

Specification of the **Bluetooth®** System



Specification Volume 0

Master Table of Contents & Compliance Requirements

Covered Core Package version: 4.1

Publication date: 03 December 2013







Revision History

The Revision History is shown in the “[Appendix](#)” on page 61[Vol. 0].

Contributors

The persons who contributed to this specification are listed in the [Appendix](#).

Web Site

This specification can also be found on the official Bluetooth web site:
<http://www.bluetooth.com>

Disclaimer and Copyright Notice

The copyright in these specifications is owned by the Promoter Members of Bluetooth SIG, Inc. (“Bluetooth SIG”). Use of these specifications and any related intellectual property (collectively, the “Specification”), is governed by the Promoters Membership Agreement among the Promoter Members and Bluetooth SIG (the “Promoters Agreement”), certain membership agreements between Bluetooth SIG and its Adopter and Associate Members (the “Membership Agreements”) and the Bluetooth Specification Early Adopters Agreements (“1.2 Early Adopters Agreements”) among Early Adopter members of the unincorporated Bluetooth special interest group and the Promoter Members (the “Early Adopters Agreement”). Certain rights and obligations of the Promoter Members under the Early Adopters Agreements have been assigned to Bluetooth SIG by the Promoter Members.

Use of the Specification by anyone who is not a member of Bluetooth SIG or a party to an Early Adopters Agreement (each such person or party, a “Member”), is prohibited. The legal rights and obligations of each Member are governed by their applicable Membership Agreement, Early Adopters Agreement or Promoters Agreement. No license, express or implied, by estoppel or otherwise, to any intellectual property rights are granted herein.

Any use of the Specification not in compliance with the terms of the applicable Membership Agreement, Early Adopters Agreement or Promoters Agreement is prohibited and any such prohibited use may result in termination of the applicable Membership Agreement or Early Adopters Agreement and other liability permitted by the applicable agreement or by applicable law to Bluetooth SIG or any of its members for patent, copyright and/or trademark infringement.



THE SPECIFICATION IS PROVIDED “AS IS” WITH NO WARRANTIES WHATSOEVER, INCLUDING ANY WARRANTY OF MERCHANTABILITY, NONINFRINGEMENT, FITNESS FOR ANY PARTICULAR PURPOSE, SATISFACTORY QUALITY, OR REASONABLE SKILL OR CARE, OR ANY WARRANTY ARISING OUT OF ANY COURSE OF DEALING, USAGE, TRADE PRACTICE, PROPOSAL, SPECIFICATION OR SAMPLE.

Each Member hereby acknowledges that products equipped with the Bluetooth® technology (“Bluetooth® Products”) may be subject to various regulatory controls under the laws and regulations of various governments worldwide. Such laws and regulatory controls may govern, among other things, the combination, operation, use, implementation and distribution of Bluetooth® Products. Examples of such laws and regulatory controls include, but are not limited to, airline regulatory controls, telecommunications regulations, technology transfer controls and health and safety regulations. Each Member is solely responsible for the compliance by their Bluetooth® Products with any such laws and regulations and for obtaining any and all required authorizations, permits, or licenses for their Bluetooth® Products related to such regulations within the applicable jurisdictions. Each Member acknowledges that nothing in the Specification provides any information or assistance in connection with securing such compliance, authorizations or licenses. NOTHING IN THE SPECIFICATION CREATES ANY WARRANTIES, EITHER EXPRESS OR IMPLIED, REGARDING SUCH LAWS OR REGULATIONS.

ALL LIABILITY, INCLUDING LIABILITY FOR INFRINGEMENT OF ANY INTELLECTUAL PROPERTY RIGHTS OR FOR NONCOMPLIANCE WITH LAWS, RELATING TO USE OF THE SPECIFICATION IS EXPRESSLY DISCLAIMED. BY USE OF THE SPECIFICATION, EACH MEMBER EXPRESSLY WAIVES ANY CLAIM AGAINST BLUETOOTH SIG AND ITS PROMOTER MEMBERS RELATED TO USE OF THE SPECIFICATION.

Bluetooth SIG reserves the right to adopt any changes or alterations to the Specification as it deems necessary or appropriate.

Copyright © 1999 - 2013

Ericsson AB,
Lenovo, (Singapore) Pte. Ltd
Intel Corporation,
Microsoft Corporation,
Motorola Mobility, LLC,
Nokia Corporation,
Toshiba Corporation

*Third-party brands and names are the property of their respective owners.

MASTER TABLE OF CONTENTS

This table of contents (TOC) covers the entire Bluetooth Specification. In addition each volume has a TOC and each part of a volume is preceded by a detailed TOC.





THE BLUETOOTH SPECIFICATION MASTER TABLE OF CONTENTS

In the following Master Table of Contents:

- The TOC for each Volume starts at the top of a page.
- The Volume number in black is followed by the Volume name in red.

Note: Each Volume is a self contained book and is equipped with a TOC of its own.

- A Volume contains one or more Parts (A, B, etc.); each Part can be viewed independently and has its own TOC.

Red or blue text on the following pages indicates hypertext links that take you directly to the indicated section, on condition that you have access to a complete specification.





Specification Volume 0
Master Table of Contents & Compliance Requirements

Part A
MASTER TABLE OF CONTENTS
Part B
BLUETOOTH COMPLIANCE REQUIREMENTS

1	Introduction	47
2	Scope	48
3	Definitions	49
3.1	Types of Bluetooth Products	49
4	Core Configurations.....	54
4.1	Basic Rate Core Configuration.....	54
4.2	Enhanced Data Rate Core Configurations.....	55
4.3	High Speed Core Configuration	56
4.4	Low Energy Core Configuration	57
4.5	Basic Rate and Low Energy Combined Core Configuration	58
4.6	Host Controller Interface Core Configuration	59

Part C
APPENDIX

1	Revision History	65
1.1	[Vol 0] Master TOC & Compliance Requirements	65
1.2	[Vol 1] Architecture & Terminology Overview	65
1.3	[Vols 2, 3, 5, 6 & 7] Core System Package	67
1.4	[Vol 4] Transport Layers	69
2	Contributors.....	70
2.1	[Vol 0] Master TOC & Compliance Requirements	70
2.2	[Vol 1] Architecture & Terminology Overview	71
2.3	[Vol 2] Core System Package, Controller.....	75
2.4	[Vol 3] Core System Package, Host	101
2.5	[Vol 4] Host Controller Interface [Transport Layer]	114
2.6	[Vol 5] Core System Package [AMP Controller volume]	116
2.7	[Vol 6] Low Energy Specification	117
2.8	[Vol 7] Core System Package [Wireless Coexistence volume]	121



Specification Volume 1
Architecture & Terminology Overview

Part A
ARCHITECTURE

1	General Description	17
1.1	Overview of BR/EDR Operation	18
1.2	Overview of Bluetooth Low Energy Operation	20
1.3	Overview of AMP Operation	23
1.4	Nomenclature	24
2	Core System Architecture	30
2.1	Core Architectural Blocks	34
3	Data Transport Architecture	39
3.1	Core Traffic Bearers	40
3.2	Transport Architecture Entities	46
3.3	Physical Channels	50
3.4	Physical Links	60
3.5	Logical Links and Logical Transports	64
3.6	L2CAP Channels	75
4	Communication Topology and Operation	76
4.1	Piconet Topology	76
4.2	Operational Procedures and Modes	80
5	Security Overview	89
5.1	Security Architecture	89
5.2	BR/EDR Secure Simple Pairing	90
5.3	Secure Connections Only Mode	95
5.4	LE Security	96
5.5	AMP Security	97
6	Bluetooth Application Architecture	99
6.1	Bluetooth Profiles	99
6.2	Generic Access Profile	100
6.3	Profile Hierarchy	101
6.4	Generic Attribute Profile	101
6.5	GATT-based Profile Hierarchy	102



7	Coexistence and Collocation	104
7.1	Core Features Supporting Coexistence and Collocation	105
7.2	Adaptive Frequency Hopping.....	105
7.3	Coexistence Between Bluetooth Devices and Wireless LAN Devices	106
7.4	Mobile Wireless Standards (MWS) Coexistence.....	106
7.5	Synchronizing Bluetooth with an External Timing Source.....	109
7.6	Piconet Clock Adjustment	110

Part B

ACRONYMS & ABBREVIATIONS

1	List of Acronyms and Abbreviations.....	115
----------	--	------------

Part C

CORE SPECIFICATION CHANGE HISTORY

1	Deprecated Features.....	130
2	Changes from V1.1 to V1.2.....	131
2.1	New Features.....	131
2.2	Structure Changes	131
2.3	Deprecated Features list.....	131
2.4	Changes in Wording.....	132
2.5	Nomenclature Changes	132
3	Changes from V1.2 to V2.0 + EDR	133
3.1	New Features.....	133
3.2	Deprecated Features	133
4	Changes from V2.0 + EDR to V2.1 + EDR.....	134
4.1	New features.....	134
4.2	Deprecated Features	134
5	Changes From V2.1 + EDR To V3.0 + HS	135
5.1	New Features.....	135
5.2	Deprecated Features	135
6	Changes From V3.0 + HS To v4.0	136
6.1	New Features.....	136
6.2	Deprecated Features	136
7	Changes from v4.0 to v4.1	137
7.1	New Features.....	137
7.2	Deprecated Features	138



Part D
MIXING OF SPECIFICATION VERSIONS

1	Mixing of Specification Versions	142
1.1	Features and their Types	144
1.2	Core Specification Addenda	146

Part E
IEEE LANGUAGE

1	Use of IEEE Language	153
1.1	Shall	154
1.2	Must	154
1.3	Will	154
1.4	Should	154
1.5	May	155
1.6	Can	155



Specification Volume 2
Core System Package
[BR/EDR Controller volume]

Part A
RADIO SPECIFICATION

1	Scope	35
2	Frequency Bands and Channel Arrangement	37
3	Transmitter Characteristics	38
3.1	Basic Rate	40
3.2	Enhanced Data Rate	42
4	Receiver Characteristics	47
4.1	Basic Rate	47
4.2	Enhanced Data Rate	49
5	Appendix A	52
5.1	Nominal Test Conditions	52
5.2	Extreme Test Conditions	53
6	Appendix B	54
7	Appendix C	55
7.1	Enhanced Data Rate Modulation Accuracy	55

Part B
BASEBAND SPECIFICATION

1	General Description	66
1.1	Bluetooth Clock	67
1.2	Bluetooth Device Addressing	69
1.3	Access Codes	70
2	Physical Channels	71
2.1	Physical Channel Definition	72
2.2	Basic Piconet Physical Channel	72
2.3	Adapted Piconet Physical Channel	79
2.4	Page Scan Physical Channel	80
2.5	Inquiry Scan Physical Channel	84
2.6	Hop Selection	86
2.7	Synchronization Scan Physical Channel	99
3	Physical Links	102
3.1	Link Supervision for Active and Parked Physical Links	102
3.2	Link Supervision for Connectionless Slave Broadcast Physical Links	103



3.3	Authenticated Payload Timeout for Active Links.....	103
4	Logical Transports	104
4.1	General	104
4.2	Logical Transport Address (LT_ADDR)	104
4.3	Synchronous Logical Transports	105
4.4	Asynchronous Logical Transport	105
4.5	Transmit/Receive Routines	106
4.6	Active Slave Broadcast Transport.....	111
4.7	Parked Slave Broadcast Transport.....	112
4.8	Connectionless Slave Broadcast Logical Transport	112
5	Logical Links	113
5.1	Link Control Logical Link (LC).....	113
5.2	ACL Control Logical Link (ACL-C)	113
5.3	User Asynchronous/Isochronous Logical Link (ACL-U).....	114
5.4	User Synchronous Data Logical Link (SCO-S)	114
5.5	User Extended Synchronous Data Logical Link (eSCO-S).....	114
5.6	Logical Link Priorities	114
5.7	Profile Broadcast Data Logical Link	114
6	Packets.....	115
6.1	General Format.....	115
6.2	Bit Ordering.....	116
6.3	Access Code.....	117
6.4	Packet Header	122
6.5	Packet Types	124
6.6	Payload Format	135
6.7	Packet Summary	141
7	Bitstream Processing	143
7.1	Error Checking	144
7.2	Data Whitening	147
7.3	Error Correction	148
7.4	FEC Code: Rate 1/3	148
7.5	FEC Code: Rate 2/3	149
7.6	ARQ Scheme	150
7.7	Erroneous Synchronous Data Reporting	158
7.8	Message Integrity Check	158
8	Link Controller Operation	159
8.1	Overview of States	159
8.2	Standby State.....	160
8.3	Connection Establishment Substates	160
8.4	Device Discovery Substates	169
8.5	Connection State	174



8.6	Active Mode	176
8.7	Sniff Mode	193
8.8	Hold Mode	197
8.9	Park State	197
8.10	Connectionless Slave Broadcast Mode	205
8.11	Synchronization Establishment Substates	207
9	Audio	210
9.1	LOG PCM CODEC	210
9.2	CVSD CODEC	210
9.3	Error Handling	213
9.4	General Audio Requirements	213
10	List of Figures	214
11	List of Tables	217
11	Appendix	218

