Physical links (one per slave device) are represented in the diagram by lines connecting the devices. The solid lines represent an active physical link, and the dashed line represents a parked physical link. Device H is parked, and hence the physical link between the master (F) and the slave (H) is shown as parked.

Logical transports, logical links and L2CAP channels are used to provide capabilities for the transport of data, but are not shown on this diagram. They are described in more detail in Section 3.5 on page 41 and Section 3.6 on page 50.

4.2 OPERATIONAL PROCEDURES AND MODES

The typical operational mode of a Bluetooth device is to be connected to other Bluetooth devices (in a piconet) and exchanging data with that Bluetooth device. As Bluetooth is an ad-hoc wireless communications technology there are also a number of operational procedures that enable piconets to be formed so that the subsequent communications can take place. Procedures and modes are applied at different layers in the architecture and therefore a device may be engaged in a number of these procedures and modes concurrently.

4.2.1 Inquiry (Discovering) Procedure

Bluetooth devices use the inquiry procedure to discover nearby devices, or to be discovered by devices in their locality.

The inquiry procedure is asymmetrical. A Bluetooth device that tries to find other nearby devices is known as an inquiring device and actively sends inquiry requests. Bluetooth devices that are available to be found are known as discoverable devices and listen for these inquiry requests and send responses. The inquiry procedure uses a special physical channel for the inquiry requests and responses.

Both inquiring and discoverable devices may already be connected to other Bluetooth devices in a piconet. Any time spent inquiring or occupying the inquiry scan physical channel needs to be balanced with the demands of the QoS commitments on existing logical transports.

The inquiry procedure does not make use of any of the architectural layers above the physical channel, although a transient physical link may be considered to be present during the exchange of inquiry and inquiry response information.

4.2.2 Paging (Connecting) Procedure

The procedure for forming connections is asymmetrical and requires that one Bluetooth device carries out the page (connection) procedure while the other Bluetooth device is connectable (page scanning.) The procedure is targeted, so that the page procedure is only responded to by one specified Bluetooth device.

The connectable device uses a special physical channel to listen for connection request packets from the paging (connecting) device. This physical channel has attributes that are specific to the connectable device, hence only a paging device with knowledge of the connectable device is able to communicate on this channel.

Both paging and connectable devices may already be connected to other Bluetooth devices in a piconet. Any time spent paging or occupying the page scan physical channel needs to be balanced with the demands of the QoS commitments on existing logical transports.

4.2.3 Connected mode

After a successful connection procedure, the devices are physically connected to each other within a piconet. This means that there is a piconet physical channel to which they are both connected, there is a physical link between the devices, and there are default ACL-C and ACL-U logical links. When in the connected mode it is possible to create and release additional logical links, and to change the modes of the physical and logical links while remaining connected to the piconet physical channel. It is also possible for the device to carry out inquiry, paging or scanning procedures or to be connected to other piconets without needing to disconnect from the original piconet physical channel.

Additional logical links are created using the Link Manager that exchanges Link Manager Protocol messages with the remote Bluetooth device to negotiate the creation and settings for these links. Default ACL-C and ACL-U logical links are always created during the connection process, and these are used for LMP messages and the L2CAP signalling channel respectively.

It is noted that two default logical links are created when two units are initially connected. One of these links (ACL-C) transports the LMP control protocol and is invisible to the layers above the Link Manager. The other link (ACL-U) transports the L2CAP signalling protocol and any multiplexed L2CAP best-effort channels. It is common to refer to a default ACL logical transport, which can be resolved by context, but typically refers to the default ACL-U logical link. Also note that these two logical links share a logical transport.

During the time that a slave device is actively connected to a piconet there is always a default ACL logical transport between the slave and the master device. There are two methods of deleting the default ACL logical transport. The first method is to detach the device from the piconet physical channel, at

which time the entire hierarchy of L2CAP channels, logical links and logical transports between the devices is deleted.

The second method is to place the physical link to the slave device in the park state, at which time it gives up its default ACL logical transport. This is only allowed if all other logical transports have been deleted (except for the ASB logical transport that cannot be explicitly created or deleted.) It is not allowed to park a device while it has any logical transports other than the default ACL and ASB logical transports.

When the slave device physical link is parked, its default ACL logical transport is released and the ASB logical transport is replaced with a PSB logical transport. The ACL-C and ACL-U logical links that are multiplexed onto the default ACL logical transport remain in existence but cannot be used for the transport of data. The Link Manager on the master device restricts itself to the use of LMP messages that are allowed to be transported over the PSB-C logical link. The Channel Manager and L2CAP Resource Manager ensure that no L2CAP unicast data traffic is submitted to the controller while the device is parked. The Channel Manager may decide to manage the parking and unparking of the device as necessary to allow data to be transported.

4.2.4 Hold mode

Hold mode is not a general device mode, but applies to unreserved slots on the physical link. When in this mode, the physical link is only active during slots that are reserved for the operation of the synchronous link types SCO and eSCO. All asynchronous links are inactive. Hold modes operate once for each invocation and are then exited when complete, returning to the previous mode.

4.2.5 Sniff mode

Sniff mode is not a general device mode, but applies to the default ACL logical transports. When in this mode the availability of these logical transports is modified by defining a duty cycle consisting of periods of presence and absence. Devices that have their default ACL logical transports in sniff mode may use the absent periods to engage in activity on another physical channel, or to enter reduced power mode. Sniff mode only affects the default ACL logical transports (i.e. their shared ACL logical transport), and does not apply to any additional SCO or eSCO logical transports that may be active. The periods of presence and absence of the physical link on the piconet physical channel is derived as a union of all logical transports that are built on the physical link.

Note that broadcast logical transports have no defined expectations for presence or absence. A master device should aim to schedule broadcasts to coincide with periods of physical link presence within the piconet physical channel, but this may not always be possible or practical. Repetition of broadcasts is defined to improve the possibilities for reaching multiple slaves without overlapping presence periods. However, broadcast logical transports cannot be considered to be reliable.

4.2.6 Parked state

A slave device may remain connected to a piconet but have its physical link in the parked state. In this state the device cannot support any logical links to the master with the exception of the PSB-C and PSB-U logical links that are used for all communication between the piconet master and the parked slave.

When the physical link to a slave device is parked this means that there are restrictions on when the master and slave may communicate, defined by the PSB logical transport parameters. During times when the PSB logical transport is inactive (or absent) then the devices may engage in activity on other physical channels, or enter reduced power mode.

4.2.7 Role switch procedure

The role switch procedure is a method for swapping the roles of two devices connected in a piconet. The procedure involves moving from the physical channel that is defined by the original master device to the physical channel that is defined by the new master device. In the process of swapping from one physical channel to the next, the hierarchy of physical links and logical transports are removed and rebuilt, with the exception of the ASB and PSB logical transports that are implied by the topology and are not preserved. After the role switch, the original piconet physical channel may cease to exist or may be continued if the original master had other slaves that are still connected to the channel.

The procedure only copies the default ACL logical links and supporting layers to the new physical channel. Any additional logical transports are not copied by this procedure, and if required this must be carried out by higher layers. The LT_ADDRs of any affected transports may not be preserved as the values may already be in use on the new physical channel.

If there are any QoS commitments or modes such as sniff mode on the original logical transports, then these are not preserved after a role switch. These must be renegotiated after the role switch has completed.

4.2.8 Enhanced Data Rate

Enhanced Data Rate is a method of extending the capacity and types of Bluetooth packets for the purposes of increasing the maximum throughput, providing better support for multiple connections, and lowering power consumption, while the remainder of the architecture is unchanged.

Enhanced Data Rate may be selected as a mode that operates independently on each logical transport. Once enabled, the packet type bits in the packet header are interpreted differently from their meaning in Basic Rate mode. This different interpretation is clarified in conjunction with the logical transport address field in the header. The result of this interpretation allows the packet payload header and payload to be received and demodulated according to the packet type. Enhanced Data Rate can be enabled only for ACL-U, eSCO-S logical transports and cannot be enabled for ACL-C, SCO-S, and the broadcast logical transports.



Acronyms & Abbreviations

1 LIST OF ACRONYMS AND ABBREVIATIONS

Acronym or abbreviation	Writing out in full	Which means
8DPSK	8 phase Differential Phase Shift Keying	3 Mbps modulation type used by Enhanced Data rate
π/4 DQPSK	pi/4 Rotated Differential Quaternary Phase Shift Keying	2Mbps modulation type used by Enhanced Data Rate
A		
ACK	Acknowledge	
ACL	Asynchronous Connection-oriented [logical transport]	Reliable or time-bounded, bi-directional, point-to-point.
ACL-C	ACL Control [logical link] (LMP)	
ACL-U	ACL User [logical link] (L2CAP)	
ACO	Authenticated Ciphering Offset	
AFH	Adaptive Frequency Hopping	
AG	Audio Gateway	
AHS	Adapted Hop Sequence	
AR_ADDR	Access Request Address	
ARQ	Automatic Repeat reQuest	
ASB	Active Slave Broadcast [logical transport]	Unreliable, uni-directional broadcast to any devices synchronized with the physical channel.
ASB-U	ASB User [logical link] (L2CAP)	
B		
BB	BaseBand	
BCH	Bose, Chaudhuri & Hocquenghem	Type of code The persons who discovered these codes in 1959 (H) and 1960 (B&C)
BD_ADDR	Bluetooth Device Address	
BER	Bit Error Rate	
BT	Bandwidth Time	
BT	Bluetooth	
C		
CAC	Channel Access Code	

Table 1.1: Acronyms and Abbreviations.

Acronym or abbreviation	Writing out in full	Which means
CC	Call Control	
CL	Connectionless	
CODEC	COder DECoder	
COF	Ciphering Offset	
CRC	Cyclic Redundancy Check	
CVSD	Continuous Variable Slope Delta Modulation	
D		
DAC	Device Access Code	
DCE	Data Communication Equipment	
DCE	Data Circuit-Terminating Equip-ment	In serial communications, DCE refers to a device between the communication endpoints whose sole task is to facilitate the commu-nications process; typically a modem
DCI	Default Check Initialization	
DEVM	Differential Error Vector Magnitude	Measure of modulation error used for Enhanced Data Rate transmit-ter testing
DH	Data-High Rate	Data packet type for high rate data
DIAC	Dedicated Inquiry Access Code	
DM	Data - Medium Rate	Data packet type for medium rate data
DPSK	Differential Phase Shift Keying	Generic description of Enhanced Data Rate modulation
DQPSK	Differential Quarternary Phase Shift Keying	Modulation type used by Enhanced Data Rate
DTE	Data Terminal Equipment	In serial communications, DTE refers to a device at the endpoint of the communications path; typically a computer or terminal.
DTMF	Dual Tone Multiple Frequency	
DUT	Device Under Test	
DV	Data Voice	Data packet type for data and voice

Table 1.1: Acronyms and Abbreviations.

Acronym or abbreviation	Writing out in full	Which means
E		
EDR	Enhanced Data Rate	
EIRP	Effective Isotropic Radiated Power	Equivalent power that an isotropic antenna must transmit to provide the same field power density
eSCO	Extended Synchronous Connection Oriented [logical transport]	Bi-directional, symmetric or asymmetric, point-to-point, general regular data, limited retransmission.
eSCO-S	Stream eSCO (unframed)	used to support isochronous data delivered in a stream without framing
ETSI	European Telecommunications Standards Institute	
EUT	Equipment Under Test	
F		
FCC	Federal Communications Commission	
FEC	Forward Error Correction code	
FH	Frequency Hopping	
FHS	Frequency Hop Synchronization	
FIFO	First In First Out	
FM	Frequency Modulation	Modulation Type
FW	Firmware	
G		
GFSK	Gaussian Frequency Shift Keying	
GIAC	General Inquiry Access Code	
GM	Group Management	
H		
HCI	Host Controller Interface	
HEC	Header-Error-Check	
HID	Human Interface Device	
HV	High quality Voice	e.g. HV1 packet
HW	Hardware	

Table 1.1: Acronyms and Abbreviations.

