		
<p>There are three different modes associated with Bluetooth security:</p> <ul style="list-style-type: none"> <li>■ Mode 1 has no security, obviously making it the least secure mode.</li> <li>■ Mode 2 invokes security when a higher layer protocol or service is accessed.</li> <li>■ Mode 3 invokes security when a connection is requested; this is the most secure mode.</li> </ul>		
	<b>Chapter 5</b>	
	<b>Service Discovery</b>	<b>167</b>
	Introduction	168
	Introduction to Service Discovery	169
	Service Discovery Protocols	170
	Bluetooth SDP	171
	Architecture of Bluetooth Service Discovery	172
	The Structure of Service Records	172
	The Service Discovery Protocol	175

Developing an Abstract C API for SDP	176
Discovering Services	180
Short-Circuiting the Service Discovery Process	181
Creating and Advertising a Service	181
Discovering Specific Services	186
Using Service Attributes	187
Browsing for Services	189
Service Discovery Application Profile	192
Service Discovery Non-Application Profiles	193
Java, C, and SDP	195
Other Service Discovery Protocols	196
Salutation	197
Service Location Protocol	198
Jini	200
Universal Plug and Play (UPnP)	202
The Future of SDP	203
Summary	204
Solutions Fast Track	205
Frequently Asked Questions	209

## Answers to Your Frequently Asked Questions

**Q:** How are services represented in SDP?

**A:** A service on a Bluetooth device is described in an SDP service record, which is stored in the device's "Service Discovery Database." A service record consists of service attributes, each of which describes some information about the available service.

<b>Chapter 6</b>	
<b>Linux Bluetooth Development</b>	<b>211</b>
Introduction	212
Assessing Linux Bluetooth Protocol Stacks	212
Comparing BlueDrekar with OpenBT	
by Features	213
Kernel Versions	214
Hardware Platforms	214
Bluetooth Protocols	214
SDP Support	214
API	215
License Terms	215
Other Considerations	216
Fair Warning	217
Understanding the Linux Bluetooth Driver	217

Learning about the Kernel Driver	218
Investigating the Kernel Module	218
What Exactly Is a TTY?	219
So What's an ldisc?	219
Building Driver Stacks in the Linux Kernel	220
Understanding the Bluetooth Driver Interface	221
Investigating the Bluetooth Device Files	221
Using the RFCOMM TTY Drivers	222
Using the Control Driver	226
Using Open Source Development Applications	226
Investigating the OpenBT Applications	226
Understanding the btd and btduser Applications	227
Understanding the sdp_Server Application	227
Understanding the BluetoothPN Application	228
Establishing a PPP Connection Using the btd Application	228
Writing Your Own Minimal Application	231
Connecting to a Bluetooth Device	233
Initializing the Bluetooth Stack	234
Preparing the Serial Driver	234
Stacking the Drivers	235
Starting Communication between the PC and the Card	236
Switching to a Higher Baud Rate	237
Finding Neighboring Devices	238
Letting Other Bluetooth Devices Discover Us	239
Sending an HCI Inquiry	239
Using Service Discovery	241
Connecting to a Remote SDP Server	241
Sending an SDP Request	242

### Security Alert

Never remove the Bluetooth driver while the sdp\_server daemon is using /proc/sdp\_srv. If you do so in the current release version of the stack (0.0.2 at the time of this writing), you will get a kernel panic when you stop the daemon. Future versions of the stack will probably not allow you to remove the driver while the sdp\_server daemon is using it.

Processing an SDP Response	244
Adding a Service to the Local Database	246
Querying the Local Database	247
Connecting to a Bluetooth Service	247
Using a Data Device	247
Creating a Connection	248
Accepting a Connection	249
Transferring Data	249
Disconnecting	250
Controlling a Bluetooth Device	251
Distinguishing between Control and Data Applications	252
Using ioctls to Control the Device	252
Covering Basic Scenarios	255
Example: Startup	255
Example: Link Loss	255
Example: User-Initiated and Automated Shutdown	257
Example: Idle Operation	257
Summary	259
Solutions Fast Track	260
Frequently Asked Questions	262

## Chapter 7

### **Embedding Bluetooth Applications 265**

Introduction	266
Understanding Embedded Systems	267
Understanding Tasks, Timers, and Schedulers	267
Understanding Messaging and Queues	268
Using Interrupts	268
Getting Started	271
Installing the Tool Set	273
Building a Sample Application	273
Running an Application under the Debugger	274
Using Plug-Ins	276
Debugging under BlueLab	280
Running an Application on BlueCore	280



### The Casira Development Kit

The Casira development kit provides a variety of useful interfaces:

- **SPI interface**  
Connects to a PC parallel port, and allows you to reconfigure the Casira using the PSTool utility.
- **Serial interface**  
Connects to a PC serial port.
- **USB port** Connects to a PC USB port, and supports the Bluetooth Specification's USB protocol (H2).
- **Audio I/O** An audio jack which connects to the headsets supplied with the Casira.
- **LEDs** These can be used to monitor applications running on the BlueCore chip.
- **PIO lines** Parallel Input-Output lines; useful for connecting custom hardware.