Part C

LINK MANAGER PROTOCOL SPECIFICATION

1	Introduction	231
2	General Rules	232
2.1	Message Transport	232
2.2	Synchronization	232
2.3	Packet Format	233
2.4	Transactions	234
2.5	Error Handling	235
2.6	Procedure Rules	236
2.7	General Response Messages	237
2.8	LMP Message Constraints	237
3	Device Features	238
3.1	General Description	238
3.2	Feature Definitions	238
3.3	Feature Mask Definition	246
3.4	Link Manager Interoperability policy	249
4	Procedure Rules	250
4.1	Connection Control	250
4.2	Security	275
4.3	Informational Requests	310
4.4	Role Switch	316
4.5	Modes of Operation	320
4.6	Logical Transports	334
4.7	Test Mode	342



5	Summary.....	348
5.1	PDU Summary	348
5.2	Parameter Definitions	359
5.3	LMP Encapsulated.....	370
5.4	Default Values.....	371
6	List of Figures	372
7	List of Tables	376

Part D

ERROR CODES

1	Overview of Error Codes.....	383
1.1	Usage Descriptions.....	383
1.2	HCI Command Errors	383
1.3	List of Error Codes.....	384
2	Error Code Descriptions	387
2.1	Unknown HCI Command (0x01).....	387
2.2	Unknown Connection Identifier (0x02).....	387
2.3	Hardware Failure (0x03).....	387
2.4	Page Timeout (0x04)	387
2.5	Authentication Failure (0x05).....	387
2.6	PIN or key Missing (0x06).....	387
2.7	Memory Capacity Exceeded (0x07).....	387
2.8	Connection Timeout (0x08).....	388
2.9	Connection Limit Exceeded (0x09).....	388
2.10	Synchronous Connection Limit to a Device Exceeded (0x0A)	388
2.11	ACL Connection Already Exists (0x0B)	388
2.12	Command Disallowed (0x0C)	388
2.13	Connection Rejected due to Limited Resources (0x0D)	388
2.14	Connection Rejected due to Security Reasons (0x0E).....	388
2.15	Connection Rejected due to Unacceptable BD_ADDR (0x0F)	389
2.16	Connection Accept Timeout Exceeded (0x10).....	389
2.17	Unsupported Feature or Parameter Value (0x11)	389
2.18	Invalid HCI Command Parameters (0x12).....	389
2.19	Remote User Terminated Connection (0x13)	389
2.20	Remote Device Terminated Connection due to Low Resources (0x14).....	390
2.21	Remote Device Terminated Connection due to Power Off (0x15).....	390
2.22	Connection Terminated by Local Host (0x16)	390
2.23	Repeated Attempts (0x17).....	390
2.24	Pairing not Allowed (0x18).....	390
2.25	Unknown LMP PDU (0x19).....	390



2.26	Unsupported Remote Feature / Unsupported LMP Feature (0x1A)	390
2.27	SCO Offset Rejected (0x1B)	390
2.28	SCO Interval Rejected (0x1C)	391
2.29	SCO Air Mode Rejected (0x1D)	391
2.30	Invalid LMP Parameters / Invalid LL Parameters (0x1E)	391
2.31	Unspecified Error (0x1F)	391
2.32	Unsupported LMP Parameter Value / Unsupported LL Parameter Value (0x20)	391
2.33	Role Change Not Allowed (0x21)	391
2.34	LMP Response Timeout / LL Response Timeout (0x22)	392
2.35	LMP Error Transaction Collision (0x23)	392
2.36	LMP PDU Not Allowed (0x24)	392
2.37	Encryption Mode Not Acceptable (0x25)	392
2.38	Link Key cannot be Changed (0x26)	392
2.39	Requested QoS Not Supported (0x27)	392
2.40	Instant Passed (0x28)	392
2.41	Pairing with Unit Key Not Supported (0x29)	392
2.42	Different Transaction Collision (0x2A)	393
2.43	QoS Unacceptable Parameter (0x2C)	393
2.44	QoS Rejected (0x2D)	393
2.45	Channel Assessment Not Supported (0x2E)	393
2.46	Insufficient Security (0x2F)	393
2.47	Parameter out of Mandatory Range (0x30)	393
2.48	Role Switch Pending (0x32)	393
2.49	Reserved Slot Violation (0x34)	393
2.50	Role Switch Failed (0x35)	394
2.51	Extended Inquiry Response Too Large (0x36)	394
2.52	Simple Pairing Not Supported By Host (0x37)	394
2.53	Host Busy–Pairing (0x38)	394
2.54	Connection Rejected Due To No Suitable Channel Found (0x39)	394
2.55	Controller Busy (0x3A)	394
2.56	Unacceptable Connection Parameters (0x3B)	394
2.57	Directed Advertising Timeout (0x3C)	395
2.58	Connection Terminated Due To MIC Failure (0x3D)	395
2.59	Connection Failed To Be Established (0x3E)	395
2.60	MAC Connection Failed (0x3F)	395
2.61	Coarse Clock Adjustment Rejected but Will Try to Adjust Using Clock Dragging (0x40)	395



Part E

HOST CONTROLLER INTERFACE FUNCTIONAL SPECIFICATION

1	Introduction	411
1.1	Lower Layers of the Bluetooth Software Stack	412
2	Overview of Host Controller Transport Layer	414
2.1	Host Controller Transport Layer and AMPS	414
3	Overview of Commands and Events	415
3.1	Generic Events	416
3.2	Device Setup	416
3.3	Controller Flow Control	417
3.4	Controller Information	418
3.5	Controller Configuration	420
3.6	Device Discovery	423
3.7	Connection Setup	426
3.8	Remote Information	431
3.9	Synchronous Connections	432
3.10	Connection State	434
3.11	Piconet Structure	437
3.12	Quality of Service	438
3.13	Physical Links	440
3.14	Host Flow Control	442
3.15	Link Information	444
3.16	Authentication and Encryption	446
3.17	Testing	453
3.18	Alphabetical List of Commands and Events	456
3.19	LE Controller Requirements	465
3.20	Connectionless Slave Broadcast	468
4	HCI Flow Control	470
4.1	Host to Controller Data Flow Control	470
4.2	Controller to Host Data Flow Control	473
4.3	Disconnection Behavior	473
4.4	Command Flow Control	474
4.5	Command Error Handling	474
5	HCI Data Formats	476
5.1	Introduction	476
5.2	Data and Parameter Formats	476
5.3	Handles	477
5.4	Exchange of HCI-Specific Information	479
6	HCI Configuration Parameters	487
6.1	Scan Enable	487
6.2	Inquiry Scan Interval	487



6.3	Inquiry Scan Window	488
6.4	Inquiry Scan Type	488
6.5	Inquiry Mode	488
6.6	Page Timeout.....	489
6.7	Connection Accept Timeout.....	489
6.8	Page Scan Interval.....	490
6.9	Page Scan Window.....	490
6.10	Page Scan Period Mode (Deprecated)	490
6.11	Page Scan Type.....	491
6.12	Voice Setting	491
6.13	PIN Type	492
6.14	Link Key	492
6.15	Failed Contact Counter	492
6.16	Authentication Enable	493
6.17	Hold Mode Activity	493
6.18	Link Policy Settings.....	493
6.19	Flush Timeout	495
6.20	Num Broadcast Retransmissions.....	495
6.21	Link Supervision Timeout.....	496
6.22	Synchronous Flow Control Enable.....	496
6.23	Local Name	497
6.24	Extended Inquiry Response.....	497
6.25	Erroneous Data Reporting	497
6.26	Class Of Device	498
6.27	Supported Commands	498
6.28	Logical Link Accept Timeout	507
6.29	Location Domain Aware	507
6.30	Location Domain	507
6.31	Location Domain Options.....	508
6.32	Location Options	508
6.33	Flow Control Mode	508
6.34	LE Supported Host.....	509
6.35	Simultaneous LE Host	509
6.36	Synchronization Train Interval.....	509
6.37	Synchronization Train Timeout.....	510
6.38	Service Data.....	510
6.39	Secure Connections Host Support.....	510
6.40	Authenticated Payload Timeout	511
6.41	Extended Page Timeout.....	511
6.42	Extended Inquiry Length	511



7	HCI Commands and Events	512
7.1	Link Control Commands	512
7.2	Link Policy Commands	625
7.3	Controller & Baseband Commands	650
7.4	Informational Parameters	795
7.5	Status Parameters	808
7.6	Testing Commands	836
7.7	Events	850
7.8	LE Controller Commands	958
8	List of Figures	1017
9	List of Tables	1018
10	Appendix A: Deprecated Commands, Events and Configuration Parameters	1019
10.1	Read Page Scan Mode Command	1020
10.2	Write Page Scan Mode Command	1021
10.3	Read Page Scan Period Mode Command	1022
10.4	Write Page Scan Period Mode Command	1023
10.5	Add SCO Connection Command	1024
10.6	Page Scan Mode Change Event	1026
10.7	Read Country Code Command	1027
10.8	Read Encryption Mode Command	1028
10.9	Write Encryption Mode Command	1029
10.10	Deprecated Parameters	1030

Part F

MESSAGE SEQUENCE CHARTS

1	Introduction	1037
1.1	Notation	1037
1.2	Flow of Control	1038
1.3	Example MSC	1038
2	Services Without Connection Request	1039
2.1	Remote Name Request	1039
2.2	One-time Inquiry	1041
2.3	Periodic Inquiry	1043
3	ACL Connection Establishment and Detachment	1045
3.1	Connection Setup	1046
4	Optional Activities After ACL Connection Establishment	1054
4.1	Authentication Requested	1054
4.2	Simple Pairing Message Sequence Charts	1056
4.3	Link Supervision Timeout Changed Event	1078
4.4	Set Connection Encryption	1079



4.5	Change Connection Link Key.....	1081
4.6	Change Connection Link Key with Encryption Pause and Resume.....	1082
4.7	Master Link Key	1083
4.8	Read Remote Supported Features	1085
4.9	Read Remote Extended Features.....	1086
4.10	Read Clock Offset	1087
4.11	Role Switch on an Encrypted Link using Encryption Pause and Resume.....	1088
4.12	Refreshing Encryption Keys.....	1089
4.13	Read Remote Version Information	1091
4.14	QOS Setup.....	1092
4.15	Switch Role	1093
4.16	AMP Physical Link Creation and Disconnect.....	1095
4.17	AMP Test Mode Sequence Charts	1103
5	Synchronous Connection Establishment and Detachment	1107
5.1	Synchronous Connection Setup.....	1107
5.2	Synchronous Connection Setup with Enhanced Synchronous Commands.....	1115
6	Sniff, Hold and Park	1121
6.1	Sniff Mode	1121
6.2	Hold Mode.....	1122
6.3	Park State.....	1125
7	Buffer Management, Flow Control.....	1129
8	Loopback Mode	1131
8.1	Local Loopback Mode	1131
8.2	Remote Loopback Mode	1134
9	Connectionless Slave Broadcast Services	1136
10	List of Figures.....	1140

**Part G****SAMPLE DATA**

1	Encryption Sample Data	1149
1.1	E0 Encryption Sample Data	1149
1.2	AES-CCM ENCRYPTION SAMPLE DATA	1184
2	Frequency Hopping Sample Data	1213
2.1	First set	1214
2.2	Second set	1220
2.3	Third set	1226
3	Access Code Sample Data	1232
4	HEC and Packet Header Sample Data	1235
5	CRC Sample Data	1236
6	Complete Sample Packets	1237
6.1	Example of DH1 Packet	1237
6.2	Example of DM1 Packet	1238
7	Simple Pairing Sample Data	1239
7.1	Elliptic Curve Sample Data	1239
7.2	Hash Functions Sample Data	1242
8	Whitening Sequence Sample Data	1254
9	FEC Sample Data	1257
10	Encryption Key Sample Data	1258
10.1	Four Tests of E1	1258
10.2	Four Tests of E21	1263
10.3	Three Tests of E22	1265
10.4	Tests of E22 With Pin Augmenting	1267
10.5	Four Tests of E3	1277
11	Connectionless Slave Broadcast Sample Data	1282

Part H**SECURITY SPECIFICATION**

1	Security Overview	1289
1.1	Pausing Encryption and Role Switch	1290
1.2	Change Connection Link Keys	1291
1.3	Periodically Refreshing Encryption Keys	1291
2	Random Number Generation	1292
3	Key Management	1293
3.1	Key Types	1293
3.2	Key Generation and Initialization	1295



4	Encryption (E0).....	1302
4.1	Encryption Key Size Negotiation.....	1303
4.2	Encryption of Broadcast Messages.....	1303
4.3	Encryption Concept.....	1304
4.4	Encryption Algorithm	1305
4.5	LFSR Initialization	1308
4.6	Key Stream Sequence	1311
5	Authentication	1312
5.1	Repeated Attempts	1315
6	The Authentication And Key-Generating Functions.....	1316
6.1	The Authentication Function E1	1316
6.2	The Functions Ar and A'r.....	1318
6.3	E2-Key Generation Function for Authentication.....	1320
6.4	E3-Key Generation Function for Encryption.....	1322
7	Secure Simple Pairing	1323
7.1	Phase 1: Public Key Exchange	1325
7.2	Phase 2: Authentication Stage 1	1325
7.3	Phase 3: Authentication Stage 2	1331
7.4	Phase 4: Link Key Calculation	1332
7.5	Phase 5: LMP Authentication and Encryption.....	1332
7.6	Elliptic Curve Definition	1332
7.7	Cryptographic Function Definitions	1334
8	AMP Security	1343
8.1	Creation of the Initial Generic AMP Link Key	1343
8.2	Creation of Dedicated AMP Link Keys	1343
8.3	Debug Considerations.....	1345
9	AES-CCM Encryption for BR/EDR	1346
9.1	Nonce Formats.....	1346
9.2	Counter Mode Blocks	1348
9.3	Encryption Blocks.....	1350
9.4	Encryption Key Size Reduction.....	1350
9.5	Repeated MIC Failures	1350
10	List of Figures.....	1351