Acronym or abbreviation	Writing out in full	Which means
I		
IAC	Inquiry Access Code	
IEEE	Institute of Electronic and Electrical Engineering	
IETF	Internet Engineering Task Force	
IP	Internet Protocol	
IrDA	Infra-red Data Association	
IrMC	Ir Mobile Communications	
ISDN	Integrated Services Digital Net-works	
ISM	Industrial, Scientific, Medical	
IUT	Implementation Under Test	
L		
L2CAP	Logical Link Control and Adaptation Protocol	
LAP	Lower Address Part	
LC	Link Controller	Link Controller (or baseband) part of the Bluetooth protocol stack. Low level Baseband protocol handler
LC	Link Control [logical link]	The control logical links LC and ACL-C are used at the link control level and link manager level, respectively.
LCP	Link Control Protocol	
LCSS	Link Controller Service Signalling	
LFSR	Linear Feedback Shift Register	
LLID	Logical Link Identifier	
LM	Link Manager	
LMP	Link Manager Protocol	For LM peer to peer communica-tion
LSB	Least Significant Bit	
LT_ADDR	Logical Transport ADDRess	
M		
M	Master or Mandatory	

Table 1.1: Acronyms and Abbreviations.

Acronym or abbreviation	Writing out in full	Which means
MAC	Medium Access Control	
MAPI	Messaging Application Procedure Interface	
Mbps	Million (Mega) bits per second	
MMI	Man Machine Interface	
MS	Mobile Station	
MS	Multiplexing sublayer	
MSB	Most Significant Bit	
MSC	Message Sequence Chart	
MTU	Maximum Transmission Unit	
N		
NAK	Negative Acknowledge	
NAP	Non-significant Address Part	
O		
O	Optional	
OBEX	OBject EXchange protocol	
OCF	OpCode Command Field	
OGF	OpCode Group Field	
P		
PCM	Pulse Coded Modulation	
PCMCIA	Personal Computer Memory Card International Association	
PDU	Protocol Data Unit	a message
PIN	Personal Identification Number	
PM_ADDR	Parked Member Address	
PN	Pseudo-random Noise	
PPM	Part Per Million	
PPP	Point-to-Point Protocol	
PRBS	Pseudo Random Bit Sequence	
PRNG	Pseudo Random Noise Generation	

Table 1.1: Acronyms and Abbreviations.

Acronym or abbreviation	Writing out in full	Which means
PSB	Parked Slave Broadcast [logical transport]	Unreliable, uni-directional broadcast to all piconet devices.
PSB-C	PSB Control [logical link] (LMP)	
PSB-U	PSB User [logical link] (L2CAP)	
PSK	Phase Shift Keying	Class of modulation types
PSTN	Public Switched Telephone Network	
ptt	Packet Type Table	The ptt parameter is used to select the logical transport types via LMP.
Q		
QoS	Quality of Service	
QPSK	Quarternary Phase Shift Keying	Modulation type used by Enhanced Data Rate
R		
RAND	Random number	
RF	Radio Frequency	
RFC	Request For Comments	
RFCMode	Retransmission and Flow Control Mode	
RFCOMM		Serial cable emulation protocol based on ETSI TS 07.10
RMS	Root Mean Square	
RSSI	Received Signal Strength Indication	
RX	Receive	
S		
S	Slave	
SAP	Service Access Points	
SAR	Segmentation and Reassembly	
SCO	Synchronous Connection-Oriented [logical transport]	Bi-directional, symmetric, point-to-point, AV channels.
SCO-S	Stream SCO (unframed)	
SCO-S	Synchronous logical link	used to support isochronous data delivered in a stream without framing

Table 1.1: Acronyms and Abbreviations.

Acronym or abbreviation	Writing out in full	Which means
SD	Service Discovery	
SDDB	Service Discovery Database	
SDP	Service Discovery Protocol	
SDU	Service Data Unit	
SEQN	Sequential Numbering scheme	
SRES	Signed Response	
SS	Supplementary Services	
SSI	Signal Strength Indication	
SUT	System Under Test	
SW	Software	
T		
TBD	To Be Defined	
TC	Test Control	Test Control layer for the test interface
TCI	Test Control Interface	
TCP/IP	Transport Control Protocol/Internet Protocol	
TCS	Telephony Control protocol Specification	
TDD	Time-Division Duplex	
TX	Transmit	
U		
UAP	Upper Address Part	
UART	Universal Asynchronous receiver Transmitter	
UI	User Interface	
UI	Unnumbered Information	
ULAP	Upper and Lower Address Parts	
USB	Universal Serial Bus	
UUID	Universal Unique Identifier	
W		
WAP	Wireless Application Protocol	
WUG	Wireless User Group	

Table 1.1: Acronyms and Abbreviations.

2 ABBREVIATIONS OF THE SPECIFICATION NAMES

Acronym or abbreviation	Writing out in full	Placement in Specification
A2DP	Advanced Audio Distribution Profile Specification	vol 10 part C
AVCTP	A/V Control Transport Protocol Specification	vol 10 part F
AVDTP	A/V Distribution Transport Profile Specification	vol 10 part A
AVRCP	A/V Remote Control Profile Specification	vol 10 part G
BB	Baseband Specification	vol 2 part B
BIP	Basic Imaging Profile	vol 8 part E
BNEP	Bluetooth Network Encapsulation Protocol Specification	vol 6 part A
BPP	Basic Printing Profile Specification	vol 8 part F
CIP	Common ISDN Access Profile Specification	vol 12 part A
CTP	Cordless Telephony Profile Specification	vol 9 part B
DUN	Dial-Up Networking Profile Specification	vol 7 part C
EDR	Enhanced Data Rate	vol 2 part A-C, H
ESDP / UPNP	Extended Service Discovery Profile	vol 6 part D
FAX	Fax Profile Specification	vol 7 part D
FTP	File Transfer Profile Specification	vol 8 part C
GAP	Generic Access Profile Specification	vol 3 part C
GAVDP	Generic A/V Distribution Profile Specification	vol 10 part B
GOEP	Generic Object Exchange Profile Specification	vol 8 part A
HCI (1)	Host Controller Interface Functional Specification	vol 2 part E
HCI (2)	Host Controller Interface Transport Layers Specification	vol 4 part A-C
HCRP	Hardcopy Cable Replacement Profile Specification	vol 11 part B
HFP	Hands-Free Profile Specification	vol 7 part E
HID	Human Interface Device Profile Specification	vol 11 part A
HSP	Headset Profile Specification	vol 7 part F
ICP	Intercom Profile Specification	vol 9 part C
L2CAP	Logical Link Control and Adaptation Protocol Specification	vol 3 part A

Table 2.1: Abbreviations of the specification names.

Acronym or abbreviation	Writing out in full	Placement in Specification
LAP	LAN Access Profile Specification	deprecated
LMP	Link Manager Protocol Specification	vol 2 part C
MSC	Message Sequence Charts	vol 2 part F
OPP	Object Push Profile Specification	vol 8 part B
PAN	Personal Area Networking Profile Specification	vol 6 part B
RF	Radio Specification	vol 2 part A
RFCOMM	RFCOMM with TS 07.10	vol 7 part A
SAP	SIM Access Profile Specification	vol 12 part C
SDAP	Service Discovery Application Profile Specification	vol 5 part B
SDP (1)	Service Discovery Protocol Specification (server)	vol 3 part B
SDP (2)	Service Discovery Protocol Specification (client)	vol 5 part A
SPP	Serial Port Profile Specification	vol 7 part B
Synch	Synchronization Profile Specification	vol 8 part D
TCI	Test Control Interface	vol 3 part D, section 2
TCP	Telephony Control Protocol Specification	vol 9 part A
UDI	Unrestricted Digital Information Profile Specification	vol 12 part B

Table 2.1: Abbreviations of the specification names.



Core Specification Change History

CONTENTS

1 Changes from V1.1 to V1.2 75
1.1 New Features 75
1.2 Structure Changes 75
1.3 Deprecated Specifications 75
1.4 Deprecated Features 76
1.5 Changes in Wording 76
1.6 Nomenclature Changes 76
2 Changes from V1.2 to V2.0 + EDR 77
2.1 New Features 77
2.2 Deprecated Features 77

1 CHANGES FROM V1.1 TO V1.2

1.1 NEW FEATURES

Several new features are introduced in the Bluetooth Core Specification 1.2. The major areas of improvement are:

- Architectural overview
- Faster connection
- Adaptive frequency hopping
- Extended SCO links
- Enhanced error detection and flow control
- Enhanced synchronization capability
- Enhanced flow specification

The feature descriptions are incorporated into the existing text in different core parts, described in vol2 and vol3.

1.2 STRUCTURE CHANGES

The Bluetooth Core Specification 1.2 has been significantly restructured for better consistency and readability. The most important structure changes have been performed in Baseband, LMP, HCI and L2CAP. The text in these sections has been rearranged to provide:

- Presentation of the information in a more logical progression
- Removal of redundant text and requirements
- Consolidation of baseband related requirements (for example, the *Baseband Timers* and *Bluetooth Audio* sections into the Baseband Specification)
- Alignment of the specification with the new architecture and terminology presented in the Architecture Overview (see Part A, IEEE Language)

In addition, new text and requirements have been added for the new features as well as many changes throughout the specification to update the text to use IEEE language (see Part E, IEEE Language).

1.3 DEPRECATED SPECIFICATIONS

As the Bluetooth Specification continues to evolve, some features, protocols, and profiles are replaced with new ways of performing the same function. Often these changes reflect the evolution of the communications industry. Some of the changes merely reflect an evolved understanding of the Bluetooth environment itself.

Those functions no longer recommended are being deprecated. The term *deprecation* does not mean that they are no longer allowed, but that they are no longer recommended as the best way of performing a given function.

Specifications that have been deprecated will not be included in the updated Bluetooth Specifications. Deprecation also discontinues all further maintenance of specific associated Test Specifications, PICS and TCRL-records. After deprecation, qualification remains enabled, however, towards a requirement and document set that no longer is maintained, but the earlier versions are still available and may be used according to the rules set forth in the Qualification Policy (PRD).

1.4 DEPRECATED FEATURES

Features deprecated in version 1.2 are:

- The use of Unit Keys for security
- Optional Paging schemes
- 23 channel hopping sequence
- Page scan period mode

1.5 CHANGES IN WORDING

Two general classes of changes to the wording of the Bluetooth Specification have been done for version 1.2. They are a formalization of the language by using conventions established by the Institute of Electrical and Electronic Engineers (IEEE), and a regularization of Bluetooth wireless technology-specific terms. Many portions of the version 1.1 specification use imprecise or inaccurate terms to describe attributes of the protocol. A more accurate terminology described in Part E has been introduced into the version 1.2 specification and will be applied in future versions.

1.6 NOMENCLATURE CHANGES

The nomenclature in Bluetooth 1.2 has also been updated due to new concepts that are introduced together with the new features and the new architecture (see [Part A] Section 1.2 on page 15).

2 CHANGES FROM V1.2 TO V2.0 + EDR

2.1 NEW FEATURES

The Bluetooth Core Specification version 2.0 + EDR introduces Enhanced Data Rate (EDR). EDR provides a set of additional packet types that use the new 2 Mbps and 3 Mbps modes.

In addition to EDR a set of errata provided in ESR for Core and HCI Transports C1.2V10r00 has been incorporated into this version and revised to include changes caused by the addition of EDR.

These additions are incorporated into the existing text in different core parts described in Volumes 2 and 3.

2.2 DEPRECATED FEATURES

The only feature deprecated in version 2.0 + EDR is the Page Scan Period Mode and associated commands (based on Erratum 694 which is also included in ESR for Core and HCI Transports C1.2V10r00.



Mixing of Specification Versions

CONTENTS

1 Mixing of Specification Versions 81

1.1 features and their types 82

1 MIXING OF SPECIFICATION VERSIONS

This part describes how different versions of the Core System Packages can be mixed in Bluetooth implementations. The Core System Packages consist of a Controller Package (see volume 2) and a Host Package (see volume 3).