Debugging Using VM Spy	283
Using VM Packets	284
Packing Format in Messages	287
Using the BlueLab Libraries	288
Basic Libraries	290
CSR Library	291
Application Libraries	291
Using Tasks and Messages	293
Tasks and Message Queues	293
Creating and Destroying Messages	294
Using the MAKE_MSG Macro	295
Connection Manager	296
Initializing and Opening the Connection Manager	297
Inquiry	302
Pairing	304
Connecting	306
Sending Data	311
Using Other Messages and Events	312
Deploying Applications	313
Summary	314
Solutions Fast Track	314
Frequently Asked Questions	316

## Chapter 8 Using the Palm OS for Bluetooth Applications

317

Introduction	318
What You Need to Get Started	318
Understanding Palm OS Profiles	320
Choosing Services through the Service Discovery Protocol	322
Updating Palm OS Applications Using the Bluetooth Virtual Serial Driver	324
Creating a VDRV Client-Only Application	329
Creating a VDRV Server-Only Application	332

Using Bluetooth Technology with Exchange Manager	335
Creating Bluetooth-Aware Palm OS Applications	337
Using Basic ACL Links	339
Creating L2CAP and RFCOMM Connections	346
Using the Service Discovery Protocol	359
Advertising a Basic Service Record for an RFCOMM or L2CAP Listener Socket	360
Retrieving Connection Information about L2CAP and RFCOMM Listeners on a Remote Device	361
Using Bluetooth Security on Palm OS	364
Writing Persistent Bluetooth Services for Palm OS	364
The Future of Palm OS Bluetooth Support	369
Summary	370
Solutions Fast Track	372
Frequently Asked Questions	376

**Warning**

Applications and the VDRV use the Bluetooth Library in different modes.

Because of this difference, the VDRV will not be able to open while the application is holding the Bluetooth stack open.

<b>Chapter 9</b>	
<b>Designing an Audio Application</b>	<b>379</b>
Introduction	380
Choosing a Codec	381
Pulse Code Modulation	383
Continuous Variable Slope Delta Modulation	385
Configuring Voice Links	389
Choosing an HV Packet Type	390
Sending Data and Voice Simultaneously	391
Using ACL Links for High-Quality Audio	393
Choosing an Audio Interface	395
Selecting an Audio Profile	396
Applications Not Covered by Profiles	401
New Audio Profiles	402
Writing Audio Applications	402
Discovering Devices	403

Using Service Discovery	405
Connecting to a Service	407
Using Power Saving with Audio	
Connections	409
Differentiating Your Audio Application	410
Physical Design	410
Designing the User Interface	410
Enabling Upgrades	411
Improving the Audio Path	412
Summary	413
Solutions Fast Track	413
Frequently Asked Questions	417

### Choosing a Codec

The Bluetooth specification supports three different audio coding schemes on the air interface:

- Continuous Variable Slope Delta Modulation (CVSD)
- Log Pulse Code Modulation (PCM) coding using A-law compression
- Log PCM with  $\mu$ -law compression

<b>Chapter 10</b>	
<b>Personal Information Base Case Study</b>	<b>419</b>
Introduction	420
Why Choose Bluetooth Technology?	422
Requirements for PIB Devices	422
Implementing Optional Extra Features	425
Choosing a Wireless Technology for the PIB Device	427
Considering the Cost of the PIB	428
Exploring the Safety and Security Concerns of a Personal Information Base	429
Enabling Data Duplication	429
Ensuring Data Integrity	430
Providing Security	431
Meeting Medical Requirements	432
Using Bluetooth Protocols to Implement a PIB	432
Understanding the Bluetooth Specification Hierarchy	433
Initializing the PIB	437
Understanding User Interactions	437
Sending and Receiving Information	438
Selecting a Device	448
Using the Service Discovery Application Profile	449

Using the Serial Port Profile	449
Using the Generic Object Exchange Profile	450
Using the Object Push Profile	450
Using the File Transfer Profile	450
Considering the User's View	454
Identifying the System's Users	454
Identifying System Use Cases	455
Identifying Barriers to Adoption	455
Managing Personal Information Base Performance	456
Summary	458
Solutions Fast Track	459
Frequently Asked Questions	460
<b>Appendix:</b>	
<b>Bluetooth Application Developer's Guide Fast Track</b>	<b>463</b>
<b>Glossary</b>	<b>483</b>
<b>Index</b>	<b>492</b>