Specification Volume 3
Core System Package
[Host volume]

Part A

**LOGICAL LINK CONTROL AND ADAPTATION PROTOCOL
SPECIFICATION**

1	Introduction	31
1.1	L2CAP Features	31
1.2	Assumptions	34
1.3	Scope.....	35
1.4	Terminology	35
2	General Operation.....	39
2.1	Channel Identifiers	39
2.2	Operation Between Devices	42
2.3	Operation Between Layers	43
2.4	Modes of Operation	44
2.5	Mapping Channels to Logical Links	46
3	Data Packet Format.....	47
3.1	Connection-oriented Channels in Basic L2CAP Mode	47
3.2	Connectionless Data Channel in Basic L2CAP Mode	48
3.3	Connection-oriented Channel in Retransmission/Flow Control/ Streaming Modes	49
3.4	Connection-Oriented Channels in LE Credit Based Flow Control Mode	57
4	Signaling Packet Formats	59
4.1	Command Reject (code 0x01)	62
4.2	Connection Request (code 0x02)	63
4.3	Connection Response (code 0x03)	64
4.4	Configuration Request (code 0x04)	66
4.5	Configuration Response (code 0x05)	68
4.6	Disconnection Request (code 0x06).....	70
4.7	Disconnection Response (code 0x07)	71
4.8	Echo Request (code 0x08)	71
4.9	Echo Response (code 0x09)	72
4.10	Information Request (code 0x0A)	72
4.11	Information Response (code 0x0B)	73
4.12	Extended Feature Mask.....	75
4.13	Fixed Channels Supported	76
4.14	Create Channel Request (code 0x0C).....	77
4.15	Create Channel Response (code 0x0D).....	78



4.16	Move Channel Request (code 0x0E)	79
4.17	Move Channel Response (code 0x0F).....	80
4.18	Move Channel Confirmation (code 0x10).....	81
4.19	Move Channel Confirmation Response (code 0x11).....	82
4.20	Connection Parameter Update Request (code 0x12)	82
4.21	Connection Parameter Update Response (code 0x13)	84
4.22	LE Credit Based Connection Request (Code 0x14).....	85
4.23	LE Credit Based Connection Response (Code 0x15).....	86
4.24	LE Flow Control Credit (Code 0x16)	88
5	Configuration Parameter Options.....	89
5.1	Maximum Transmission Unit (MTU).....	89
5.2	Flush Timeout Option.....	91
5.3	Quality of Service (QoS) Option.....	92
5.4	Retransmission and Flow Control Option.....	96
5.5	Frame Check Sequence (FCS) Option	101
5.6	Extended Flow Specification Option	102
5.7	Extended Window Size Option.....	107
6	State Machine	109
6.1	General rules for the state machine:	109
6.2	Timers events.....	125
7	General Procedures	130
7.1	Configuration Process.....	130
7.2	Fragmentation and Recombination	137
7.3	Encapsulation of SDUs	139
7.4	Delivery of Erroneous L2CAP SDUs.....	141
7.5	Operation with Flushing On ACL-U Logical Links	141
7.6	Connectionless Data Channel.....	142
7.7	Operation Collision Resolution.....	144
7.8	Aggregating Best Effort Extended Flow Specifications	144
7.9	Prioritizing Data over HCI.....	145
7.10	Supporting Extended Flow Specification for BR/EDR and BR/ EDR/LE Controllers.....	146
8	Procedures for Flow Control and Retransmission	148
8.1	Information Retrieval	148
8.2	Function of PDU Types for Flow Control and Retransmission ..	148
8.3	Variables and Sequence Numbers.....	149
8.4	Retransmission Mode	153
8.5	Flow Control Mode	160
8.6	Enhanced Retransmission Mode	164
8.7	Streaming Mode	194



9	Procedure for AMP Channel Creation and Handling	196
9.1	Create Channel.....	196
9.2	Move Channel.....	199
9.3	Disconnect Channel.....	207
10	Procedures for Credit Based Flow Control	208
10.1	LE Credit Based Flow Control Mode	208
11	List of Figures	209
12	List of Tables	211

Part B

SERVICE DISCOVERY PROTOCOL (SDP) SPECIFICATION

1	Introduction	221
1.1	General Description	221
1.2	Motivation	221
1.3	Requirements.....	221
1.4	Non-requirements and Deferred Requirements.....	222
1.5	Conventions	222
2	Overview	223
2.1	SDP Client-Server Architecture	223
2.2	Service Record	224
2.3	Service Attribute	226
2.4	Service Class.....	227
2.5	Searching for Services.....	228
2.6	Browsing for Services	229
3	Data Representation	232
3.1	Data Element	232
3.2	Data Element Type Descriptor	232
3.3	Data Element Size Descriptor.....	233
3.4	Data Element Examples	234
4	Protocol Description.....	235
4.1	Transfer Byte Order	235
4.2	Protocol Data Unit Format	235
4.3	Partial Responses and Continuation State	237
4.4	Error Handling.....	237
4.5	ServiceSearch Transaction.....	239
4.6	ServiceAttribute Transaction.....	242
4.7	ServiceSearchAttribute Transaction	245



5	Service Attribute Definitions	249
5.1	Universal Attribute Definitions	249
5.2	ServiceDiscoveryServer Service Class Attribute Definitions....	259
5.3	BrowseGroupDescriptor Service Class Attribute Definitions....	261
6	Security	262

Part C

GENERIC ACCESS PROFILE

1	Introduction	288
1.1	Scope	288
1.2	Symbols and Conventions	289
2	Profile Overview	291
2.1	Profile Stack	291
2.2	Profile Roles.....	291
2.3	User Requirements and Scenarios	295
2.4	Profile Fundamentals	295
2.5	Conformance	295
3	User Interface Aspects	296
3.1	The User Interface Level.....	296
3.2	Representation of Bluetooth Parameters	296
3.3	Pairing	300
4	Modes – BR/EDR Physical Transport.....	301
4.1	Discoverability Modes	301
4.2	Connectability Modes.....	305
4.3	Bondable Modes	307
4.4	Synchronizability Modes	308
5	Security Aspects – BR/EDR Physical Transport	309
5.1	Authentication	309
5.2	Security Modes	311
6	Idle Mode Procedures – BR/EDR Physical Transport.....	328
6.1	General Inquiry	328
6.2	Limited Inquiry.....	329
6.3	Name Discovery.....	331
6.4	Device Discovery	332
6.5	Bonding.....	334



7	Establishment Procedures – BR/EDR Physical Transport.....	337
7.1	Link Establishment.....	337
7.2	Channel Establishment.....	340
7.3	Connection Establishment	342
7.4	Establishment of Additional Connection	343
7.5	Synchronization Establishment.....	344
8	Extended Inquiry Response Data Format.....	345
9	Operational Modes and Procedures – LE Physical Transport.....	347
9.1	Broadcast Mode and Observation Procedure.....	347
9.2	Discovery Modes and Procedures	348
9.3	Connection Modes and Procedures	356
9.4	Bonding Modes and Procedures	367
10	Security Aspects – LE Physical Transport	370
10.1	Requirements.....	370
10.2	LE Security Modes.....	370
10.3	Authentication Procedure	372
10.4	Data Signing	379
10.5	Authorization Procedure	381
10.6	Encryption Procedure	381
10.7	Privacy Feature.....	381
10.8	Random Device Address	383
11	Advertising and Scan Response Data Format	387
12	GAP Service and Characteristics for GATT Server.....	388
12.1	Device Name Characteristic	389
12.2	Appearance Characteristic	389
12.3	Peripheral Preferred Connection Parameters Characteristic...	390
13	BR/EDR/LE Operation.....	392
13.1	Modes, Procedures and Security Aspects	392
13.2	Bonding for BR/EDR/LE Device Type.....	393
13.3	Relationship between Physical Transports	393
14	BR/EDR/LE Security Aspects.....	394
15	Bluetooth Device Requirements	395
15.1	Bluetooth Device Address	395
15.2	GATT Profile Requirements	395
15.3	SDP Requirements	396
15.4	SDP Service Record Requirement	396



16	Definitions	397
16.1	General Definitions	397
16.2	Connection-related Definitions	397
16.3	Device-related Definitions	398
16.4	Procedure-related Definitions	399
16.5	Security-related Definitions	399
17	Appendix A (Normative): Timers and Constants	401
18	Appendix B (Informative): Information Flows of Related Procedures	405
18.1	LMP – Authentication	405
18.2	LMP – Pairing	406
18.3	Service Discovery	407
18.4	Generating a Resolvable Private Address	407
18.5	Resolving a Resolvable Private Address	407
19	References	408

Part D

TEST SUPPORT

1	Test Methodology	417
1.1	BR/EDR Test Scenarios	417
1.2	AMP Test Scenarios	427
1.3	References	435
2	Test Control Interface (TCI)	436
2.1	Introduction	436
2.2	TCI Configurations	437
2.3	TCI Configuration and Usage	440



Part E

AMP MANAGER PROTOCOL SPECIFICATION

1	Introduction	449
1.1	General Description	449
2	General Operation.....	450
2.1	Basic Capabilities.....	450
2.2	AMP Manager Channel Over L2CAP	451
2.3	Using the AMP Manager Protocol	452
2.4	Controller IDs.....	454
2.5	Controller Types.....	454
3	Protocol Description.....	455
3.1	Packet Formats.....	455
3.2	AMP Command Reject (Code 0x01)	457
3.3	AMP Discover Request (Code 0x02).....	458
3.4	AMP Discover Response (Code 0x03)	459
3.5	AMP Change Notify (Code 0x04)	462
3.6	AMP Change Response (Code 0x05)	463
3.7	AMP Get Info Request (Code 0x06)	463
3.8	AMP Get Info Response (Code 0x07)	464
3.9	AMP Get AMP Assoc Request (Code 0x08)	466
3.10	AMP Get AMP Assoc Response (Code 0x09).....	466
3.11	AMP Create Physical Link Request (Code 0x0A).....	467
3.12	AMP Create Physical Link Response (Code 0x0B).....	468
3.13	AMP Disconnect Physical Link Request (Code 0x0C)	471
3.14	AMP Disconnect Physical Link Response (Code 0x0D).....	471
3.15	Create Physical Link Collision Resolution	473
3.16	Response Timeout.....	473
3.17	Unexpected BR/EDR Physical Link Disconnect	473

Part F

ATTRIBUTE PROTOCOL (ATT)

1	Introduction	481
1.1	Scope.....	481
1.2	Conformance	481
2	Protocol Overview	482
3	Protocol Requirements.....	483
3.1	Introduction	483
3.2	Basic Concepts	483
3.3	Attribute PDU	488
3.4	Attribute Protocol PDUs.....	492
4	Security Considerations.....	525



Part G

GENERIC ATTRIBUTE PROFILE (GATT)

1	Introduction	533
1.1	Scope	533
1.2	Profile Dependency	533
1.3	Conformance	533
1.4	Bluetooth Specification Release Compatibility	534
1.5	Conventions	534
2	Profile Overview	535
2.1	Protocol Stack	535
2.2	Configurations and Roles	535
2.3	User Requirements and Scenarios	536
2.4	Profile Fundamentals	536
2.5	Attribute Protocol	537
2.6	GATT Profile Hierarchy	541
2.7	Configured Broadcast	543
3	Service Interoperability Requirements.....	544
3.1	Service Definition	544
3.2	Include Definition	545
3.3	Characteristic Definition	545
3.4	Summary of GATT Profile Attribute Types	557
4	GATT Feature Requirements.....	558
4.1	Overview	558
4.2	Feature Support and Procedure Mapping.....	558
4.3	Server Configuration	560
4.4	Primary Service Discovery	561
4.5	Relationship Discovery.....	564
4.6	Characteristic Discovery	565
4.7	Characteristic Descriptor Discovery	568
4.8	Characteristic Value Read.....	570
4.9	Characteristic Value Write	573
4.10	Characteristic Value Notification	578
4.11	Characteristic Value Indications	579
4.12	Characteristic Descriptors	580
4.13	GATT Procedure Mapping to ATT Protocol Opcodes	583
4.14	Procedure Timeouts	585
5	L2CAP Interoperability Requirements.....	586
5.1	BR/EDR L2CAP Interoperability Requirements	586
5.2	LE L2CAP Interoperability Requirements	587



6	GAP Interoperability Requirements	589
6.1	BR/EDR GAP Interoperability Requirements	589
6.2	LE GAP Interoperability Requirements	589
6.3	Disconnected Events	590
7	Defined Generic Attribute Profile Service	591
7.1	Service Changed	591
8	Security Considerations.....	593
8.1	Authentication Requirements.....	593
8.2	Authorization Requirements.....	594
9	SDP Interoperability Requirements	595
10	References.....	596
11	Appendix: Example Attribute Server Attributes	597