In order to describe how these packages can be mixed, one needs to distinguish between four categories of features specified in the different specification versions. The four categories are:

Category	Description
Type 1	Feature that exists below HCI and cannot be configured via HCI
Type 2	Feature that exists below HCI and can be configured/enabled via HCI
Type 3	Feature that exists below and above HCI and requires HCI command/ events to function
Type 4	Feature that exists only above HCI

The outcome of mixing different core system packages are derived from the feature definitions in the table above:

- If an implementation contains features of type 1 or type 4, these features can function with any combination of Host Package and- Controller Package versions.
- If an implementation contains features of type 2, these features can only be used under a default condition if a Host Package of an older version is mixed with a Controller Package of this version.
- In order to fully use the feature under all conditions, the Host Package and Controller Package must be of the same version.
- If an implementation contains features of type 3, these features can only function with a Host Package and a Controller Package both in the same version.

1.1 FEATURES AND THEIR TYPES

The following table lists the features and their types.

Feature	Version	Type
Basic AFH operation	V1.2	1
Enhanced inquiry	V1.2	1
Configuration of AFH (setting channels and enabling/disabling channel assessment)	V1.2	2
Enhanced synchronization capability	V1.2	2
Interlaced inquiry scan	V1.2	2
Interlaced page scan	V1.2	2
Broadcast encryption	V1.2	2
Enhanced flow specification and flush time-out	V1.2	3
Extended SCO links	V1.2	3
Inquiry Result with RSSI	V1.2	3
L2CAP flow and error control	V1.2	4
2Mbps EDR	V2.0 + EDR	2
3Mbps EDR	V2.0 + EDR	2
3 slot packets in EDR	V2.0 + EDR	2
5 slot packets in EDR	V2.0 + EDR	2
2 Mbps eSCO	V2.0 + EDR	2*
3 Mbps eSCO	V2.0 + EDR	2*
3 slot packets for EDR eSCO	V2.0 + EDR	2*

The EDR eSCO options are marked as 2* because eSCO requires profile support, but if a product includes the eSCO option from V1.2, then EDR eSCO will be supported without any new support above HCI.



IEEE Language

CONTENTS

1 Use of IEEE Language 87

1.1 Shall 87

1.2 Must 88

1.3 Will 88

1.4 Should 88

1.5 May 88

1.6 Can 89

1 USE OF IEEE LANGUAGE

One of the purposes of this terminology is to make it easy for the reader to identify text that diatribes requirements as opposed to background information. The general term for text that describes attributes that are required for proper implementation of Bluetooth wireless technology is normative. The general term for language that provides background and context for normative text is informative. These terms are used in various sections to clarify implementation requirements.

Many portions of the Bluetooth Specification use imprecise or inaccurate terms to describe attributes of the protocol. This subsection describes the correct usage of key terms that indicate degree of requirements for processes and data structures. The information here was derived from the Institute of Electrical and Electronic Engineers (IEEE) Style Guide, see http://standards.ieee.org/guides/style/.

The following list is a summary of the terms to be discussed in more detail below:

shall	is required to – used to define requirements
must	is a natural consequence of -- used only to describe unavoidable situations
will	it is true that -- only used in statements of fact
should	is recommended that – used to indicate that among several possibilities one is recommended as particularly suitable, but not required
may	is permitted to – used to allow options
can	is able to – used to relate statements in a causal fashion
is	is defined as – used to further explain elements that are previously required or allowed
note	<informational text ONLY>

For clarity of the definition of those terms, the following sections document why and how they are used. For these sections only, the IEEE terms are italicized to indicate their use as a noun. Uses and examples of the use of the terms in this section are underlined.

1.1 SHALL

The word *shall* is used to indicate mandatory requirements that shall be followed in order to conform to the specification and from which no deviation is permitted.

There is a strong implication that the presence of the word *shall* indicates a testable requirement. All testable requirements shall be reflected in the Protocol Implementation Conformance Statement (PICS). In turn, all PICS indicators should be reflected in the Test Cases (TCs) either directly or indirectly.

A direct reference is a specific test for the attribute cited in the text. For example, a minimum value for a given parameter may be an entry in the TCs. Indirect test coverage may be appropriate if the existence of the attribute is requisite for passing a higher level test.

1.2 MUST

The word *must* shall not be used when stating mandatory requirements. *Must* is used only to describe unavoidable situations and is seldom appropriate for the text of a Specification.

An example of an appropriate use of the term *must* is: “the Bluetooth radios must be in range of each other to communicate”.

1.3 WILL

The use of the word *will* shall not be used when stating mandatory requirements. The term *will* is only used in statements of fact. As with the term *must*, *will* is not generally applicable to the description of a protocol. An example of appropriate use of will is: “when power is removed from the radio, it can be assumed that communications will fail”

1.4 SHOULD

Should equals *is recommended that*. The word *should* is used to indicate that among several possibilities one is recommended as particularly suitable without mentioning or excluding others. Alternatively it may indicate that a certain course of action is preferred but not necessarily required. Finally, in the negative form, it indicates a certain course of action is deprecated but not prohibited.

In the Bluetooth Specification the term designates an optional attribute that may require an entry in the PICS.

Explicit specification of alternatives should be done when using *should*.

1.5 MAY

The word *may* is used to indicate a course of action permissible within the limits of the specification. The term *may* equals *is permitted*. This is generally used when there is a single, optional attribute described, but multiple alternatives may be cited.

The use of *may* implies an optional condition in the PICS and therefore may need to be reflected in the corresponding test cases.

1.6 CAN

The word *can* is used for statements of possibility and capability, whether material, physical, or causal. The term *can* equals *is able to*.

The term *can* shall be used only in informative text. It describes capabilities by virtue of the rules established by normative text.





Specification Volume 2

Specification of the Bluetooth System

Wireless connections made easy

Core System Package

[Controller volume]

Covered Core Package version:
2.0 + EDR
Current Master TOC issued:
4 November 2004

Bluetooth®

Revision History

The Revision History is shown in the “Appendix” on page 51[vol. 0].

Contributors

The persons who contributed to this specification are listed in the “Appendix” on page 51[vol. 0].

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, 2000, 2001, 2002, 2003, 2004

Agere Systems, Inc.,
Ericsson Technology Licensing, AB,
IBM Corporation,
Intel Corporation,
Microsoft Corporation,
Motorola, Inc.,
Nokia Corporation,
Toshiba Corporation

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

Part A
RADIO SPECIFICATION

Contents **25**

1 Scope **27**

2 Frequency Bands and Channel Arrangement **29**

3 Transmitter Characteristics **31**

3.1 Basic Rate 32

3.1.1 Modulation Characteristics 32

3.1.2 Spurious Emissions 33

3.1.3 Radio Frequency Tolerance 34

3.2 Enhanced Data Rate 34

3.2.1 Modulation Characteristics 34

3.2.2 Spurious Emissions 37

3.2.3 Radio Frequency Tolerance 38

3.2.4 Relative Transmit Power 39

4 Receiver Characteristics **41**

4.1 Basic Rate 41

4.1.1 Actual Sensitivity Level 41

4.1.2 Interference Performance 41

4.1.3 Out-of-Band Blocking 42

4.1.4 Intermodulation Characteristics 42

4.1.5 Maximum Usable Level 43

4.1.6 Receiver Signal Strength Indicator **43**

4.1.7 Reference Signal Definition 43

4.2 Enhanced Data Rate 43

4.2.1 Actual Sensitivity Level 43

4.2.2 BER Floor Performance 43

4.2.3 Interference Performance 43

4.2.4 Maximum Usable Level 44

4.2.5 Out-of-Band and Intermodulation Characteristics 45

4.2.6 Reference Signal Definition 45

5 Appendix A **47**

5.1 Nominal Test Conditions 47

5.1.1 Nominal temperature 47

5.1.2 Nominal power source 47

5.2 Extreme Test Conditions 48

5.2.1 Extreme temperatures 48

5.2.2 Extreme power source voltages 48

6 Appendix B 49

7 Appendix C 51

7.1 Enhanced Data Rate Modulation Accuracy 51

Part B
BASEBAND SPECIFICATION

Contents 57

1 General Description 63

1.1 Bluetooth Clock 64

1.2 Bluetooth Device Addressing 66

1.2.1 Reserved addresses 66

1.3 Access Codes 67

2 Physical Channels 69

2.1 Physical Channel Definition 70

2.2 Basic Piconet Physical Channel 70

2.2.1 Master-slave definition 70

2.2.2 Hopping characteristics 71

2.2.3 Time slots 71

2.2.4 Piconet clocks 72

2.2.5 Transmit/receive timing 72

2.3 Adapted Piconet Physical Channel 75

2.3.1 Hopping characteristics 75

2.4 Page Scan Physical Channel 76

2.4.1 Clock estimate for paging 76

2.4.2 Hopping characteristics 76

2.4.3 Paging procedure timing 77

2.4.4 Page response timing 78

2.5 Inquiry Scan Physical Channel 80

2.5.1 Clock for inquiry 80

2.5.2 Hopping characteristics 80

2.5.3 Inquiry procedure timing 80

2.5.4 Inquiry response timing 80

2.6 Hop Selection 82

2.6.1 General selection scheme 82

2.6.2 Selection kernel 86

2.6.3 Adapted hop selection kernel 89

2.6.4 Control word 90

3 Physical Links 95

3.1 Link Supervision 95

4 Logical Transports 97
4.1 General 97
4.2 Logical Transport Address (LT_ADDR) 97
4.3 Synchronous Logical Transports 98
4.4 Asynchronous Logical Transport 98
4.5 Transmit/Receive Routines 99
4.5.1 TX Routine 99
4.5.2 RX routine 102
4.5.3 Flow control 103
4.6 Active Slave Broadcast Transport 104
4.7 Parked Slave Broadcast Transport 105
4.7.1 Parked member address (PM_ADDR) 105
4.7.2 Access request address (AR_ADDR) 105
5 Logical Links 107
5.1 Link Control Logical Link (LC) 107
5.2 ACL Control Logical Link (ACL-C) 107
5.3 User Asynchronous/Isochronous Logical Link (ACL-U) 107
5.3.1 Pausing the ACL-U logical link 108
5.4 User Synchronous Data Logical Link (SCO-S) 108
5.5 User Extended Synchronous Data Logical Link (eSCO-S) 108
5.6 Logical Link Priorities 108
6 Packets 109
6.1 General Format 109
6.1.1 Basic Rate 109
6.1.2 Enhanced Data Rate 109
6.2 Bit Ordering 110
6.3 Access Code 111
6.3.1 Access code types 111
6.3.2 Preamble 112
6.3.3 Sync word 112
6.3.4 Trailer 115
6.4 Packet Header 116
6.4.1 LT_ADDR 116
6.4.2 TYPE 116
6.4.3 FLOW 117
6.4.4 ARQN 117
6.4.5 SEQN 117
6.4.6 HEC 117
6.5 Packet Types 118
6.5.1 Common packet types 119

6.5.2 SCO packets 123
6.5.3 eSCO packets 124
6.5.4 ACL packets 126
6.6 Payload Format 128
6.6.1 Synchronous data field 128
6.6.2 Asynchronous data field 130
6.7 Packet Summary 134
7 Bitstream Processing 137
7.1 Error Checking 138
7.1.1 HEC generation 138
7.1.2 CRC generation 139
7.2 Data Whitening 141
7.3 Error Correction 142
7.4 FEC Code: Rate 1/3 142
7.5 FEC Code: Rate 2/3 143
7.6 ARQ Scheme 144
7.6.1 Unnumbered ARQ 144
7.6.2 Retransmit filtering 147
7.6.3 Flushing payloads 150
7.6.4 Multi-slave considerations 150
7.6.5 Broadcast packets 150
8 Link Controller Operation 153
8.1 Overview of States 153
8.2 Standby State 154
8.3 Connection Establishment Substates 154
8.3.1 Page scan substate 154
8.3.2 Page substate 156
8.3.3 Page response substates 159
8.4 Device Discovery Substates 163
8.4.1 Inquiry scan substate 164
8.4.2 Inquiry substate 165
8.4.3 Inquiry response substate 166
8.5 Connection State 167
8.6 Active Mode 168
8.6.1 Polling in the active mode 169
8.6.2 SCO 169
8.6.3 eSCO 171
8.6.4 Broadcast scheme 173
8.6.5 Role switch 175