Part H

SECURITY MANAGER SPECIFICATION

1	Introduction	607
1.1	Scope.....	607
1.2	Conventions	607
2	Security Manager	608
2.1	Introduction	608
2.2	Cryptographic Toolbox	609
2.3	Pairing Methods	613
2.4	Security in Bluetooth low energy	622
3	Security Manager Protocol	630
3.1	Introduction	630
3.2	Security Manager Channel over L2CAP	630
3.3	Command Format.....	630
3.4	SMP Timeout	631
3.5	Pairing Methods.....	632
3.6	Security in Bluetooth low energy	639
4	References.....	645
5	Appendices.....	648
5.1	Appendix A – EDIV and Rand Generation.....	648
5.2	Appendix B – Key Management	650
5.3	Message Sequence Charts.....	654



Specification Volume 4
Host Controller Interface
[Transport Layer]

Part A

UART TRANSPORT LAYER

1	General	13
2	Protocol	14
3	RS232 Settings	15
4	Error Recovery	16

Part B

USB TRANSPORT LAYER

1	Overview	21
2	USB Endpoint Expectations	25
	2.1 Descriptor Overview	25
	2.2 Control Endpoint Expectations	32
	2.3 Bulk Endpoints Expectations	34
	2.4 Interrupt Endpoint Expectations	34
	2.5 Isochronous Endpoints Expectations	34
3	Class Code	36
	3.1 Bluetooth Codes	36
4	Device Firmware Upgrade	38
5	Limitations	39
	5.1 Power Specific Limitations	39
	5.2 Other Limitations	39
6	Bluetooth Composite Device Implementation	40
	6.1 Configurations	40
	6.2 Using USB Interface Association Descriptors for a Primary Controller Function	40
	6.3 Combined Primary Controller Function and Single AMP Controller Function	41
7	References	45



Part C

SECURE DIGITAL (SD)

TRANSPORT LAYER

1	Introduction	50
2	Goals	51
2.1	Hardware Goals	51
2.2	Software Goals	51
2.3	Configuration Goals	52
2.4	Configuration for Multiple Controllers	52
3	Physical Interface Documents	53
4	Communication	54
4.1	Overview	54
5	Appendix A - Acronyms and Abbreviations	55
6	Appendix B - Related Documents	56
7	Appendix C - Tests	57
7.1	Test Suite Structure	57

Part D

THREE-WIRE UART TRANSPORT LAYER

1	General	63
2	Overview	64
3	Slip Layer	65
3.1	Encoding a Packet	65
3.2	Decoding a Packet	65
4	Packet Header	67
4.1	Sequence Number	67
4.2	Acknowledge Number	68
4.3	Data Integrity Check Present	68
4.4	Reliable Packet	68
4.5	Packet Type	68
4.6	Payload Length	69
4.7	Packet Header Checksum	69
5	Data Integrity Check	70
5.1	16 Bit CCITT-CRC	70



6	Reliable Packets	71
6.1	Header Checksum Error	71
6.2	Slip Payload Length Error	71
6.3	Data Integrity Check Error	71
6.4	Out Of Sequence Packet Error	71
6.5	Acknowledgement	72
6.6	Resending Packets	72
6.7	Example Reliable Packet Flow	72
7	Unreliable Packets	75
7.1	Unreliable Packet Header	75
7.2	Unreliable Packet Error	75
8	Link Establishment	76
8.1	Uninitialized State	77
8.2	Initialized State	77
8.3	Active State	77
8.4	Sync Message	78
8.5	Sync Response Message	78
8.6	Config Message	78
8.7	Config Response Message	79
8.8	Configuration Field	79
9	Low Power	82
9.1	Wakeup Message	82
9.2	Woken Message	82
9.3	Sleep Message	83
10	Out of Frame Control	84
10.1	Software Flow Control	84
11	Hardware Configuration	85
11.1	Wires	85
11.2	Hardware Flow	85
12	Recommended Parameters	86
12.1	Timing Parameters	86
13	References	87



Specification Volume 5
Core System Package
[AMP Controller volume]

Part A

802.11 PROTOCOL ADAPTATION LAYER FUNCTIONAL SPECIFICATION

1	Introduction	13
1.1	Organization of the 802.11 PAL	13
2	AMP Host Controller Interface	15
2.1	Read Local Version Information Command	15
2.2	Read Local Amp Info Command	15
2.3	Reset Command	18
2.4	Read Failed Contact Counter Command	18
2.5	Read Link Quality Command	18
2.6	Read RSSI Command	18
2.7	Short Range Mode Command	19
2.8	Write Best Effort Flush Timeout Command	19
2.9	Read Best Effort Flush Timeout Command	20
2.10	Physical Link Loss Early Warning Event	20
2.11	Physical Link Recovery Event	20
2.12	Channel Selected Event	20
2.13	Short Range Mode Change Complete Event	20
2.14	Data Structures	21
2.15	Connection Accept Timeout Configuration Parameter	27
2.16	Enable Device Under Test Mode	27
3	Physical Link Manager	28
3.1	Physical Link State Machine	28
3.2	Channel Selection	37
3.3	802.11 Link Creation	44
3.4	Physical Link Maintenance	46
3.5	Physical Link Security	47
3.6	Physical Link Support for QOS	49
4	Logical Link Manager	50
4.1	Logical Link Creation	50
4.2	Logical Link Updates	52
4.3	Logical Link Deletion	52



5	Data Manager	53
5.1	Encapsulation.....	53
5.2	Coexistence and Local Interference.....	54
5.3	Explicit Flush	57
5.4	Automatic Flush	57
5.5	Quality Of Service Violations.....	57
6	Constants	58
7	Message Sequence Charts	59
8	Appendix A: Test Support	60
8.1	AMP Test Command	60
8.2	AMP Start Test Event	64
8.3	AMP Test End Event	65
9	References	66


Specification Volume 6
Core System Package [Low Energy Controller volume]
Part A
PHYSICAL LAYER SPECIFICATION

1	Scope	14
2	Frequency Bands and Channel Arrangement	16
3	Transmitter Characteristics	17
3.1	Modulation Characteristics	17
3.2	Spurious Emissions	18
3.3	Radio Frequency Tolerance	19
4	Receiver Characteristics	20
4.1	Actual Sensitivity Level	20
4.2	Interference Performance	21
4.3	Out-of-Band Blocking	22
4.4	Intermodulation Characteristics	22
4.5	Maximum Usable Level	23
4.6	Reference Signal Definition	23
5	Appendix A	24
5.1	Normal Operating Conditions (NOC)	24
5.2	Extreme Operating Conditions (EOC)	24
6	Appendix B - Operating Conditions	25

Part B
LINK LAYER SPECIFICATION

1	General Description	32
1.1	Link Layer States	32
1.2	Bit Ordering	34
1.3	Device Address	34
1.4	Physical Channel	35
2	Air Interface Packets	37
2.1	Packet Format	37
2.2	Reserved for Future Use (RFU)	38
2.3	Advertising Channel PDU	38
2.4	Data Channel PDU	45
3	Bit Stream Processing	56
3.1	Error Checking	56
3.2	Data Whitening	57



4	Air Interface Protocol.....	58
4.1	Inter Frame Space	58
4.2	Timing Requirements	58
4.3	Link Layer Device Filtering.....	58
4.4	Non-Connected States	60
4.5	Connection State.....	71
4.6	Feature Support	81
5	Link Layer Control	83
5.1	Link Layer Control Procedures.....	83
5.2	Procedure Response Timeout	102
5.3	Procedure Collisions	103
5.4	LE Authenticated Payload Timeout.....	103

Part C

SAMPLE DATA

1	Encryption sample data.....	107
1.1	Encrypt Command	109
1.2	Derivation of the MIC and Encrypted Data.....	109

Part D

MESSAGE SEQUENCE CHARTS

1	Introduction	116
1.1	Notation.....	116
1.2	Control Flow	117
1.3	Example MSC	117
2	Standby State.....	118
2.1	Initial Setup	118
2.2	Random Device Address	119
2.3	White Lists.....	119
3	Advertising State.....	120
3.1	Undirected Advertising	120
3.2	Directed Advertising	121
4	Scanning State	123
4.1	Passive Scanning	123
4.2	Active Scanning	124
5	Initiating State.....	125
5.1	Initiating a Connection	125
5.2	Canceling an Initiation.....	126



6	Connection State.....	127
6.1	Sending Data	127
6.2	Connection Update	128
6.3	Channel Map Update.....	128
6.4	Features Exchange.....	129
6.5	Version Exchange.....	130
6.6	Start Encryption	131
6.7	Start Encryption without Long Term Key	132
6.8	Start Encryption with Event Masked	133
6.9	Start Encryption Without Slave Supporting Encryption	134
6.10	Restart Encryption	135
6.11	Disconnect	136
6.12	Connection Parameters Request.....	137
6.13	LE Ping	141

Part E

LOW ENERGY LINK LAYER SECURITY

1	Encryption and Authentication Overview.....	147
2	CCM.....	148
2.1	CCM Nonce	148
2.2	Counter Mode Blocks	149
2.3	Encryption Blocks	150

Part F

DIRECT TEST MODE

1	Introduction	154
2	Low Energy Test Scenarios	155
2.1	Test Sequences	155
2.2	Message Sequence Charts.....	156
3	UART Test Interface	157
3.1	UART Interface Characteristics	157
3.2	UART Functional Description.....	157
3.3	Commands and Events.....	158
3.4	Events	159
3.5	Timing – Command and Event	161
4	LE Test Packet Definition	162
4.1	LE test packets format	162



Specification Volume 7
Core System Package [Wireless Coexistence volume]

Part A

MWS COEXISTENCE LOGICAL SIGNALING SPECIFICATION

1	Introduction	10
2	Logical Interface.....	11
2.1	Coexistence Signals.....	11
2.2	Tolerances for Offsets and Jitter	14

Part B

WIRELESS COEXISTENCE INTERFACE 1 (WCI-1) TRANSPORT SPECIFICATION

1	Introduction	20
2	Physical Layer	21
2.1	Physical Signal Specifications (Informative)	22
3	Transport Layer	24
3.1	Message Types	24

Part C

WIRELESS COEXISTENCE INTERFACE 2 (WCI-2) TRANSPORT SPECIFICATION

1	Introduction	32
2	Physical Layer	33
3	Transport Layer	34
3.1	Message Types	34



8 LINK CONTROLLER OPERATION

This section describes how a piconet is established and how devices can be added to and released from the piconet. Several states of operation of the devices are defined to support these functions. In addition, the operation of several piconets with one or more common members, the scatternet, is discussed.

8.1 OVERVIEW OF STATES

Figure 8.1 on page 159 shows a state diagram illustrating the different states used in the link controller. There are three major states: **STANDBY**, **CONNECTION**, and **PARK**; in addition, there are nine substates, **page**, **page scan**, **inquiry**, **inquiry scan**, **synchronization train**, **synchronization scan**, **master response**, **slave response**, and **inquiry response**. Note that the **master response**, **slave response**, and **inquiry response** substates are not shown in the simplified figure below. The substates are interim states that are used to establish connections and enable device discovery. To move from one state or substate to another, either commands from the link manager are used, or internal signals in the link controller are used (such as the trigger signal from the correlator and the timeout signals).

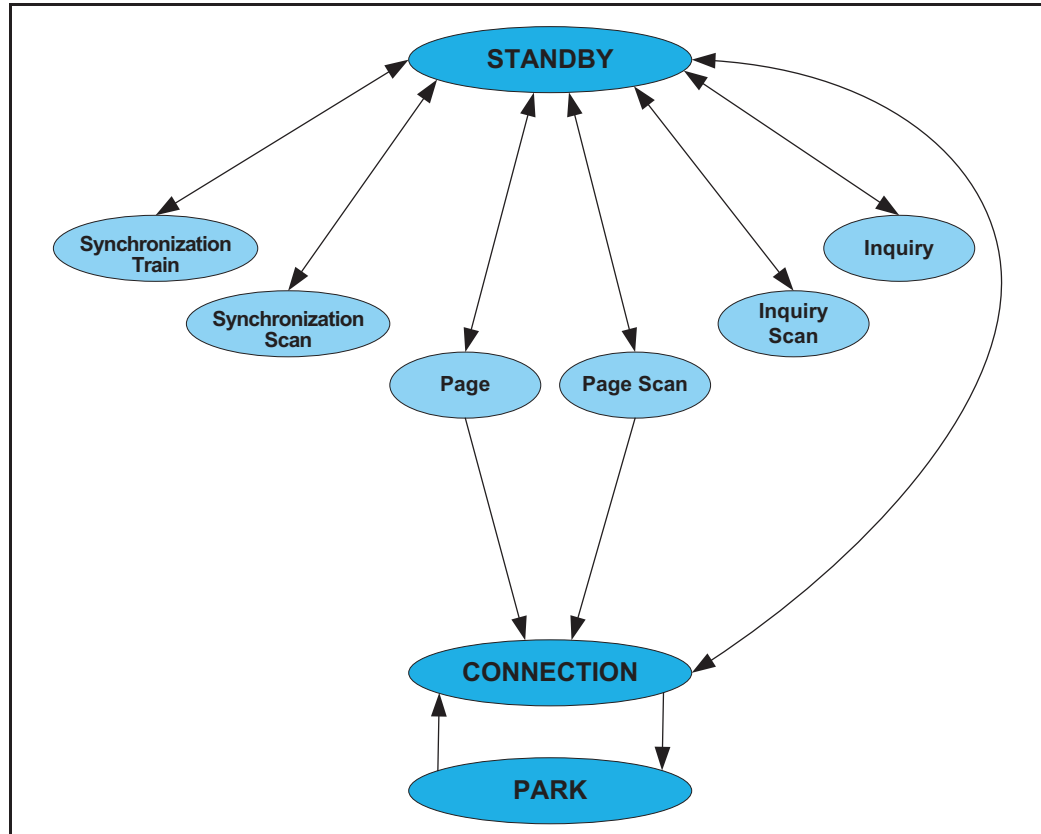


Figure 8.1: State diagram of link controller

8.2 STANDBY STATE

The **STANDBY** state is the default state in the device. In this state, the device may be in a low-power mode. Only the native clock is running at the accuracy of the LPO (or better).

The controller may leave the **STANDBY** state to scan for page or inquiry messages, or to page or inquiry itself.

8.3 CONNECTION ESTABLISHMENT SUBSTATES

In order to establish new connections the paging procedure or the synchronization scan procedure is used. Only the Bluetooth device address is required to set up a connection using the paging procedure. Knowledge about the clock, obtained from the inquiry procedure (see [Section 8.4 on page 169](#)) or from a previous connection with this device, and the page scanning mode of the other device will accelerate the paging procedure. A device that establishes a connection using a page procedure will automatically become the master of the connection. A device that establishes a connection using a synchronization scan procedure does so in two steps. First, from within the **synchronization scan** substate, the BR/EDR Controller follows the synchronization scan procedure to collect clock, packet timing, and AFH channel map information from the master and then transitions to the **STANDBY** state. Second, as commanded by the Host, the BR/EDR Controller transitions from the **STANDBY** state to the connectionless slave broadcast mode of the **CONNECTION** state.

The truncated page procedure is a modification of the paging procedure and is used to deliberately generate a page response timeout on the slave device.

8.3.1 Page Scan Substate

In the **page scan** substate, a device may be configured to use either the standard or generalized interlaced scanning procedure. During a standard scan, a device listens for the duration of the scan window $T_{w_page_scan}$ (11.25ms default, see HCI [\[Part E\] Section 7.3.20 on page 681](#)), while the generalized interlaced scan is performed as two back to back scans of $T_{w_page_scan}$. If the scan interval is not at least twice the scan window, then generalized interlaced scan shall not be used. During each scan window, the device shall listen at a single hop frequency, its correlator matched to its device access code (DAC). The scan window shall be long enough to completely scan 16 page frequencies.

When a device enters the **page scan** substate, it shall select the scan frequency according to the page hopping sequence determined by the device's Bluetooth device address, see [Section 2.6.4.1 on page 95](#). The phase in the sequence shall be determined by $CLKN_{16-12}$ of the device's native clock; that is, every 1.28s a different frequency is selected.



In the case of a standard scan, if the correlator exceeds the trigger threshold during the **page scan**, the device shall enter the **slave response** substate described in [Section 8.3.3.1 on page 167](#). The scanning device may also use generalized interlaced scan. In this case, if the correlator does not exceed the trigger threshold during the first scan it shall scan a second time using the phase in the sequence determined by $[\text{CLKN}_{16-12} + \text{interlace_offset}] \bmod 32$. If on this second scan the correlator exceeds the trigger threshold the device shall enter the **slave response** substate using $[\text{CLKN}_{16-12} + \text{interlace_offset}] \bmod 32$ as the frozen CLK_N* in the calculation for X_{prs}⁽⁷⁹⁾ (see [Section 2.6.4.3 on page 96](#) for details). If the correlator does not exceed the trigger threshold during a scan in normal mode or during the second scan in interlaced scan mode it shall return to either the **STANDBY** or **CONNECTION** state.

The *interlace_offset* value ranges from 0 to 31. The value 16 should be used unless the pattern of slots that are not available for scanning implies a different value should be used.

The **page scan** substate can be entered from the **STANDBY** state or the **CONNECTION** state. In the **STANDBY** state, no connection has been established and the device can use all the capacity to carry out the **page scan**. Before entering the **page scan** substate from the **CONNECTION** state, the device should reserve as much capacity as possible for scanning. If desired, the device may place ACL connections in Hold, Park, or Sniff (see [Section 8.8 on page 197](#) and [Section 8.9 on page 197](#)). Synchronous connections should not be interrupted by the page scan, although eSCO retransmissions should be paused during the scan. The page scan may be interrupted by the reserved synchronous slots which should have higher priority than the **page scan**. SCO packets should be used requiring the least amount of capacity (**HV3** packets). The scan window shall be increased to minimize the setup delay. If one SCO logical transport is present using **HV3** packets and $T_{\text{SCO}}=6$ slots or one eSCO logical transport is present using **EV3** packets and $T_{\text{ESCO}}=6$ slots, a total scan window $T_{\text{w page scan}}$ of at least 36 slots (22.5ms) is recommended; if two SCO links are present using **HV3** packets and $T_{\text{SCO}}=6$ slots or two eSCO links are present using **EV3** packets and $T_{\text{ESCO}}=6$ slots, a total scan window of at least 54 slots (33.75ms) is recommended.

The scan interval $T_{\text{page scan}}$ is defined as the interval between the beginnings of two consecutive page scans. A distinction is made between the case where the scan interval is equal to the scan window $T_{\text{w page scan}}$ (continuous scan), the scan interval is maximal 1.28s, or the scan interval is maximal 2.56s. These three cases shall determine the behavior of the paging device; that is, whether the paging device shall use R0, R1 or R2, see also [Section 8.3.2 on page 162](#). [Table 8.1](#) illustrates the relationship between $T_{\text{page scan}}$ and modes R0, R1 and R2. Although scanning in the R0 mode is continuous, the scanning may be interrupted for example by reserved synchronous slots. The scan interval information is included in the SR field in the FHS packet.

SR mode	$T_{\text{page scan}}$
R0	$\leq 1.28\text{s}$ and $= T_{\text{w page scan}}$
R1	$\leq 1.28\text{s}$
R2	$\leq 2.56\text{s}$
Reserved	-

Table 8.1: Relationship between scan interval, and paging modes R0, R1, and R2

8.3.2 Page substate

The **page** substate is used by the master (source) to activate and connect to a slave (destination) in the **page scan** substate. The master tries to coincide with the slave's scan activity by repeatedly transmitting the paging message consisting of the slave's device access code (DAC) in different hop channels. Since the Bluetooth clocks of the master and the slave are not synchronized, the master does not know exactly when the slave wakes up and on which hop frequency. Therefore, it transmits a train of identical page scan messages at different hop frequencies and listens in between the transmit intervals until it receives a response from the slave.

The page procedure in the master consists of a number of steps. First, the Host communicates the BD_ADDR of the slave to the Controller. This BD_ADDR shall be used by the master to determine the page hopping sequence; see [Section 2.6.4.2 on page 96](#). For the phase in the sequence, the master shall use an estimate of the slave's clock. For example, this estimate can be derived from timing information that was exchanged during the last encounter with this particular device (which could have acted as a master at that time), or from an inquiry procedure. With this estimate CLKE of the slave's Bluetooth clock, the master can predict on which hop channel the slave starts page scanning.

The estimate of the Bluetooth clock in the slave can be completely wrong. Although the master and the slave use the same hopping sequence, they use different phases in the sequence and might never select the same frequency. To compensate for the clock drifts, the master shall send its page message during a short time interval on a number of wake-up frequencies. It shall transmit also on hop frequencies just before and after the current, predicted hop frequency. During each TX slot, the master shall sequentially transmit on two different hop frequencies. In the following RX slot, the receiver shall listen sequentially to two corresponding RX hops for an ID packet. The RX hops shall be selected according to the page response hopping sequence. The page response hopping sequence is strictly related to the page hopping sequence: for each page hop there is a corresponding page response hop. The RX/TX timing in the **page** substate is described in [Section 2.2.5](#), see also [Figure 2.7 on page 81](#). In the next TX slot, the master shall transmit on two hop frequen-



cies different from the former ones. Note: The hop rate is increased to 3200 hops/s.

With the increased hopping rate as described above, the transmitter can cover 16 different hop frequencies in 16 slots or 10 ms. The page hopping sequence is divided over two paging trains **A** and **B** of 16 frequencies. Train **A** includes the 16 hop frequencies surrounding the current, predicted hop frequency $f(k)$, where k is determined by the clock estimate $CLKE_{16-12}$. The first train consists of hops

$f(k-8), f(k-7), \dots, f(k), \dots, f(k+7)$

When the difference between the Bluetooth clocks of the master and the slave is between -8×1.28 s and $+7 \times 1.28$ s, one of the frequencies used by the master will be the hop frequency the slave will listen to. Since the master does not know when the slave will enter the **page scan** substate, the master has to repeat this train **A** N_{page} times or until a response is obtained, whichever is shorter. If the slave scan interval corresponds to R1, the repetition number is at least 128; if the slave scan interval corresponds to R2 or if the master has not previously read the slave's SR mode, the repetition number is at least 256. If the master has not previously read the slave's SR mode it shall use $N_{\text{page}} \geq 256$. Note that $CLKE_{16-12}$ changes every 1.28 s; therefore, every 1.28 s, the trains will include different frequencies of the page hopping set.

When the difference between the Bluetooth clocks of the master and the slave is less than -8×1.28 s or larger than $+7 \times 1.28$ s, the remaining 16 hops are used to form the new 10 ms train **B**. The second train consists of hops

$f(k-16), f(k-15), \dots, f(k-9), f(k+8), \dots, f(k+15)$

Train **B** shall be repeated for N_{page} times. If no response is obtained, k_{nudge} may be updated in the case where slots to receive are periodically not available and train **A** shall be tried again N_{page} times. Alternate use of train **A** and train **B** and updates of k_{nudge} shall be continued until a response is received or the timeout *pageTO* is exceeded. When *extended_pageTO* is greater than zero, the timeout may be extended to $(\text{pageTO} + \text{extended_page_TO})$. If a response is returned by the slave, the master device enters the **master response** substate.

The **page** substate may be entered from the **STANDBY** state or the **CONNECTION** state. In the **STANDBY** state, no connection has been established and the device can use all the capacity to carry out the page. Before entering the **page** substate from the **CONNECTION** state, the device should free as much capacity as possible for paging. To ensure this, it is recommended that the ACL connections are put on hold or park. However, the synchronous connections shall not be disturbed by the page. This means that the page will be interrupted by the reserved SCO and eSCO slots which have higher priority than the page. In order to obtain as much capacity for paging, it is recommended to use the SCO packets which use the least amount of capacity (**HV3** packets). If SCO or

eSCO links are present, the repetition number N_{page} of a single train shall be increased, see [Table 8.2](#). Here it has been assumed that the **HV3** packet are used with an interval $T_{\text{SCO}}=6$ slots or **EV3** packets are used with an interval of $T_{\text{ESCO}}=6$ slots, which would correspond to a 64 kb/s synchronous link.

SR mode	no synchronous link	one synchronous link (HV3)	two synchronous links (HV3)
R0	$N_{\text{page}} \geq 1$	$N_{\text{page}} \geq 2$	$N_{\text{page}} \geq 3$
R1	$N_{\text{page}} \geq 128$	$N_{\text{page}} \geq 256$	$N_{\text{page}} \geq 384$
R2	$N_{\text{page}} \geq 256$	$N_{\text{page}} \geq 512$	$N_{\text{page}} \geq 768$

Table 8.2: Relationship between train repetition, and paging modes R0, R1 and R2 when synchronous links are present

The construction of the page train shall be independent of the presence of synchronous links; that is, synchronous packets are sent on the reserved slots but shall not affect the hop frequencies used in the unreserved slots, see [Figure 8.2 on page 164](#).

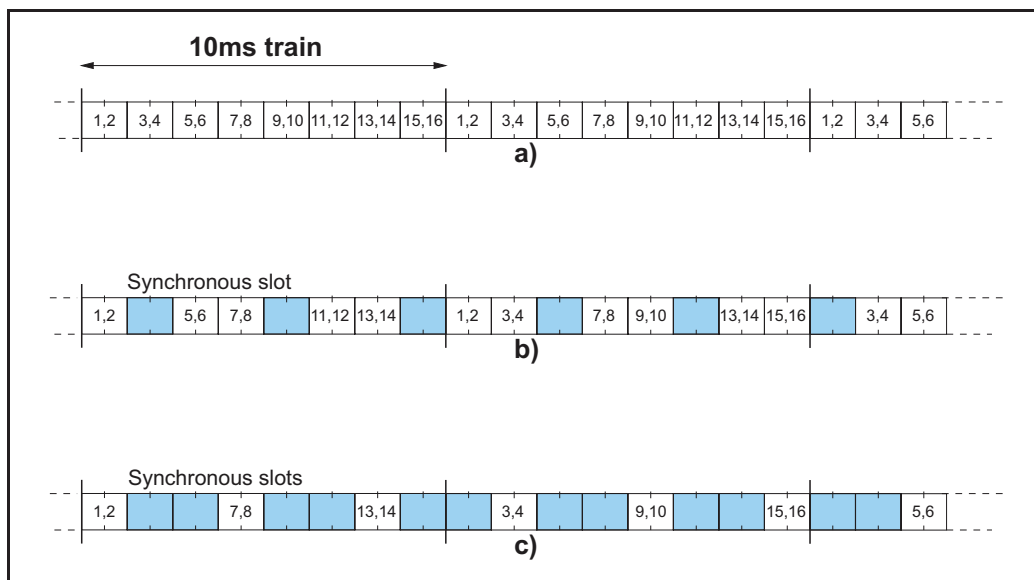


Figure 8.2: Conventional page (a), page while one synchronous link present (b), page while two synchronous links present (c)

8.3.3 Page Response Substates

When a page message is successfully received by the slave, there is a coarse FH synchronization between the master and the slave. Both the master and the slave enter a response substate to exchange vital information to continue the connection setup. It is important for the piconet connection that both devices shall use the same channel access code, use the same channel hopping sequence, and their clocks are synchronized. These parameters shall be derived from the master device. The device that initializes the connection (starts paging) is defined as the master device (which is thus only valid during the time the piconet exists). The channel access code and channel hopping sequence shall be derived from the Bluetooth device address (BD_ADDR) of the master. The timing shall be determined by the master clock. An offset shall be added to the slave's native clock to temporarily synchronize the slave clock to the master clock. At start-up, the master parameters are transmitted from the master to the slave. The messaging between the master and the slave at start-up is specified in this section.