8.6.6 Scatternet 177
8.6.7 Hop sequence switching 178
8.6.8 Channel classification and channel map selection 181
8.6.9 Power Management 182
8.7 sniff Mode 183
8.7.1 Sniff Transition Mode 184
8.8 Hold Mode 185
8.9 Park State 185
8.9.1 Beacon train 186
8.9.2 Beacon access window 189
8.9.3 Parked slave synchronization 190
8.9.4 Parking 191
8.9.5 Master-initiated unparking 192
8.9.6 Slave-initiated unparking 192
8.9.7 Broadcast scan window 193
8.9.8 Polling in the park state 193

9 Audio 195
9.1 LOG PCM CODEC 195
9.2 CVSD CODEC 195
9.3 Error Handling 198
9.4 General Audio Requirements 198
9.4.1 Signal levels 198
9.4.2 CVSD audio quality 198

10 List of Figures 199

11 List of Tables 203

12 Appendix 203
Appendix A: ..... General Audio Recommendations 204
Appendix B: ..... Timers 207
Appendix C: .....
Recommendations for AFH Operation in Park, Hold and Sniff 209

Part C
LINK MANAGER PROTOCOL

Contents 213

1 Introduction 217

2 General Rules 219
2.1 Message Transport 219
2.2 Synchronization 219
2.3 Packet Format 220

2.4 Transactions 221
2.4.1 LMP Response Timeout 222
2.5 Error Handling 222
2.5.1 Transaction collision resolution 223
2.6 Procedure Rules 223
2.7 General Response Messages 224
2.8 LMP Message Constraints 224
3 Device Features 225
3.1 General Description 225
3.2 Feature Definitions 225
3.3 Feature Mask Definition 230
3.4 Link Manager Interoperability policy 232
4 Procedure Rules 233
4.1 Connection Control 233
4.1.1 Connection establishment 233
4.1.2 Detach 234
4.1.3 Power control 235
4.1.4 Adaptive frequency hopping 237
4.1.5 Channel classification 240
4.1.6 Link supervision 242
4.1.7 Channel quality driven data rate change (CQDDR) 243
4.1.8 Quality of service (QoS) 244
4.1.9 Paging scheme parameters 246
4.1.10 Control of multi-slot packets 247
4.1.11 Enhanced Data Rate 247
4.2 Security 249
4.2.1 Authentication 249
4.2.2 Pairing 251
4.2.3 Change link key 254
4.2.4 Change current link key type 255
4.2.5 Encryption 257
4.2.6 Request supported encryption key size 261
4.3 Informational Requests 262
4.3.1 Timing accuracy 262
4.3.2 Clock offset 263
4.3.3 LMP version 263
4.3.4 Supported features 264
4.3.5 Name request 266
4.4 Role Switch 267

4.4.1 Slot offset 267
4.4.2 Role switch 268
4.5 Modes of Operation 270
4.5.1 Hold mode 270
4.5.2 Park state 272
4.5.3 Sniff mode 278
4.6 Logical Transports 281
4.6.1 SCO logical transport 281
4.6.2 eSCO logical transport 284
4.7 Test Mode 289
4.7.1 Activation and deactivation of test mode 289
4.7.2 Control of test mode 290
4.7.3 Summary of test mode PDUs 291
5 Summary 295
5.1 PDU Summary 295
5.2 Parameter Definitions 303
5.3 Default Values 311
6 List of Figures 313
7 List of Tables 317

Part D
ERROR CODES

Contents 321
1 Overview of Error Codes 323
1.1 Usage Descriptions 323
1.2 HCI Command Errors 323
1.3 List of Error Codes 324
2 Error Code Descriptions 327
2.1 Unknown HCI Command (0X01) 327
2.2 Unknown Connection Identifier (0X02) 327
2.3 Hardware Failure (0X03) 327
2.4 Page Timeout (0X04) 327
2.5 Authentication Failure (0X05) 327
2.6 PIN or key Missing (0X06) 327
2.7 Memory Capacity Exceeded (0X07) 327
2.8 Connection Timeout (0X08) 328
2.9 Connection Limit Exceeded (0X09) 328
2.10 Synchronous Connection Limit to a Device Exceeded (0X0A) 328
2.11 ACL Connection Already Exists (0X0B) 328
2.12 Command Disallowed (0X0C) 328

2.13 Connection Rejected due to Limited Resources (0X0D) 328
2.14 Connection Rejected due to Security Reasons (0X0E) 328
2.15 Connection Rejected due to Unacceptable BD_ADDR (0X0F)329
2.16 Connection Accept Timeout Exceeded (0X10) 329
2.17 Unsupported Feature or Parameter Value (0X11) 329
2.18 Invalid HCI Command Parameters (0X12) 329
2.19 Remote User Terminated Connection (0X13) 329
2.20 Remote Device Terminated Connection due to Low Resources (0X14)330
2.21 Remote Device Terminated Connection due to Power Off (0X15). 330
2.22 Connection Terminated by Local Host (0X16) 330
2.23 Repeated Attempts (0X17) 330
2.24 Pairing not Allowed (0X18) 330
2.25 Unknown LMP PDU (0X19) 330
2.26 Unsupported Remote Feature / Unsupported LMP Feature (0X1A)330
2.27 SCO Offset Rejected (0X1B) 330
2.28 SCO Interval Rejected (0X1C) 331
2.29 SCO Air Mode Rejected (0X1D) 331
2.30 Invalid LMP Parameters (0X1E) 331
2.31 Unspecified Error (0X1F) 331
2.32 Unsupported LMP Parameter Value (0X20) 331
2.33 Role Change Not Allowed (0X21) 331
2.34 LMP Response Timeout (0X22) 331
2.35 LMP Error Transaction Collision (0X23) 332
2.36 LMP PDU Not Allowed (0X24) 332
2.37 Encryption Mode Not Acceptable (0X25) 332
2.38 Link Key Can Not be Changed (0X26) 332
2.39 Requested Qos Not Supported (0X27) 332
2.40 Instant Passed (0X28) 332
2.41 Pairing with Unit Key Not Supported (0X29) 332
2.42 Different Transaction Collision (0x2a) 332
2.43 QoS Unacceptable Parameter (0X2C) 332
2.44 QoS Rejected (0X2D) 333
2.45 Channel Classification Not Supported (0X2E) 333
2.46 Insufficient Security (0X2F) 333
2.47 Parameter out of Mandatory Range (0X30) 333
2.48 Role Switch Pending (0X32) 333
2.49 Reserved Slot Violation (0X34) 333
2.50 Role Switch Failed (0X35) 333

Part E

HOST CONTROLLER INTERFACE FUNCTIONAL SPECIFICATION

Contents **337**

1 Introduction **343**
1.1 Lower Layers of the Bluetooth Software Stack 343

2 Overview of Host Controller Transport Layer **345**

3 Overview of Commands and Events **347**
3.1 Generic Events 348
3.2 Device Setup 348
3.3 Controller Flow Control 349
3.4 Controller Information 349
3.5 Controller Configuration 350
3.6 Device Discovery 351
3.7 Connection Setup 353
3.8 Remote Information 355
3.9 Synchronous Connections 356
3.10 Connection State 357
3.11 Piconet Structure 358
3.12 Quality of Service 359
3.13 Physical Links 360
3.14 Host Flow Control 361
3.15 Link Information 362
3.16 Authentication and Encryption 363
3.17 Testing 365
3.18 Alphabetical List of Commands and Events 366

4 HCI Flow Control **371**
4.1 Host to Controller Data Flow Control 371
4.2 Controller to Host Data Flow Control 372
4.3 Disconnection Behavior 373
4.4 Command Flow Control 373
4.5 Command Error Handling 374

5 HCI Data Formats **375**
5.1 Introduction 375
5.2 Data and Parameter Formats 375
5.3 Connection Handles 376
5.4 Exchange of HCI-Specific Information 377
5.4.1 HCI Command Packet 377
5.4.2 HCI ACL Data Packets 379
5.4.3 HCI Synchronous Data Packets 381
5.4.4 HCI Event Packet 382

6 HCI Configuration Parameters **383**

6.1 Scan Enable 383
6.2 Inquiry Scan Interval 383
6.3 Inquiry Scan Window 384
6.4 Inquiry Scan Type 384
6.5 Inquiry Mode 384
6.6 Page Timeout 385
6.7 Connection Accept Timeout 385
6.8 Page Scan Interval 386
6.9 Page Scan Window 386
6.10 Page Scan Period Mode (Deprecated) 386
6.11 Page Scan Type 387
6.12 Voice Setting 387
6.13 PIN Type 388
6.14 Link Key 388
6.15 Authentication Enable 388
6.16 Encryption Mode 389
6.17 Failed Contact Counter 390
6.18 Hold Mode Activity 390
6.19 Link Policy Settings 391
6.20 Flush Timeout 392
6.21 Num Broadcast Retransmissions 392
6.22 Link Supervision Timeout 393
6.23 Synchronous Flow Control Enable 393
6.24 Local Name 394
6.25 Class Of Device 394
6.26 Supported Commands 395

7 HCI Commands and Events 399

7.1 Link Control Commands 399
7.1.1 Inquiry Command 399
7.1.2 Inquiry Cancel Command 401
7.1.3 Periodic Inquiry Mode Command 402
7.1.4 Exit Periodic Inquiry Mode Command 405
7.1.5 Create Connection Command 406
7.1.6 Disconnect Command 409
7.1.7 Create Connection Cancel Command 410
7.1.8 Accept Connection Request Command 412
7.1.9 Reject Connection Request Command 414
7.1.10 Link Key Request Reply Command 415
7.1.11 Link Key Request Negative Reply Command 417
7.1.12 PIN Code Request Reply Command 418
7.1.13 PIN Code Request Negative Reply Command 420

7.1.14 Change Connection Packet Type Command 421
7.1.15 Authentication Requested Command.....424
7.1.16 Set Connection Encryption Command 425
7.1.17 Change Connection Link Key Command 426
7.1.18 Master Link Key Command 427
7.1.19 Remote Name Request Command 428
7.1.20 Remote Name Request Cancel Command 430
7.1.21 Read Remote Supported Features Command.....431
7.1.22 Read Remote Extended Features Command 432
7.1.23 Read Remote Version Information Command.....433
7.1.24 Read Clock Offset Command.....434
7.1.25 Read LMP Handle Command 435
7.1.26 Setup Synchronous Connection Command 437
7.1.27 Accept Synchronous Connection Request Command 442
7.1.28 Reject Synchronous Connection Request Command .446
7.2 Link Policy Commands.....447
7.2.1 Hold Mode Command 447
7.2.2 Sniff Mode Command.....449
7.2.3 Exit Sniff Mode Command.....452
7.2.4 Park State Command 453
7.2.5 Exit Park State Command 455
7.2.6 QoS Setup Command 456
7.2.7 Role Discovery Command.....458
7.2.8 Switch Role Command.....459
7.2.9 Read Link Policy Settings Command 460
7.2.10 Write Link Policy Settings Command 461
7.2.11 Read Default Link Policy Settings Command 463
7.2.12 Write Default Link Policy Settings Command 464
7.2.13 Flow Specification Command 465
7.3 Controller & Baseband Commands.....467
7.3.1 Set Event Mask Command.....467
7.3.2 Reset Command 469
7.3.3 Set Event Filter Command 470
7.3.4 Flush Command 475
7.3.5 Read PIN Type Command 477
7.3.6 Write PIN Type Command.....478
7.3.7 Create New Unit Key Command 479
7.3.8 Read Stored Link Key Command 480