The initial messaging between master and slave is shown in [Table 8.3 on page 165](#) and in [Figure 8.3 on page 166](#) and [Figure 8.4 on page 166](#). In those two figures frequencies $f(k)$, $f(k+1)$, etc. are the frequencies of the page hopping sequence determined by the slave's BD_ADDR. The frequencies $f'(k)$, $f'(k+1)$, etc. are the corresponding page_response frequencies (slave-to-master). The frequencies $g(m)$ belong to the basic channel hopping sequence.

Step	Message	Packet Type	Direction	Hopping Sequence	Access Code and Clock
1	Page	ID	Master to slave	Page	Slave
2	First slave page response	ID	Slave to master	Page response	Slave
3	Master page response	FHS	Master to slave	Page	Slave
4	Second slave page response	ID	Slave to master	Page response	Slave
5	1st packet master	POLL	Master to slave	Channel	Master
6	1st packet slave	Any type	Slave to master	Channel	Master

Table 8.3: Initial messaging during start-up

In step 1 (see [Table 8.3 on page 165](#)), the master device is in **page** substate and the slave device in the **page scan** substate. Assume in this step that the page message sent by the master reaches the slave. On receiving the page message, the slave enters the **slave response** in step 2. The master waits for a reply from the slave and when this arrives in step 2, it shall enter the **master response** in step 3. Note that during the initial message exchange, all param-

ters are derived from the slave's device address, and that only the page hopping and page response hopping sequences are used (are also derived from the slave's device address). Note that when the master and slave enter the response states, their clock input to the page and page response hop selection is frozen as is described in [Section 2.6.4.3 on page 96](#).

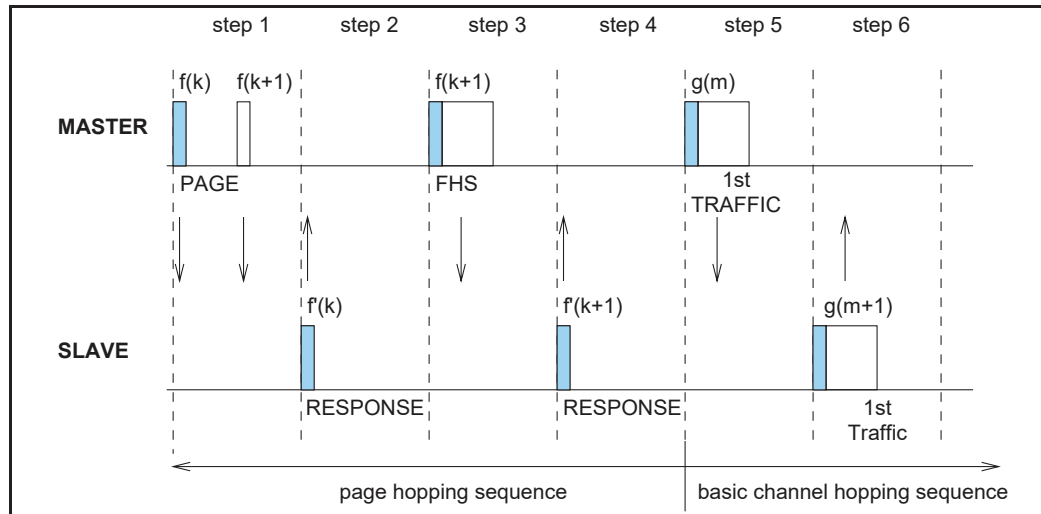


Figure 8.3: Messaging at initial connection when slave responds to first page message

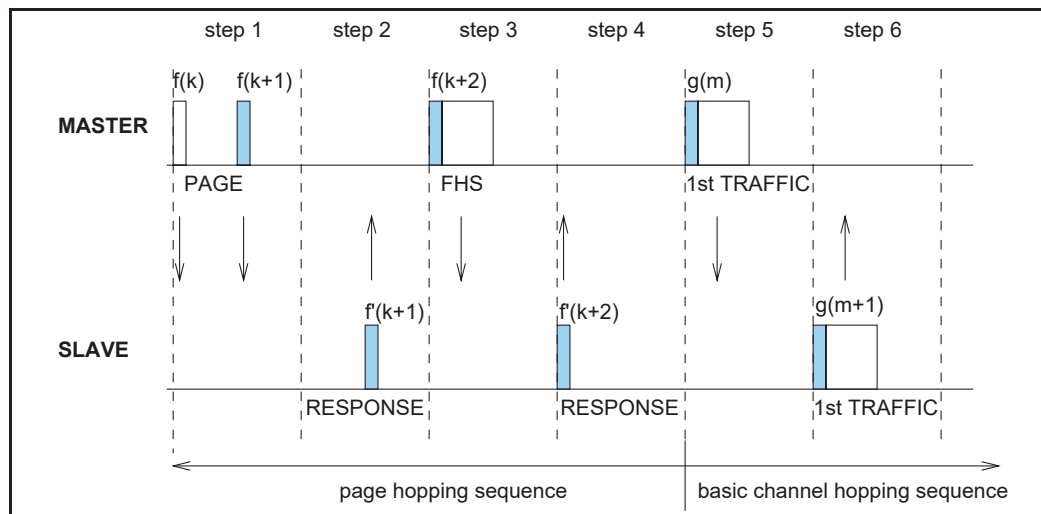


Figure 8.4: Messaging at initial connection when slave responds to second page message

In the case of the truncated page procedure, the messaging stops after step 2 in the sequence shown in [Table 8.3 on page 165](#). This procedure is illustrated in [Figure 8.5](#) and [Figure 8.6](#).

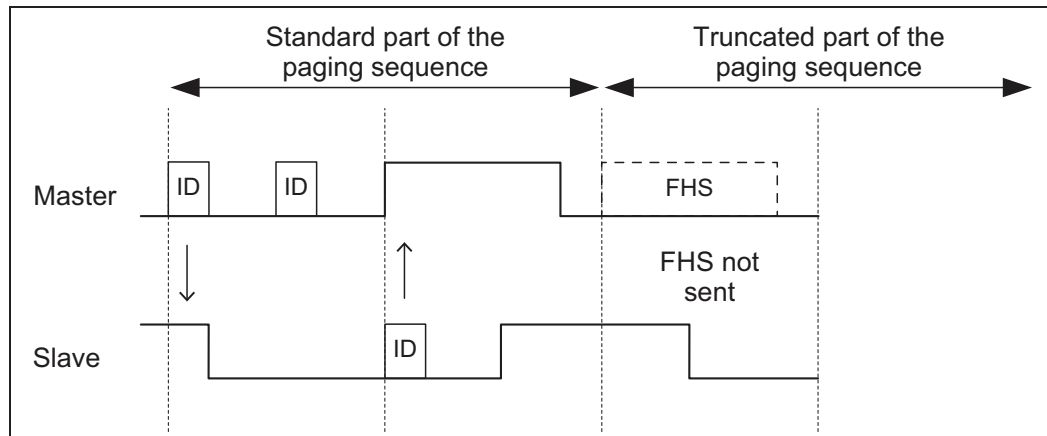


Figure 8.5: First half slot truncated page

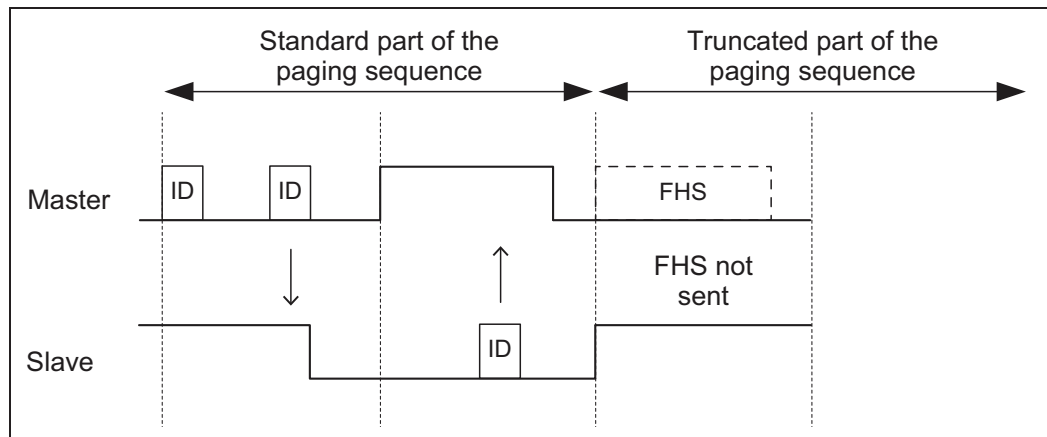


Figure 8.6: Second half slot truncated page

8.3.3.1 Slave response substate

After having received the page message in step 1, the slave device shall transmit a slave page response message (the slave's device access code) in step 2. This response message shall be the slave's device access code. The slave shall transmit this response 625 μ s after the beginning of the received page message and at the response hop frequency that corresponds to the hop frequency in which the page message was received. The slave transmission is therefore time aligned to the master transmission. During initial messaging, the slave shall still use the page response hopping sequence to return information to the master. The clock input $CLKN_{16-12}$ shall be frozen at the value it had at the time the page message was received.

After having sent the response message, the slave's receiver shall be activated 312.5 μ s after the start of the response message and shall await the arrival of an **FHS** packet. Note that an **FHS** packet can arrive 312.5 μ s after the arrival of the page message as shown in [Figure 8.4 on page 166](#), and not after 625 μ s as



is usually the case in the piconet physical channel RX/TX timing. More details about the timing can be found in [Section 2.4.4 on page 82](#).

If the setup fails before the **CONNECTION** state has been reached, the following procedure shall be carried out. The slave shall listen as long as no **FHS** packet is received until *pagerespTO* is exceeded. Every 1.25 ms, however, it shall select the next master-to-slave hop frequency according to the page hop sequence. If nothing is received after *pagerespTO*, the slave shall return back to the **page scan** substate for one scan period. Length of the scan period depends on the synchronous reserved slots present. If no page message is received during this additional scan period, the slave shall resume scanning at its regular scan interval and return to the state it was in prior to the first page scan state.

If an **FHS** packet is received by the slave in the **slave response** substate, the slave shall return a slave page response message in step 4 to acknowledge reception of the **FHS** packet. This response shall use the page response hopping sequence. The transmission of the slave page response packet is based on the reception of the **FHS** packet. Then the slave shall change to the master's channel access code and clock as received from the **FHS** packet. Only the 26 MSBs of the master clock are transferred: the timing shall be such that CLK_1 and CLK_0 are both zero at the time the **FHS** packet was received as the master transmits in even slots only. The offset between the master's clock and the slave's clock shall be determined from the master's clock in the **FHS** packet and reported to the slave's Baseband Resource Manager.

Finally, the slave enters the **CONNECTION** state in step 5. From then on, the slave shall use the master's clock and the master's *BD_ADDR* to determine the basic channel hopping sequence and the channel access code. The slave shall use the *LT_ADDR* in the **FHS** payload as the primary *LT_ADDR* in the **CONNECTION** state. The connection mode shall start with a POLL packet transmitted by the master. The slave may respond with any type of packet. If the POLL packet is not received by the slave, or the response packet is not received by the master, within *newconnectionTO* number of slots after FHS packet acknowledgement, the master and the slave shall return to **page** and **page scan** substates, respectively. See [Section 8.5 on page 174](#)

8.3.3.2 Master response substate

When the master has received a slave page response message in step 2, and the master is not executing the truncated page procedure, it shall enter the **master response** routine. It shall freeze the current clock input to the page hop selection scheme. The master shall then transmit an **FHS** packet in step 3 containing the master's real-time Bluetooth clock, the master's *BD_ADDR*, the BCH parity bits, and the class of device. The **FHS** packet contains all information to construct the channel access code without requiring a mathematical derivation from the master's Bluetooth device address. The *LT_ADDR* field in the packet header of FHS packets in the master response substate shall be set to all-zeros. The **FHS** packet



shall be transmitted at the beginning of the master-to-slave slot following the slot in which the slave responded. The FHS packet shall carry the all-zero LT_ADDR. The TX timing of the **FHS** is not based on the reception of the response packet from the slave. The **FHS** packet may therefore be sent 312.5 μ s after the reception of the response packet like shown in [Figure 8.4 on page 166](#) and not 625 μ s after the received packet as is usual in the piconet physical channel RX/TX timing, see also [Section 2.4.4 on page 82](#).