7.3.9 Write Stored Link Key Command 481
7.3.10 Delete Stored Link Key Command 483
7.3.11 Write Local Name Command 484
7.3.12 Read Local Name Command 485
7.3.13 Read Connection Accept Timeout Command 486
7.3.14 Write Connection Accept Timeout Command 487
7.3.15 Read Page Timeout Command 488
7.3.16 Write Page Timeout Command 489
7.3.17 Read Scan Enable Command 490
7.3.18 Write Scan Enable Command 491
7.3.19 Read Page Scan Activity Command 492
7.3.20 Write Page Scan Activity Command 494
7.3.21 Read Inquiry Scan Activity Command 495
7.3.22 Write Inquiry Scan Activity Command 496
7.3.23 Read Authentication Enable Command 497
7.3.24 Write Authentication Enable Command 498
7.3.25 Read Encryption Mode Command 499
7.3.26 Write Encryption Mode Command 500
7.3.27 Read Class of Device Command 501
7.3.28 Write Class of Device Command 502
7.3.29 Read Voice Setting Command 503
7.3.30 Write Voice Setting Command 504
7.3.31 Read Automatic Flush Timeout Command 505
7.3.32 Write Automatic Flush Timeout Command 506
7.3.33 Read Num Broadcast Retransmissions Command 507
7.3.34 Write Num Broadcast Retransmissions Command 508
7.3.35 Read Hold Mode Activity Command 509
7.3.36 Write Hold Mode Activity Command 510
7.3.37 Read Transmit Power Level Command 511
7.3.38 Read Synchronous Flow Control Enable Command ... 513
7.3.39 Write Synchronous Flow Control Enable Command ... 514
7.3.40 Set Controller To Host Flow Control Command 515
7.3.41 Host Buffer Size Command 516
7.3.42 Host Number Of Completed Packets Command 518
7.3.43 Read Link Supervision Timeout Command 520
7.3.44 Write Link Supervision Timeout Command 521
7.3.45 Read Number Of Supported IAC Command 523
7.3.46 Read Current IAC LAP Command 524

7.3.47 Write Current IAC LAP Command....525
7.3.48 Read Page Scan Period Mode Command (Deprecated) .. 527
7.3.49 Write Page Scan Period Mode Command (Deprecated) .. 528
7.3.50 Set AFH Host Channel Classification Command 529
7.3.51 Read Inquiry Scan Type Command 530
7.3.52 Write Inquiry Scan Type Command 531
7.3.53 Read Inquiry Mode Command 532
7.3.54 Write Inquiry Mode Command 533
7.3.55 Read Page Scan Type Command 534
7.3.56 Write Page Scan Type Command 535
7.3.57 Read AFH Channel Assessment Mode Command 536
7.3.58 Write AFH Channel Assessment Mode Command 537
7.4 Informational Parameters....539
7.4.1 Read Local Version Information Command....539
7.4.2 Read Local Supported Commands Command....541
7.4.3 Read Local Supported Features Command....542
7.4.4 Read Local Extended Features Command 543
7.4.5 Read Buffer Size Command....545
7.4.6 Read BD_ADDR Command....547
7.5 Status Parameters....548
7.5.1 Read Failed Contact Counter Command 548
7.5.2 Reset Failed Contact Counter Command 550
7.5.3 Read Link Quality Command 551
7.5.4 Read RSSI Command....552
7.5.5 Read AFH Channel Map Command 554
7.5.6 Read Clock Command 556
7.6 Testing Commands 558
7.6.1 Read Loopback Mode Command 558
7.6.2 Write Loopback Mode Command....559
7.6.3 Enable Device Under Test Mode Command 562
7.7 Events 563
7.7.1 Inquiry Complete Event....563
7.7.2 Inquiry Result Event....564
7.7.3 Connection Complete Event....566
7.7.4 Connection Request Event....567
7.7.5 Disconnection Complete Event 569
7.7.6 Authentication Complete Event 570

7.7.7 Remote Name Request Complete Event 571
7.7.8 Encryption Change Event 572
7.7.9 Change Connection Link Key Complete Event 573
7.7.10 Master Link Key Complete Event 574
7.7.11 Read Remote Supported Features Complete Event ... 575
7.7.12 Read Remote Version Information Complete Event ... 576
7.7.13 QoS Setup Complete Event 577
7.7.14 Command Complete Event 579
7.7.15 Command Status Event 580
7.7.16 Hardware Error Event 581
7.7.17 Flush Occurred Event 581
7.7.18 Role Change Event 582
7.7.19 Number Of Completed Packets Event 583
7.7.20 Mode Change Event 584
7.7.21 Return Link Keys Event 586
7.7.22 PIN Code Request Event 587
7.7.23 Link Key Request Event 588
7.7.24 Link Key Notification Event 589
7.7.25 Loopback Command Event 590
7.7.26 Data Buffer Overflow Event 590
7.7.27 Max Slots Change Event 591
7.7.28 Read Clock Offset Complete Event 592
7.7.29 Connection Packet Type Changed Event 593
7.7.30 QoS Violation Event 596
7.7.31 Page Scan Repetition Mode Change Event 597
7.7.32 Flow Specification Complete Event 598
7.7.33 Inquiry Result with RSSI Event 600
7.7.34 Read Remote Extended Features Complete Event 602
7.7.35 Synchronous Connection Complete Event 603
7.7.36 Synchronous Connection Changed event 605

8 List of Figures 607

9 List of Tables 609

10 Appendix 609

Appendix A: Deprecated Commands, Events and Configuration Parameters 611

Part F
MESSAGE SEQUENCE CHARTS

Contents **621**

1 Introduction **623**
1.1 Notation 623
1.2 Flow of Control 624
1.3 Example MSC 624

2 Services Without Connection Request **625**
2.1 Remote Name Request 625
2.2 One-time Inquiry 626
2.3 Periodic Inquiry 628

3 ACL Connection Establishment and Detachment **631**
3.1 Connection Setup 632

4 Optional Activities After ACL Connection Establishment **639**
4.1 Authentication Requested 639
4.2 Set Connection Encryption 640
4.3 Change Connection Link Key 641
4.4 Master Link Key 642
4.5 Read Remote Supported Features 644
4.6 Read Remote Extended Features 644
4.7 Read Clock Offset 645
4.8 Read Remote Version Information 645
4.9 QOS Setup 646
4.10 Switch Role 646

5 Synchronous Connection Establishment and Detachment **649**
5.1 Synchronous Connection Setup 649

6 Sniff, Hold and Park **655**
6.1 sniff Mode 655
6.2 Hold Mode 656
6.3 Park State 658

7 Buffer Management, Flow Control **661**

8 Loopback Mode **663**
8.1 Local Loopback Mode 663
8.2 Remote Loopback Mode 665

9 List of Figures **667**

Part G
SAMPLE DATA

Contents **671**

1 Encryption Sample Data **673**
1.1 Generating Kc' from Kc, ... 673

1 Encryption Sample Data 673
1.2 First Set of Sample Data 676
1.3 Second Set of Sample Data 684
1.4 Third Set of Samples 692
1.5 Fourth Set of Samples 700
2 Frequency Hopping Sample Data 709
2.1 First set 710
2.2 Second set 716
2.3 Third set 722
3 Access Code Sample Data 729
4 HEC and Packet Header Sample Data 733
5 CRC Sample Data 735
6 Complete Sample Packets 737
6.1 Example of DH1 Packet 737
6.2 Example of DM1 Packet 738
7 Whitening Sequence Sample Data 739
8 FEC Sample Data 743
9 Encryption Key Sample Data 745
9.1 Four Tests of E1 745
9.2 Four Tests of E21 750
9.3 Three Tests of E22 752
9.4 Tests of E22 With Pin Augmenting 754
9.5 Four Tests of E3 764

Part H
SECURITY SPECIFICATION

Contents 771
1 Security Overview 773
2 Random Number Generation 775
3 Key Management 777
3.1 Key Types 777
3.2 Key Generation and Initialization 779
3.2.1 Generation of initialization key, ... 780
3.2.2 Authentication 780
3.2.3 Generation of a unit key 780
3.2.4 Generation of a combination key 781
3.2.5 Generating the encryption key 782
3.2.6 Point-to-multipoint configuration 783

3.2.7 Modifying the link keys 784
3.2.8 Generating a master key 784
4 Encryption 787
4.1 Encryption Key Size Negotiation 788
4.2 Encryption of Broadcast Messages 788
4.3 Encryption Concept 789
4.4 Encryption Algorithm 790
4.4.1 The operation of the cipher 792
4.5 LFSR Initialization 793
4.6 Key Stream Sequence 796
5 Authentication 797
5.1 Repeated Attempts 799
6 The Authentication And Key-Generating Functions 801
6.1 The Authentication Function E1 801
6.2 The Functions Ar and A'r 803
6.2.1 The round computations 803
6.2.2 The substitution boxes "e" and "l" 803
6.2.3 Key scheduling 804
6.3 E2-Key Generation Function for Authentication 805
6.4 E3-Key Generation Function for Encryption 807
7 List of Figures 809
8 List of Tables 811

Core System Package [Controller volume]
Part A



RADIO SPECIFICATION

CONTENTS

1 Scope 27

2 Frequency Bands and Channel Arrangement 29

3 Transmitter Characteristics 31

3.1 Basic Rate 32

3.1.1 Modulation Characteristics 32

3.1.2 Spurious Emissions 33

3.1.2.1 In-band spurious emission 33

3.1.3 Radio Frequency Tolerance 34

3.2 Enhanced Data Rate 34

3.2.1 Modulation Characteristics 34

3.2.1.1 Modulation Method Overview 34

3.2.1.2 Differential Phase Encoding 35

3.2.1.3 Pulse Shaping 36

3.2.1.4 Modulation Accuracy 36

3.2.2 Spurious Emissions 37

3.2.2.1 In-band Spurious Emission 37

3.2.3 Radio Frequency Tolerance 38

3.2.4 Relative Transmit Power 39

4 Receiver Characteristics 41

4.1 Basic Rate 41

4.1.1 Actual Sensitivity Level 41

4.1.2 Interference Performance 41

4.1.3 Out-of-Band Blocking 42

4.1.4 Intermodulation Characteristics 42

4.1.5 Maximum Usable Level 43

4.1.6 Receiver Signal Strength Indicator 43

4.1.7 Reference Signal Definition 43

4.2 Enhanced Data Rate 43

4.2.1 Actual Sensitivity Level 43

4.2.2 BER Floor Performance 43

4.2.3 Interference Performance 43

4.2.4 Maximum Usable Level 44

4.2.5 Out-of-Band and Intermodulation Characteristics 45

4.2.6 Reference Signal Definition 45

5 Appendix A 47

5.1 Nominal Test Conditions 47

5.1.1 Nominal temperature 47

5.1.2 Nominal power source 47
5.1.2.1 Mains voltage 47
5.1.2.2 Lead-acid battery power sources used in vehicles 47
5.1.2.3 Other power sources 47
5.2 Extreme Test Conditions 48
5.2.1 Extreme temperatures 48
5.2.2 Extreme power source voltages 48
5.2.2.1 Mains voltage 48
5.2.2.2 Lead-acid battery power source used on vehicles 48
5.2.2.3 Power sources using other types of batteries 48
5.2.2.4 Other power sources 48
6 Appendix B 49
7 Appendix C 51
7.1 Enhanced Data Rate Modulation Accuracy 51

1 SCOPE

Bluetooth devices operate in the unlicensed 2.4 GHz ISM (Industrial Scientific Medical) band. A frequency hop transceiver is applied to combat interference and fading.

Two modulation modes are defined. A mandatory mode, called Basic Rate, uses a shaped, binary FM modulation to minimize transceiver complexity. An optional mode, called Enhanced Data Rate, uses PSK modulation and has two variants: π/4-DQPSK and 8DPSK. The symbol rate for all modulation schemes is 1 Ms/s. The gross air data rate is 1 Mbps for Basic Rate, 2 Mbps for Enhanced Data Rate using π/4-DQPSK and 3 Mbps for Enhanced Data Rate using 8DPSK.

For full duplex transmission, a Time Division Duplex (TDD) scheme is used in both modes. This specification defines the requirements for a Bluetooth radio for the Basic Rate and Enhanced Data Rate modes.

Requirements are defined for two reasons:

- Provide compatibility between radios used in the system
- Define the quality of the system

The Bluetooth radio shall fulfil the stated requirements under the operating conditions specified in Appendix A and Appendix B. The radio parameters shall be measured according to the methods described in the RF Test Specification.

This specification is based on the established regulations for Europe, Japan and North America. The standard documents listed below are only for information, and are subject to change or revision at any time.

Europe:

Approval Standards: European Telecommunications Standards Institute, ETSI
Documents: EN 300 328, ETS 300-826
Approval Authority: National Type Approval Authorities

Japan:

Approval Standards: Association of Radio Industries and Businesses, ARIB
Documents: ARIB STD-T66
Approval Authority: Ministry of Post and Telecommunications, MPT.