After the master has sent its **FHS** packet, it shall wait for a second slave page response message in step 4 acknowledging the reception of the **FHS** packet. This response shall be the slave's device access code. If no response is received, the master shall retransmit the **FHS** packet with an updated clock and still using the slave's parameters. It shall retransmit the FHS packet with the clock updated each time until a second slave page response message is received, or the timeout of *pagerespTO* is exceeded. In the latter case, the master shall return to the **page** substate and send an error message to the Baseband Resource Manager. During the retransmissions of the **FHS** packet, the master shall use the page hopping sequence.

If the slave's response is received, the master shall change to using the master parameters, so it shall use the channel access code and the master clock. The lower clock bits CLK₀ and CLK₁ shall be reset to zero at the start of the **FHS** packet transmission and are not included in the **FHS** packet. Finally, the master enters the **CONNECTION** state in step 5. The master BD_ADDR shall be used to change to a new hopping sequence, the *basic channel hopping sequence*. The basic channel hopping sequence uses all 79 hop channels in a pseudo-random fashion, see also [Section 2.6.4.7 on page 98](#). The master shall now send its first traffic packet in a hop determined with the new (master) parameters. This first packet shall be a POLL packet. See [Section 8.5 on page 174](#). This packet shall be sent within *newconnectionTO* number of slots after reception of the FHS packet acknowledgement. The slave may respond with any type of packet. If the POLL packet is not received by the slave or the POLL packet response is not received by the master within *newconnectionTO* number of slots, the master and the slave shall return to **page** and **page scan** substates, respectively.

8.4 DEVICE DISCOVERY SUBSTATES

In order to discover other devices a device shall enter **inquiry** substate. In this substate, it shall repeatedly transmit the inquiry message (ID packet, see [Section 6.5.1.1 on page 126](#)) at different hop frequencies. The **inquiry** hop sequence is derived from the LAP of the GIAC. Thus, even when DIACs are used, the applied hopping sequence is generated from the GIAC LAP. A device that allows itself to be discovered, shall regularly enter the **inquiry scan** substate to respond to inquiry messages. The following sections describe the message exchange and contention resolution during inquiry response. The inquiry response is optional: a device is not forced to respond to an inquiry message.



During the **inquiry** substate, the discovering device collects the Bluetooth device addresses and clocks of all devices that respond to the inquiry message. In addition, the discovering device also collects extended information (e.g. local name and supported services) from devices that respond with an extended inquiry response packet. It can then, if desired, make a connection to any one of the discovered devices by means of the previously described page procedure.

The inquiry message broadcast by the source does not contain any information about the source. However, it may indicate which class of devices should respond. There is one general inquiry access code (GIAC) to inquire for any device, and a number of dedicated inquiry access codes (DIAC) that only inquire for a certain type of device. The inquiry access codes are derived from reserved Bluetooth device addresses and are further described in [Section 6.3.1](#).

8.4.1 Inquiry scan substate

The **inquiry scan** substate is very similar to the **page scan** substate. However, instead of scanning for the device's device access code, the receiver shall scan for the inquiry access code long enough to completely scan for 16 inquiry frequencies. Two types of scans are defined: standard and generalized interlaced. In the case of a standard scan the length of this scan period is denoted $T_{w_inquiry_scan}$ (11.25ms default, see HCI [\[Part E\] Section 7.3.22 on page 684](#)). The standard scan is performed at a single hop frequency as defined by Xir_{4-0} (see [Section 2.6.4.6 on page 98](#)). The generalized interlaced scan is performed as two back to back scans of $T_{w_inquiry_scan}$ where the first scan is on the normal hop frequency and the second scan is defined by $[Xir_{4-0} + interlace_offset] \bmod 32$. If the scan interval is not at least twice the scan window then generalized interlaced scan shall not be used. The inquiry procedure uses 32 dedicated inquiry hop frequencies according to the inquiry hopping sequence. These frequencies are determined by the general inquiry address. The phase is determined by the native clock of the device carrying out the **inquiry scan**; the phase changes every 1.28s.

The $interlace_offset$ value ranges from 0 to 31. The value 16 should be used unless the pattern of slots that are not available for scanning implies a different value should be used.

Instead of, or in addition to, the general inquiry access code, the device may scan for one or more dedicated inquiry access codes. However, the scanning shall follow the inquiry scan hopping sequence determined by the general inquiry address. If an inquiry message is received during an inquiry wake-up period, the device shall enter the **inquiry response** substate.

The **inquiry scan** substate can be entered from the **STANDBY** state or the **CONNECTION** state. In the **STANDBY** state, no connection has been established and the device can use all the capacity to carry out the **inquiry scan**.



Before entering the **inquiry scan** substate from the **CONNECTION** state, the device should reserve as much capacity as possible for scanning. If desired, the device may place ACL logical transports in Sniff, Hold, or Park. Synchronous logical transports are preferably not interrupted by the **inquiry scan**, although eSCO retransmissions should be paused during the scan. In this case, the **inquiry scan** may be interrupted by the reserved synchronous slots. SCO packets should be used requiring the least amount of capacity (**HV3** packets). The scan window, $T_{w \text{ inquiry scan}}$, shall be increased to increase the probability to respond to an inquiry message. If one SCO logical transport is present using HV3 packets and $T_{SCO}=6$ slots or one eSCO logical transport is present using EV3 packets and $T_{ESCO}=6$ slots, a total scan window of at least 36 slots (22.5ms) is recommended; if two SCO links are present using HV3 packets and $T_{SCO}=6$ slots or two eSCO links are present using EV3 packets and $T_{ESCO}=6$ slots, a total scan window of at least 54 slots (33.75ms) is recommended.

The scan interval $T_{\text{inquiry scan}}$ is defined as the interval between two consecutive inquiry scans. The **inquiry scan** interval shall be less than or equal to 2.56 s.

8.4.2 Inquiry Substate

The **inquiry** substate is used to discover new devices. This substate is very similar to the **page** substate; the TX/RX timing shall be the same as in paging, see [Section 2.4.4 on page 82](#) and [Figure 2.7 on page 81](#). The TX and RX frequencies shall follow the inquiry hopping sequence and the inquiry response hopping sequence, and are determined by the general inquiry access code and the native clock of the discovering device. In between inquiry transmissions, the receiver shall scan for inquiry response messages. When a response is received, the entire packet (an FHS packet) shall be read. If the EIR bit in the FHS packet is set to one, the device should try to receive the extended inquiry response packet 1250μs after the start of the FHS packet. After this, the device shall continue with inquiry transmissions. The device in an **inquiry** substate shall not acknowledge the inquiry response messages. If enabled by the Host (see HCI [\[Part E\] Section 7.3.50 on page 721](#)), the RSSI value of the inquiry response message shall be measured. It shall keep probing at different hop channels and in between listening for response packets. As in the **page** substate, two 10 ms trains **A** and **B** are defined, splitting the 32 frequencies of the inquiry hopping sequence into two 16-hop parts. A single train shall be repeated for at least $N_{\text{inquiry}}=256$ times before a new train is used. In order to collect all responses in an error-free environment, at least three train switches must have taken place. As a result, the **inquiry** substate may have to last for 10.24 s unless the inquirer collects enough responses and aborts the **inquiry** substate earlier. If desired, the inquirer may also prolong the **inquiry** substate to increase the probability of receiving all responses in an error-prone environment. When some receive slots are periodically not available, it may require up to 31 train switches to collect all responses in an error-free environment, depending on the pattern of the available receive slots. Before each switch to



train **A**, k_{nudge} may be updated. As a result, the **inquiry** substate may have to last for 40.96s. If an inquiry procedure is automatically initiated periodically (say a 10 s period every minute), then the interval between two inquiry instances shall be determined randomly. This is done to avoid two devices synchronizing their inquiry procedures.

The **inquiry** substate is continued until stopped by the Baseband Resource Manager (when it decides that it has sufficient number of responses), when a timeout has been reached (*Inquiry_Length*), or by a command from the host to cancel the inquiry procedure. In case *Extended_Inquiry_Length* is different from zero, the timeout may be extended to (*Inquiry_Length* + *Extended_Inquiry_Length*).

The **inquiry** substate can be entered from the **STANDBY** state or the **CONNECTION** state. In the **STANDBY** state, no connection has been established and the device can use all the capacity to carry out the inquiry. Before entering the **inquiry** substate from the **CONNECTION** state, the device should free as much capacity as possible for inquiry. To ensure this, it is recommended that the ACL logical transports are placed in Sniff, Hold, or Park. However, the reserved slots of synchronous logical transports shall not be disturbed by the inquiry. This means that the inquiry will be interrupted by the reserved SCO and eSCO slots which have higher priority than the inquiry. In order to obtain as much capacity as possible for inquiry, it is recommended to use the SCO packets which use the least amount of capacity (**HV3** packets). If SCO or eSCO links are present, the repetition number N_{inquiry} shall be increased, see [Table 8.4 on page 172](#).

Here it has been assumed that **HV3** packets are used with an interval $T_{\text{SCO}}=6$ slots or **EV3** packets are used with an interval of $T_{\text{ESCO}}=6$ slots, which would correspond to a 64 kb/s synchronous link.

	No synchronous links	One synchronous link (HV3)	Two synchronous links (HV3)
N_{inquiry}	≥ 256	≥ 512	≥ 768

Table 8.4: Increase of train repetition when synchronous links are present

If an extended inquiry response packet could not be received because of higher priority traffic, the reception failed due to HEC or CRC failure, or because the packet type is not supported by the device, the inquiry response shall be reported to higher layers as an extended inquiry response with all-zero data.

8.4.3 Inquiry Response Substate

The slave response substate for inquiries differs completely from the slave response substate applied for pages. When the inquiry message is received in the inquiry scan substate, the recipient shall return an inquiry response (FHS) packet containing the recipient's device address (BD_ADDR) and other parameters. If the

recipient has non-zero extended inquiry response data to send it shall return an extended inquiry response packet after the FHS packet.

The following protocol in the slave's **inquiry response** shall be used. On the first inquiry message received in the inquiry scan substate the slave shall enter the inquiry response substate. If the slave has non-zero extended inquiry response data to send it shall return an FHS packet with the EIR bit set to one to the master 625 μ s after the inquiry message was received. It shall then return an extended inquiry response packet 1250 μ s after the start of the FHS packet. If the slave's extended inquiry response data is all zeroes the slave shall only return an FHS packet with the EIR bit set to zero. A contention problem could arise when several devices are in close proximity to the inquiring device and all respond to an inquiry message at the same time. However, because every device has a free running clock it is highly unlikely that they all use the same phase of the inquiry hopping sequence. In order to avoid repeated collisions between devices that wake up in the same inquiry hop channel simultaneously, a device shall back-off for a random period of time. Thus, if the device receives an inquiry message and returns an FHS packet, it shall generate a random number, RAND, between 0 and MAX_RANDOM. For scanning intervals ≥ 1.28 s MAX_RANDOM shall be 1023, however, for scanning intervals < 1.28 s MAX_RANDOM may be as small as 127. A profile that uses a special DIAC may choose to use a smaller MAX_RANDOM than 1023 even when the scanning interval is ≥ 1.28 s. The slave shall return to the **CONNECTION** or **STANDBY** state for the duration of at least RAND time slots. Before returning to the **CONNECTION** and **STANDBY** state, the device may go through the **page scan** substate. After at least RAND slots, the device shall add an offset of 1 to the phase in the inquiry hop sequence (the phase has a 1.28 s resolution) and return to the **inquiry scan** substate again. If the slave is triggered again, it shall repeat the procedure using a new RAND. The offset to the clock accumulates each time an **FHS** packet is returned. During a probing window, a slave may respond multiple times, but on different frequencies and at different times. Reserved synchronous slots should have priority over response packets; that is, if a response packet overlaps with a reserved synchronous slot, it shall not be sent but the next inquiry message is awaited. If a device has extended inquiry response data to send but the extended inquiry response packet overlaps with a reserved synchronous slot the FHS packet may be sent with the EIR bit set to zero.

The messaging during the inquiry routines is summarized in [Table 8.5 on page 174](#). In step 1, the master transmits an inquiry message using the inquiry access code and its own clock. The slave responds with the **FHS** packet containing the slave's Bluetooth device address, native clock and other slave information. This **FHS** packet is returned at times that tend to be random. The **FHS** packet is not acknowledged in the inquiry routine, but it is retransmitted at other times and frequencies as long as the master is probing with inquiry messages. If the slave has non-zero extended inquiry response data it sends an extended inquiry response packet to the master in step 3.



The extended inquiry response packet is an ACL packet with type DM1, DM3, DM5, DH1, DH3 or DH5. To minimize interference it is recommended to use the shortest packet that fits the data. The packet shall be sent on the same frequency as the FHS packet, 1250 μ s after the start of the FHS packet. In the packet header, LT_ADDR shall be set to zero. TYPE shall be one of DM1, DM3, DM5, DH1, DH3 or DH5. FLOW, ARQN and SEQN shall all be set to zero and ignored during receipt. The HEC LFSR shall be initialized with the same DCI (default check initialization) as for the FHS packet. In the payload header, LLID shall contain the value 10 (start of an L2CAP message or no fragmentation). FLOW shall be set to zero and ignored upon receipt. The length of the payload body (LENGTH) shall be smaller than or equal to 240 bytes. The CRC LFSR shall be initialized with the same DCI as for the FHS packet. The data whitening LFSR shall be initialized with the same value as for the FHS packet.