North America:

Approval Standards: Federal Communications Commission, FCC, USA
Documents: CFR47, Part 15, Sections 15.205, 15.209, 15.247 and 15.249

Approval Standards: Industry Canada, IC, Canada
Documents: GL36

Approval Authority: FCC (USA), Industry Canada (Canada)

2 FREQUENCY BANDS AND CHANNEL ARRANGEMENT

The Bluetooth system operates in the 2.4 GHz ISM band. This frequency band is 2400 - 2483.5 MHz.

Regulatory Range	RF Channels
2.400-2.4835 GHz	f=2402+k MHz, k=0,…,78

Table 2.1: Operating frequency bands

RF channels are spaced 1 MHz and are ordered in channel number k as shown in Table 2.1. In order to comply with out-of-band regulations in each country, a guard band is used at the lower and upper band edge.

Lower Guard Band	Upper Guard Band
2 MHz	3.5 MHz

Table 2.2: Guard Bands

3 TRANSMITTER CHARACTERISTICS

The requirements stated in this section are given as power levels at the antenna connector of the Bluetooth device. If the device does not have a connector, a reference antenna with 0 dBi gain is assumed.

Due to difficulty in measurement accuracy in radiated measurements, systems with an integral antenna should provide a temporary antenna connector during type approval.

If transmitting antennas of directional gain greater than 0 dBi are used, the applicable paragraphs in EN 300 328, EN 301 489-17and FCC part 15 shall be compensated for.

The device is classified into three power classes.

Power Class	Maximum Output Power (Pmax)	Nominal Output Power	Minimum Output Power[1]	Power Control
1	100 mW (20 dBm)	N/A	1 mW (0 dBm)	Pmin<+4 dBm to Pmax Optional: Pmin[2] to Pmax
2	2.5 mW (4 dBm)	1 mW (0 dBm)	0.25 mW (-6 dBm)	Optional: Pmin[2)] to Pmax
3	1 mW (0 dBm)	N/A	N/A	Optional: Pmin[2)] to Pmax

Table 3.1: Power classes

1. Minimum output power at maximum power setting.
2. The lower power limit Pmin<-30dBm is suggested but is not mandatory, and may be chosen according to application needs.

Power class 1 device shall implement power control. The power control is used for limiting the transmitted power over +4 dBm. Power control capability under +4 dBm is optional and could be used for optimizing the power consumption and overall interference level. The power steps shall form a monotonic sequence, with a maximum step size of 8 dB and a minimum step size of 2 dB. A class 1 device with a maximum transmit power of +20 dBm shall be able to control its transmit power down to 4 dBm or less.

Devices with power control capability optimizes the output power in a physical link with LMP commands (see Link Manager Protocol). It is done by measuring RSSI and reporting back if the transmission power shall be increased or decreased if possible.

In a connection, the output power shall not exceed the maximum output power of power class 2 for transmitting packets if the receiving device does not support the necessary messaging for sending the power control messages, see

Link Manager Protocol Section 4.1.3 on page 235. In this case, the transmitting device shall comply with the rules of a class 2 or class 3 device.

If a class 1 device is paging or inquiring very close to another device, the input power can be larger than the requirement in Section 4.1.5 on page 43. This can cause the receiving device to fail to respond. It may therefore be useful to page at Class 2 or 3 power in addition to paging at power class 1.

Devices shall not exceed the maximum allowed transmit power levels set by controlling regulatory bodies. The maximum allowed transmit power level may depend upon the modulation mode.

3.1 BASIC RATE

3.1.1 Modulation Characteristics

The Modulation is GFSK (Gaussian Frequency Shift Keying) with a bandwidth-bit period product BT=0.5. The Modulation index shall be between 0.28 and 0.35. A binary one shall be represented by a positive frequency deviation, and a binary zero shall be represented by a negative frequency deviation. The symbol timing shall be less than ±20 ppm.

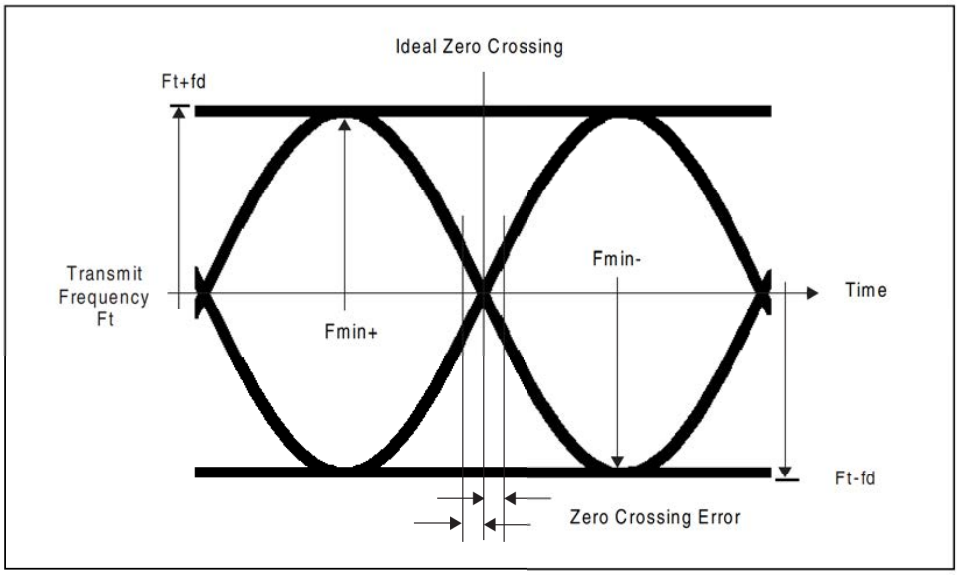


Figure 3.1: GFSK parameters definition.

For each transmission, the minimum frequency deviation, Fmin = min{|Fmin+|, Fmin-}, which corresponds to 1010 sequence shall be no smaller than ±80% of the frequency deviation (fd) with respect to the transmit frequency Ft, which corresponds to a 00001111 sequence.

In addition, the minimum frequency deviation shall never be smaller than 115 kHz. The data transmitted has a symbol rate of 1 Ms/s.

The zero crossing error is the time difference between the ideal symbol period and the measured crossing time. This shall be less than ± 1/8 of a symbol period.

3.1.2 Spurious Emissions

In-band spurious emissions shall be measured with a frequency hopping radio transmitting on one RF channel and receiving on a second RF channel; this means that the synthesizer may change RF channels between reception and transmission, but always returns to the same transmit RF channel. There will be no reference in this document to out of ISM band spurious emissions; the equipment manufacturer is responsible for compliance in the intended country of use.

3.1.2.1 In-band spurious emission

Within the ISM band the transmitter shall pass a spectrum mask, given in Table 3.2. The spectrum shall comply with the 20dB bandwidth definition in FCC part 15.247 and shall be measured accordingly. In addition to the FCC requirement an adjacent channel power on adjacent channels with a difference in RF channel number of two or greater is defined. This adjacent channel power is defined as the sum of the measured power in a 1 MHz RF channel. The transmitted power shall be measured in a 100 kHz bandwidth using maximum hold. The device shall transmit on RF channel M and the adjacent channel power shall be measured on RF channel number N. The transmitter shall transmit a pseudo random data pattern in the payload throughout the test.

Frequency offset	Transmit Power
± 500 kHz	-20 dBc
2MHz (|M-N| = 2)	-20 dBm
3MHz or greater (|M-N| ≥ 3)	-40 dBm

Table 3.2: Transmit Spectrum mask.

Note: If the output power is less than 0dBm then, wherever appropriate, the FCC's 20 dB relative requirement overrules the absolute adjacent channel power requirement stated in the above table.

Exceptions are allowed in up to three bands of 1 MHz width centered on a frequency which is an integer multiple of 1 MHz. They shall comply with an absolute value of –20 dBm.

3.1.3 Radio Frequency Tolerance

The transmitted initial center frequency shall be within ±75 kHz from F_C. The initial frequency accuracy is defined as being the frequency accuracy before any packet information is transmitted. Note that the frequency drift requirement is not included in the ±75 kHz.

The limits on the transmitter center frequency drift within a packet are specified in Table 3.3. The different packets are defined in the Baseband Specification.

Duration of Packet	Frequency Drift
Max length one slot packet	±25 kHz
Max length three slot packet	±40 kHz
Max length five slot packet	±40 kHz
Maximum drift rate[1]	400 Hz/µs

Table 3.3: Maximum allowable frequency drifts in a packet.

1. The maximum drift rate is allowed anywhere in a packet.

3.2 ENHANCED DATA RATE

A key characteristic of the Enhanced Data Rate mode is that the modulation scheme is changed within the packet. The access code and packet header, as defined in Table 6.1 in the Baseband Specification, are transmitted with the Basic Rate 1 Mbps GFSK modulation scheme, whereas the subsequent synchronization sequence, payload, and trailer sequence are transmitted using the Enhanced Data Rate PSK modulation scheme.

3.2.1 Modulation Characteristics

During access code and packet header transmission the Basic Rate GFSK modulation scheme shall be used. During the transmission of the synchronization sequence, payload, and trailer sequence a PSK type of modulation with a data rate of 2 Mbps or optionally 3 Mbps shall be used. The following subsections specify the PSK modulation for this transmission.

3.2.1.1 Modulation Method Overview

The PSK modulation format defined for the 2 Mbps transmission shall be π/4 rotated differential encoded quaternary phase shift keying (π/4-DQPSK).

The PSK modulation format defined for the 3 Mbps transmission shall be differential encoded 8-ary phase shift keying (8DPSK).

The modulation shall employ square-root raised cosine pulse shaping to generate the equivalent lowpass information-bearing signal v(t). The output of the transmitter shall be a bandpass signal that can be represented as

$$S(t) = Re\left[v(t)e^{j2\pi F_c t}\right] \quad \text{(EQ 1)}$$

with F_c denoting the carrier frequency.

3.2.1.2 Differential Phase Encoding

For the M-ary modulation, the binary data stream $\{b_n\}$, n=1,2,3, …N, shall be mapped onto a corresponding sequence {Sk}, k=1,2, …$N/\log_2(M)$ of complex valued signal points. M=4 applies for 2 Mbps and M=8 applies for 3 Mbps. Gray coding shall be applied as shown in Table 3.4 and Table 3.5. In the event that the length of the binary data stream N is not an integer multiple of log2(M), the last symbol of the sequence $\{S_k\}$ shall be formed by appending data zeros to the appropriate length. The signal points S_k shall be defined by:

$$S_k = S_{k-1}e^{j\varphi_k} \qquad k = 1, 2, ..N/\log_2(M) \quad \text{(EQ 2)}$$

$$S_0 = e^{j\phi} \qquad \text{with } \phi \in [0, 2\pi) \quad \text{(EQ 3)}$$

The relationship between the binary input b_k and the phase ϕ_k shall be as defined in Table 3.4 for the 2 Mbps transmission and in Table 3.5 for the 3 Mbps transmission.

b_{2k-1}	b_{2k}	φ_k
0	0	π/4
0	1	3π/4
1	1	-3π/4
1	0	-π/4

Table 3.4: π/4-DQPSK mapping.

b_{3k-2}	b_{3k-1}	b_{3k}	φ_k
0	0	0	0
0	0	1	π/4
0	1	1	π/2
0	1	0	3π/4
1	1	0	π
1	1	1	-3π/4
1	0	1	-π/2
1	0	0	-π/4

Table 3.5: 8DPSK mapping.

3.2.1.3 Pulse Shaping

The lowpass equivalent information-bearing signal v(t) shall be generated according to

$$v(t) = \sum_k S_k p(t - kT) \qquad \text{(EQ 4)}$$

in which the symbol period T shall be 1μs.

The frequency spectrum P(f), which corresponds to the square-root raised cosine pulse p(t) of the pulse shaping filter is:

$$|P(f)| = \begin{cases} 1 & 0 \le |f| \le \frac{1-\beta}{2T} \\ \sqrt{\frac{1}{2}\left(1 - \sin\left(\frac{\pi(2fT-1)}{2\beta}\right)\right)} & \frac{1-\beta}{2T} \le |f| \le \frac{1+\beta}{2T} \\ 0 & \text{elsewhere} \end{cases} \qquad \text{(EQ 5)}$$

The roll off factor β shall be 0.4.