The payload data has two parts, a significant part followed by a non-significant part. The significant part contains a sequence of data structures as defined in [\[Vol. 3, Part C\] Section 8 on page 345](#). The non-significant part contains all-zero octets.

The baseband shall not change any octets in the significant part. When transmitting data, the non-significant part octets may be omitted from the payload.

A device shall store a single extended inquiry response packet. This packet shall be used with all IACs.

Step	Message	Packet Type	Direction	Hopping Sequence	Access Code and Clock
1	Inquiry	ID	master to slave	inquiry	inquiry
2	Inquiry response	FHS	slave to master	inquiry response	inquiry
3	Extended Inquiry Response	DM1, DM3, DM5, DH1, DH3, DH5	slave to master	inquiry response *	inquiry

Table 8.5: Messaging during inquiry routines

* The extended inquiry response packet is sent on the same frequency as the inquiry response (FHS) packet.

8.5 CONNECTION STATE

In the **CONNECTION** state, the connection has been established and packets can be sent back and forth, with the exception of connectionless slave broadcast mode, in which case packets are only sent from the master. In both devices, the channel (master) access code, the master's Bluetooth clock, and

the AFH_channel_map are used. **CONNECTION** state uses the *basic* or *adapted channel hopping sequence*.

There are two ways to enter the **CONNECTION** state. A device can transition from the page/page scan substates to the **CONNECTION** state or directly from the **STANDBY** state to the connectionless slave broadcast mode of the **CONNECTION** state.

If a device enters from the page/page scan substates, the **CONNECTION** state starts with a POLL packet sent by the master to verify the switch to the master's timing and channel frequency hopping. The slave may respond with any type of packet. If the slave does not receive the POLL packet or the master does not receive the response packet for *newconnectionTO* number of slots, both devices shall return to **page/page scan** substates.

The first information packets in the **CONNECTION** state contain control messages that characterize the link and give more details regarding the devices. These messages are exchanged between the link managers of the devices. For example, they may define the SCO logical transport and the sniff parameters. Then the transfer of user information can start by alternately transmitting and receiving packets.

The **CONNECTION** state is left through a **detach** or **reset** command. The **detach** command is used if the link has been disconnected in the normal way; all configuration data in the link controller shall remain valid. The **reset** command is a soft reset of the link controller. The functionality of the soft reset is described in [\[Part E\] Section 7.3.2 on page 653](#).

In the **CONNECTION** state, if a device is not going to be nominally present on the channel at all times it may describe its unavailability by using sniff mode or hold mode (see [Figure 8.7 on page 175](#)).

If a device enters the connectionless slave broadcast mode of the **CONNECTION** state, the master starts by sending packets on the CSB logical transport and the slave starts by receiving packets sent on the CSB logical transport.

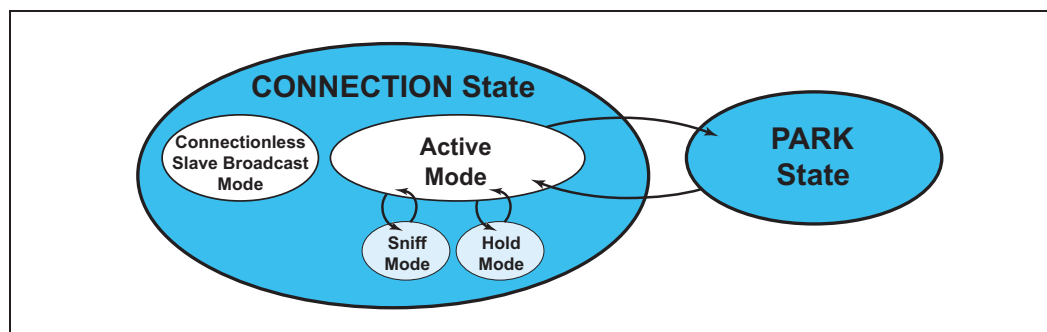


Figure 8.7: Connection state



9 AUDIO

On the air-interface, either a 64 kb/s log PCM (Pulse Code Modulation) format (A-law or μ -law) may be used, or a 64 kb/s CVSD (Continuous Variable Slope Delta Modulation) may be used. The latter format applies an adaptive delta modulation algorithm with syllabic companding.

The voice coding on the line interface is designed to have a quality equal to or better than the quality of 64 kb/s log PCM.

[Table 9.1 on page 210](#) summarizes the voice coding schemes supported on the air interface. The appropriate voice coding scheme is selected after negotiations between the Link Managers.

Voice Codecs	
linear	CVSD
8-bit logarithmic	A-law
	μ -law

Table 9.1: Voice coding schemes supported on the air interface

9.1 LOG PCM CODEC

Since the synchronous logical transports on the air-interface can support a 64 kb/s information stream, a 64 kb/s log PCM traffic can be used for transmission. Either A-law or μ -law compression may be applied. In the event that the line interface uses A-law and the air interface uses μ -law or vice versa, a conversion from A-law to μ -law shall be performed. The compression method shall follow ITU-T recommendations G. 711.

9.2 CVSD CODEC

A more robust format for voice over the air interface is delta modulation. This modulation scheme follows the waveform where the output bits indicate whether the prediction value is smaller or larger than the input waveform. To reduce slope overload effects, syllabic companding is applied: the step size is adapted according to the average signal slope. The input to the CVSD encoder shall be 64 ksamples/s linear PCM (typically 16 bits, but actual value is implementation specific). Block diagrams of the CVSD encoder and CVSD decoder are shown in [Figure 9.1 on page 211](#), [Figure 9.2 on page 211](#) and [Figure 9.3 on page 211](#). The system shall be clocked at 64 kHz.

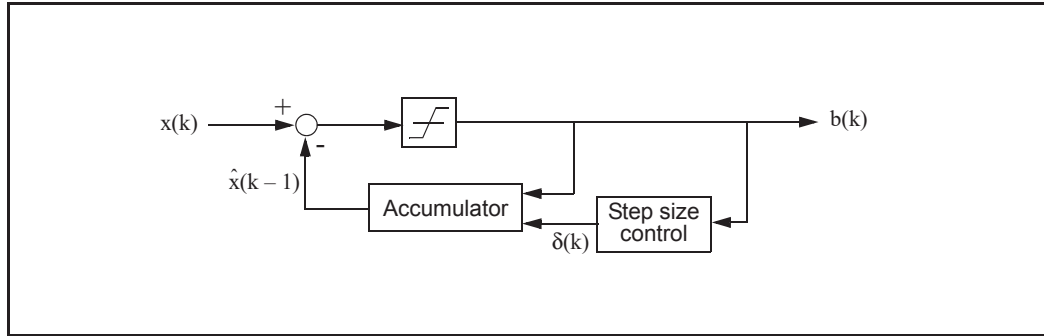


Figure 9.1: Block diagram of CVSD encoder with syllabic companding

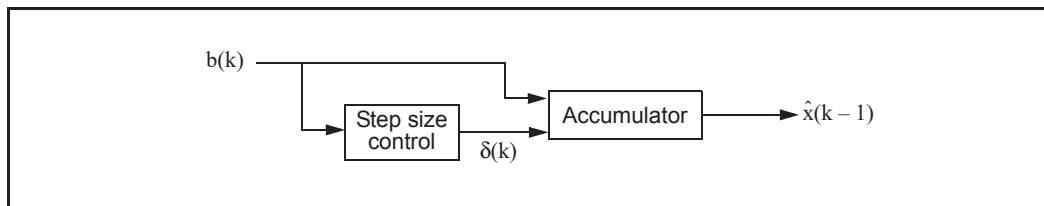


Figure 9.2: Block diagram of CVSD decoder with syllabic companding

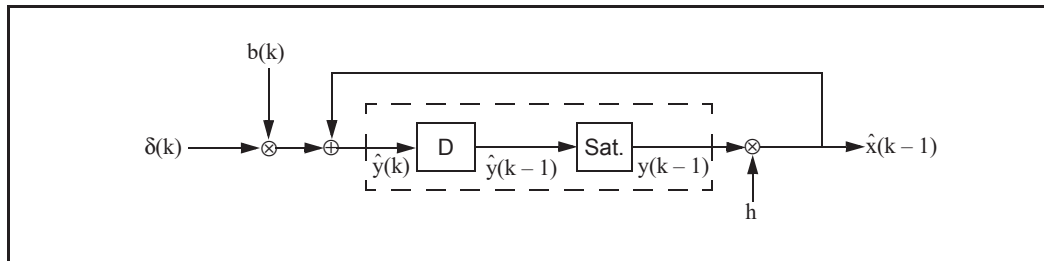


Figure 9.3: Accumulator procedure

Let $\text{sgn}(x) = 1$ for $x \geq 0$, otherwise $\text{sgn}(x) = -1$. On air these numbers shall be represented by the sign bit; i.e. negative numbers are mapped on “1” and positive numbers are mapped on “0”.

Denote the CVSD encoder output bit $b(k)$, the encoder input $x(k)$, the accumulator contents $y(k)$, and the step size $\delta(k)$. Furthermore, let h be the decay factor for the accumulator, let β denote the decay factor for the step size, and, let α be the syllabic companding parameter. The latter parameter monitors the slope by considering the K most recent output bits

Let

$$\hat{x}(k) = h y(k). \quad (\text{EQ } 14)$$

Then, the CVSD encoder internal state shall be updated according to the following set of equations:

$$b(k) = \text{sgn}\{x(k) - \hat{x}(k-1)\}, \quad (\text{EQ 15})$$

$$\alpha = \begin{cases} 1, & \text{if } J \text{ bits in the last } K \text{ output bits are equal,} \\ 0, & \text{otherwise,} \end{cases} \quad (\text{EQ 16})$$

$$\delta(k) = \begin{cases} \min\{\delta(k-1) + \delta_{\min}, \delta_{\max}\}, & \alpha = 1, \\ \max\{\beta\delta(k-1), \delta_{\min}\}, & \alpha = 0, \end{cases} \quad (\text{EQ 17})$$

$$y(k) = \begin{cases} \min\{\hat{y}(k), y_{\max}\}, & \hat{y}(k) \geq 0. \\ \max\{\hat{y}(k), y_{\min}\}, & \hat{y}(k) < 0. \end{cases} \quad (\text{EQ 18})$$

where

$$\hat{y}(k) = \hat{x}(k-1) + b(k)\delta(k). \quad (\text{EQ 19})$$

In these equations, $\delta_{\min}$ and $\delta_{\max}$ are the minimum and maximum step sizes, and, $y_{\min}$ and $y_{\max}$ are the accumulator's negative and positive saturation values, respectively. Over air, the bits shall be sent in the same order they are generated by the CVSD encoder.

For a 64 kb/s CVSD, the parameters as shown in [Table 9.2](#) shall be used. The numbers are based on a 16 bit signed number output from the accumulator. These values result in a time constant of 0.5 ms for the accumulator decay, and a time constant of 16 ms for the step size decay

Parameter	Value
h	$1 - \frac{1}{32}$
β	$1 - \frac{1}{1024}$
J	4
K	4
$\delta_{\min}$	10
$\delta_{\max}$	1280
$y_{\min}$	-2^{15} or $-2^{15} + 1$
$y_{\max}$	$2^{15} - 1$

Table 9.2: CVSD parameter values. The values are based on a 16 bit signed number output from the accumulator

9.3 ERROR HANDLING

In the DV, HV3, EV3, EV5, 2-EV3, 3-EV3, 2-EV5 and 3-EV5 packets, the voice is not protected by FEC. The quality of the voice in an error-prone environment then depends on the robustness of the voice coding scheme and, in the case of eSCO, the retransmission scheme. CVSD, in particular, is rather insensitive to random bit errors, which are experienced as white background noise. However, when a packet is rejected because either the channel access code, the HEC test was unsuccessful, or the CRC has failed, measures have to be taken to “fill” in the lost speech segment.

The voice payload in the **HV2** and **EV4** packets are protected by a 2/3 rate FEC. For errors that are detected but cannot be corrected, the receiver should try to minimize the audible effects. For instance, from the 15-bit FEC segment with uncorrected errors, the 10-bit information part as found before the FEC decoder should be used. The **HV1** packet is protected by a 3 bit repetition FEC. For this code, the decoding scheme will always assume zero or one-bit errors. Thus, there exist no detectable but uncorrectable error events for **HV1** packets.

9.4 GENERAL AUDIO REQUIREMENTS

9.4.1 Signal Levels

For A-law and μ -law log-PCM encoded signals the requirements on signal levels shall follow the ITU-T recommendation G.711.

Full swing at the 16 bit linear PCM interface to the CVSD encoder is defined to be 3 dBm0.

9.4.2 CVSD Audio Quality

For Bluetooth audio quality the requirements are put on the transmitter side. The 64 ksamples/s linear PCM input signal should have negligible spectral power density above 4 kHz. The power spectral density in the 4-32 kHz band of the decoded signal at the 64 ksamples/s linear PCM output, should be more than 20 dB below the maximum in the 0-4 kHz range.