3.2.1.4 Modulation Accuracy

The measurement of modulation accuracy utilizes differential error vector magnitude (DEVM) with tracking of the carrier frequency drift. The definition of DEVM and the derivation of the RMS and peak measures of DEVM are given in 51.

The DEVM shall be measured over the synchronization sequence and payload portions of the packet, but not the trailer symbols. For each modulation method and each measurement carrier frequency, DEVM measurement is made over a total of 200 non-overlapping blocks, where each block contains 50 symbols.

The transmitted packets shall be the longest supported packet type for each modulation method, as defined in Table 6.9 and Table 6.10 in the Baseband part.

The DEVM is measured using a square-root raised cosine filter, with a roll-off of 0.4 and a 3 dB bandwidth of ±500 kHz.

3.2.1.4.1 RMS DEVM

The RMS DEVM for any of the measured blocks shall not exceed 0.20 for π/4-DQPSK and 0.13 for 8DPSK.

3.2.1.4.2 99% DEVM

The 99% DEVM (defined as the DEVM value for which 99% of measured symbols have a lower DEVM) shall not exceed 0.30 for π/4-DQPSK and 0.20 for 8DPSK.

3.2.1.4.3 Peak DEVM

The Peak DEVM shall not exceed 0.35 for π/4-DQPSK and 0.25 for 8DPSK.

3.2.2 Spurious Emissions

In-band spurious emissions shall be measured with a frequency hopping radio transmitting on one RF channel and receiving on a second RF channel; this means that the synthesizer may change RF channels between reception and transmission, but always returns to the same transmit RF channel. There will be no reference in this document to out of ISM band spurious emissions; the equipment manufacturer is responsible for compliance in the intended country of use.

3.2.2.1 In-band Spurious Emission

Within the ISM band the power spectral density of the transmitter shall comply with the following requirements when sending pseudo random data. All power measurements shall use a 100 kHz bandwidth with maximum hold. The power measurements between 1 MHz and 1.5 MHz from the carrier shall be at least 26 dB below the maximum power measurement up to 500 kHz from the carrier. The adjacent channel power for channels at least 2 MHz from the carrier is defined as the sum of the power measurements over a 1 MHz channel and shall not exceed -20 dBm for the second adjacent channels and -40 dBm for the third and subsequent adjacent channels. These requirements shall apply to

the transmitted signal from the start of the guard time to the end of the power down ramp. The spectral mask is illustrated in Figure 3.2.

Exceptions are allowed in up to 3 bands of 1 MHz width centered on a frequency which is an integer multiple of 1 MHz. They shall comply with an absolute value of –20 dBm.

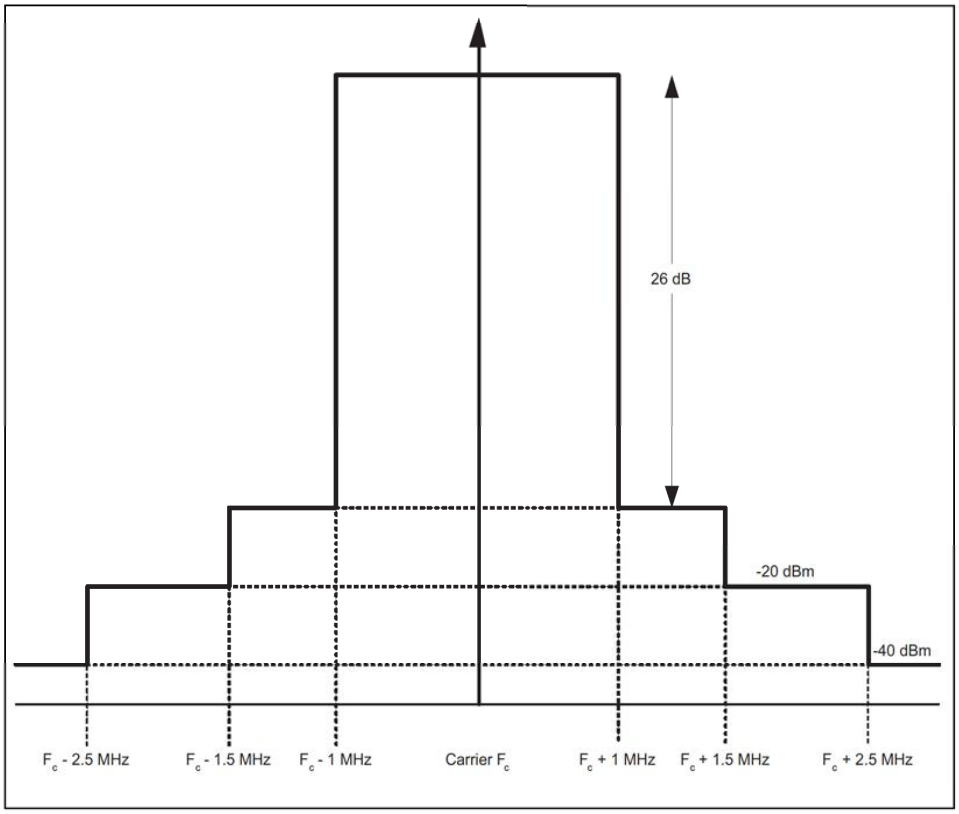


Figure 3.2: Transmitter spectrum mask

3.2.3 Radio Frequency Tolerance

The same carrier frequencies F_c as used for Basic Rate transmissions shall be used for the Enhanced Data Rate transmissions. The transmitted initial center frequency accuracy shall be within ±75 kHz from F_c. The maximum excursion from F_c (frequency offset plus drift) shall not exceed ±75 kHz.

The initial frequency accuracy is defined as being the frequency accuracy before any information is transmitted.

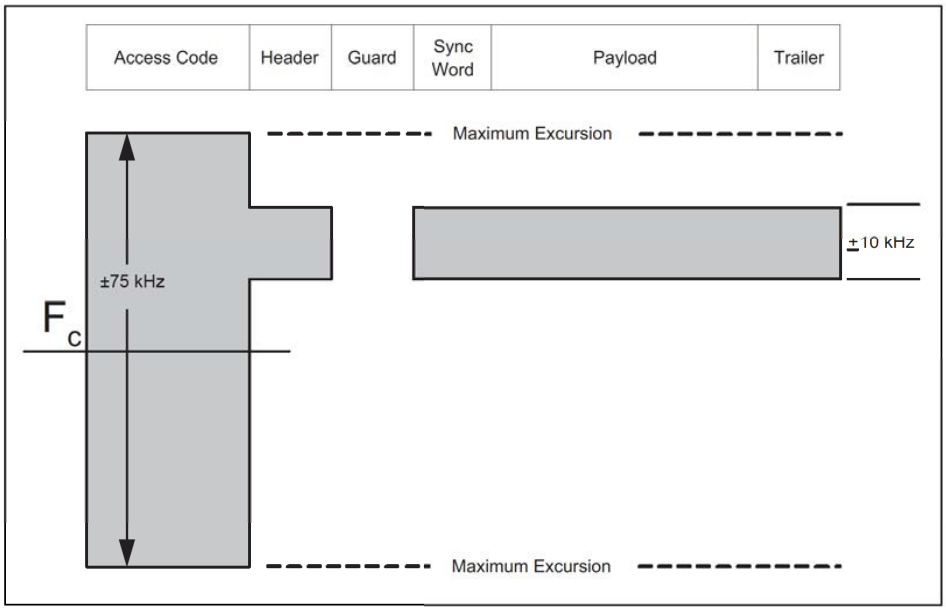


Figure 3.3: Carrier frequency mask

The requirements on accuracy and stability are illustrated by Figure 3.3 for the Enhanced Data Rate packet format defined in 55. The higher frequency accuracy requirement shall start at the first symbol of the header. The maximum drift over the header, synchronization sequence and payload shall be ±10 kHz.

3.2.4 Relative Transmit Power

The requirement on the relative power of the GFSK and PSK portions of the Enhanced Data Rate packet is defined as follows. The average power level during the transmission of access code and header is denoted as P_{GFSK} and the average power level during the transmission of the synchronization sequence and the payload is denoted as P_{DFSK}.The following inequalities shall be satisfied independently for every Enhanced Data Rate packet transmitted:

$(P_{GFSK} - 4\ dB) < P_{DPSK} < (P_{GFSK} + 1\ dB)$

4 RECEIVER CHARACTERISTICS

The receiver characteristics shall be measured using loopback as defined in Section 1, "Test Methodology," on page 231.

The reference sensitivity level referred to in this chapter is -70 dBm.

4.1 BASIC RATE

4.1.1 Actual Sensitivity Level

The actual sensitivity level is defined as the input level for which a raw bit error rate (BER) of 0.1% is met. The receiver sensitivity shall be below or equal to –70 dBm with any Bluetooth transmitter compliant to the transmitter specification specified in Section 3 on page 31.

4.1.2 Interference Performance

The interference performance on Co-channel and adjacent 1 MHz and 2 MHz shall be measured with the wanted signal 10 dB over the reference sensitivity level. For interference performance on all other RF channels the wanted signal shall be 3 dB over the reference sensitivity level. If the frequency of an interfering signal is outside of the band 2400-2483.5 MHz, the out-of-band blocking specification (see Section 4.1.3 on page 42) shall apply. The interfering signal shall be Bluetooth-modulated (see Section 4.1.7 on page 43). The BER shall be ≤0.1% for all the signal-to-interference ratios listed in Table 4.1:

Frequency of Interference	Ratio
Co-Channel interference, $C/I_{co\text{-}channel}$	11 dB
Adjacent (1 MHz) interference, C/I_{1MHz}	0 dB
Adjacent (2 MHz) interference, C/I_{2MHz}	-30 dB
Adjacent (≥3 MHz) interference, $C/I_{\geq 3MHz}$	-40 dB
Image frequency Interference[1] [2], C/I_{Image}	-9 dB
Adjacent (1 MHz) interference to in-band image frequency, $C/I_{Image\pm 1MHz}$	-20 dB

Table 4.1: Interference performance

1. In-band image frequency
2. If the image frequency ≠ n*1 MHz, then the image reference frequency is defined as the closest n*1 MHz frequency.

   If two adjacent channel specifications from Table 4.1 are applicable to the same channel, the more relaxed specification applies.

These specifications are only to be tested at nominal temperature conditions with a device receiving on one RF channel and transmitting on a second RF channel;

this means that the synthesizer may change RF channels between reception and transmission, but always returns to the same receive RF channel.

RF channels where the requirements are not met are called spurious response RF channels. Five spurious response RF channels are allowed at RF channels with a distance of ≥2 MHz from the wanted signal. On these spurious response RF channels a relaxed interference requirement C/I = -17 dB shall be met.

4.1.3 Out-of-Band Blocking

The out-of-band suppression (or rejection) shall be measured with the wanted signal 3 dB over the reference sensitivity level. The interfering signal shall be a continuous wave signal. The BER shall be ≤ 0.1%. The out-of-band blocking shall fulfil the following requirements:

Interfering Signal Frequency	Interfering Signal Power Level
30 MHz - 2000 MHz	-10 dBm
2000 - 2399 MHz	-27 dBm
2484 – 3000 MHz	-27 dBm
3000 MHz – 12.75 GHz	-10 dBm

Table 4.2: Out-of-band suppression (or rejection) requirements.

24 exceptions are permitted which are dependent upon the given RF channel and are centered at a frequency which is an integer multiple of 1 MHz. For at least 19 of these spurious response frequencies, a reduced interference level of at least -50dBm is allowed in order to achieve the required BER=0.1% performance, whereas for a maximum of 5 of the spurious frequencies the interference level may be assumed arbitrarily lower.

4.1.4 Intermodulation Characteristics

The reference sensitivity performance, BER = 0.1%, shall be met under the following conditions:

- The wanted signal shall be at frequency f_0 with a power level 6 dB over the reference sensitivity level.
- A static sine wave signal shall be at a frequency f_1 with a power level of –39 dBm.
- A Bluetooth modulated signal (see Section 4.1.7 on page 43) shall be at f_2 with a power level of -39 dBm.

Frequencies f0, f1 and f2 shall be chosen such that $f_0=2f_1-f_2$ and $|f_2-f_1|=n*1$ MHz, where n can be 3, 4, or 5. The system shall fulfill at least one of the three alternatives (n=3, 4, or 5).

4.1.5 Maximum Usable Level

The maximum usable input level that the receiver operates at shall be greater than -20 dBm. The BER shall be less than or equal to 0.1% at –20 dBm input power.

4.1.6 Receiver Signal Strength Indicator

If a device supports Receive Signal Strength Indicator (RSSI) the accuracy shall be +/- 6 dBm.

4.1.7 Reference Signal Definition

A Bluetooth modulated interfering signal shall be defined as:

Modulation = GFSK

Modulation index = 0.32±1%

BT= 0.5±1%

Bit Rate = 1 Mbps ±1 ppm

Modulating Data for wanted signal = PRBS9

Modulating Data for interfering signal = PRBS 15

Frequency accuracy better than ±1 ppm.

4.2 ENHANCED DATA RATE

4.2.1 Actual Sensitivity Level

The actual sensitivity level shall be defined as the input level for which a raw bit error rate (BER) of 0.01% is met. The requirement for a Bluetooth π/4-DQPSK and 8DPSK Enhanced Data Rate receiver shall be an actual sensitivity level of –70 dBm or better. The receiver shall achieve the –70 dBm sensitivity level with any Bluetooth transmitter compliant to the Enhanced Data Rate transmitter specification as defined in Section 3.2.

4.2.2 BER Floor Performance

The receiver shall achieve a BER less than 0.001% at 10 dB above the reference sensitivity level.

4.2.3 Interference Performance

The interference performance for co-channel and adjacent 1 MHz and 2 MHz channels shall be measured with the wanted signal 10 dB above the reference sensitivity level. On all other frequencies the wanted signal shall be 3 dB above the reference sensitivity level. The requirements in this section shall only apply if the frequency of the interferer is inside of the band 2400-2483.5 MHz.

The interfering signal for co-channel interference shall be similarly modulated as the desired signal. The interfering signal for other channels shall be equivalent to a nominal Bluetooth Basic Rate GFSK transmitter. The interfering signal shall carry random data.

A BER of 0.1% or better shall be achieved for the signal to interference ratios defined in Table 4.3.

Frequency of Interference	π/4-DQPSK Ratio	8DPSK Ratio
Co-Channel interference, $C/I_{co\text{-}channel}$	13 dB	21 dB
Adjacent (1 MHz) interference[1], C/I_{1MHz}	0 dB	5 dB
Adjacent (2MHz) interference[1], C/I_{2MHz}	-30 dB	-25 dB
Adjacent (≥3MHz) interference[1]	-40 dB	-33 dB
Image frequency interference[1,2,3], C/I_{Image}	-7 dB	0 dB
Adjacent (1 MHz) interference to in-band image frequency[1,2,3], $C/I_{Image \pm 1MHz}$	-20 dB	-13 dB

Table 4.3: Interference Performance

1. If two adjacent channel specifications from Table 4.3 are applicable to the same channel, the more relaxed specification applies.
2. In-band image frequency.
3. If the image frequency is not equal to n*1 MHz, then the image reference frequency is defined as the closest n*1 MHz frequency.

These specifications are only to be tested at nominal temperature conditions with a receiver hopping on one frequency; this means that the synthesizer may change frequency between receive slot and transmit slot, but always returns to the same receive frequency.

Frequencies where the requirements are not met are called spurious response frequencies. Five spurious response frequencies are allowed at frequencies with a distance of ≥2 MHz from the wanted signal. On these spurious response frequencies a relaxed interference requirement C/I = -15 dB for π/4-DQPSK and C/I = -10 dB for 8DPSK shall be met.

4.2.4 Maximum Usable Level

The maximum usable input level that the receiver operates at shall be greater than -20 dBm. The BER shall be less than or equal to 0.1% at -20 dBm input power.

4.2.5 Out-of-Band and Intermodulation Characteristics

Note: The Basic Rate out-of-band blocking and intermodulation requirements ensure adequate Enhanced Data Rate performance, and therefore there are no specific requirements for Enhanced Data Rate.

4.2.6 Reference Signal Definition

A 2 Mbps Bluetooth signal used as "wanted" or "interfering signal" is defined as:

Modulation = π/4-DQPSK
Symbol Rate = 1 Msym/s ± 1 ppm
Frequency accuracy better than ±1 ppm
Modulating Data for wanted signal = PRBS9
Modulating Data for interfering signal = PRBS15
RMS Differential Error Vector Magnitude < 5%
Average power over the GFSK and DPSK portions of the packet shall be equal to within +/- 1 dB

A 3 Mbps Bluetooth signal used as "wanted" or "interfering signal" is defined as:

Modulation = 8DPSK
Symbol Rate = 1 Msym/s ± 1 ppm
Frequency accuracy better than ±1 ppm
Modulating Data for wanted signal = PRBS9
Modulating Data for interfering signal = PRBS15
RMS Differential Error Vector Magnitude < 5%
Average power over the GFSK and DPSK portions of the packet shall be equal to within +/- 1 dB

5 APPENDIX A

5.1 NOMINAL TEST CONDITIONS

5.1.1 Nominal temperature

The nominal temperature conditions for tests shall be +15 to +35 ^{o}C. When it is impractical to carry out the test under this condition a note to this effect, stating the ambient temperature, shall be recorded. The actual value during the test shall be recorded in the test report.

5.1.2 Nominal power source

5.1.2.1 Mains voltage

The nominal test voltage for equipment to be connected to the mains shall be the nominal mains voltage. The nominal voltage shall be the declared voltage or any of the declared voltages for which the equipment was designed. The frequency of the test power source corresponding to the AC mains shall be within 2% of the nominal frequency.

5.1.2.2 Lead-acid battery power sources used in vehicles

When radio equipment is intended for operation from the alternator-fed lead-acid battery power sources which are standard in vehicles, then the nominal test voltage shall be 1.1 times the nominal voltage of the battery (6V, 12V, etc.).

5.1.2.3 Other power sources

For operation from other power sources or types of battery (primary or secondary), the nominal test voltage shall be as declared by the equipment manufacturer. This shall be recorded in the test report.

5.2 EXTREME TEST CONDITIONS

5.2.1 Extreme temperatures

The extreme temperature range shall be the largest temperature range given by the combination of:

- The minimum temperature range 0 °C to +35 °C
- The product operating temperature range declared by the manufacturer.

This extreme temperature range and the declared operating temperature range shall be recorded in the test report.

5.2.2 Extreme power source voltages

Tests at extreme power source voltages specified below are not required when the equipment under test is designed for operation as part of and powered by another system or piece of equipment. Where this is the case, the limit values of the host system or host equipment shall apply. The appropriate limit values shall be declared by the manufacturer and recorded in the test report.

5.2.2.1 Mains voltage

The extreme test voltage for equipment to be connected to an AC mains source shall be the nominal mains voltage ±10%.

5.2.2.2 Lead-acid battery power source used on vehicles

When radio equipment is intended for operation from the alternator-fed lead-acid battery power sources which are standard in vehicles, then extreme test voltage shall be 1.3 and 0.9 times the nominal voltage of the battery (6V, 12V etc.)

5.2.2.3 Power sources using other types of batteries

The lower extreme test voltage for equipment with power sources using the following types of battery, shall be

a) for Leclanché, alkaline, or lithium type battery: 0.85 times the nominal voltage of the battery

b) for mercury or nickel-cadmium types of battery: 0.9 times the nominal voltage of the battery.

In both cases, the upper extreme test voltage shall be 1.15 times the nominal voltage of the battery.

5.2.2.4 Other power sources

For equipment using other power sources, or capable of being operated from a variety of power sources (primary or secondary), the extreme test voltages shall be those declared by the manufacturer. These shall be recorded in the test report.

6 APPENDIX B

The Basic Rate radio parameters shall be tested in the following conditions

Parameter	Temperature	Power source
Output Power	ETC	ETC
Power control	NTC	NTC
Modulation index	ETC	ETC
Initial Carrier Frequency accuracy	ETC	ETC
Carrier Frequency drift	ETC	ETC
Conducted in-band spurious emissions	ETC	ETC
Radiated in-band emissions	NTC	NTC
Sensitivity	ETC	ETC
Interference Performance	NTC	NTC
Intermodulation Characteristics	NTC	NTC
Out-of-band blocking	NTC	NTC
Maximum Usable Level	NTC	NTC
Receiver Signal Strength Indicator	NTC	NTC

ETC = Extreme Test Conditions
NTC = Nominal Test Conditions

The Enhanced Data Rate radio parameters shall be tested in the following conditions

Parameter	Temperature	Power source
Modulation accuracy	ETC	ETC
Carrier frequency stability	ETC	ETC
In-band spurious emissions	ETC	ETC
Relative transmit power	ETC	ETC
Sensitivity	ETC	ETC
BER floor sensitivity	NTC	NTC
Interference Performance	NTC	NTC
Maximum usable level	NTC	NTC

ETC = Extreme Test Conditions
NTC = Nominal Test Conditions

7 APPENDIX C

7.1 ENHANCED DATA RATE MODULATION ACCURACY

The Enhanced Data Rate modulation accuracy is defined by the differential error vector, being the difference between the vectors representing consecutive symbols of the transmitted signal, after passing the signal through a specified measurement filter, sampling it at the symbol rate with an optimum sampling phase and compensating it for carrier frequency error and for the ideal carrier phase changes. The magnitude of the normalized differential error vector is called the Differential Error Vector Magnitude (DEVM). The objective of the DEVM is to estimate the modulation errors that would be perceived by a differential receiver.

In an ideal transmitter, the input bit sequence $\{b_j\}$ is mapped onto a complex valued symbol sequence $\{S_k\}$. Subsequently, this symbol sequence is transformed into a baseband signal S(t) by means of a pulse-shaping filter.

In an actual transmitter implementation, the bit sequence $\{b_j\}$ generates a baseband equivalent transmitted signal Y(t). This signal Y(t) contains, besides the desired component S(t), multiple distortion components. This is illustrated in Figure 7.1.

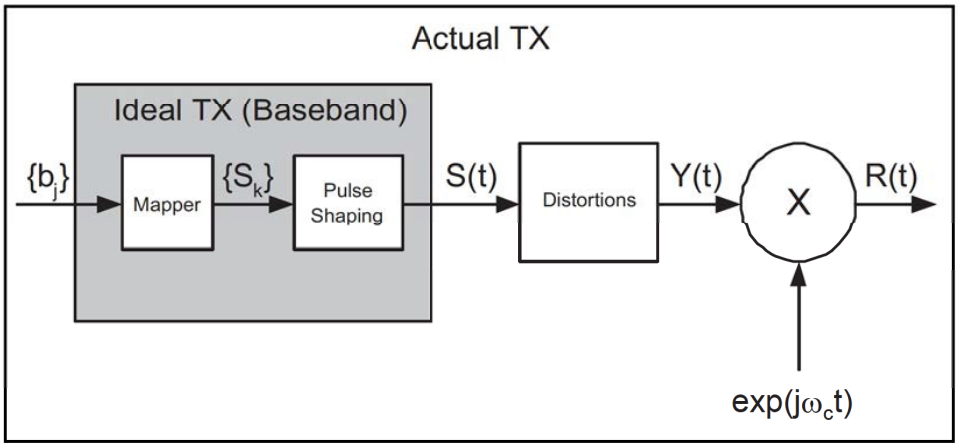


Figure 7.1: TX model.

Let Z(t) be the output of the measurement filter after first compensating the received signal for the initial center frequency error, ω_i, of the received packet, i.e. the output after down conversion and filtering the transmit signal R(t) (see Figure 7.2).The measurement filter is defined by a square-root raised cosine shaping filter with a roll-off factor equal to 0.4 and 3 dB bandwidth of ±500 kHz.

Let $\{Z_k(\varepsilon)\}$ be the sequence of samples obtained by sampling the signal Z(t) with a sampling period equal to the symbol period T and a sampling phase equal to ε such that $Z_k(\varepsilon)=Z((k+\varepsilon)T)$. Note that this sequence $\{Z_k(\varepsilon)\}$ would coincide with the symbol sequence $\{S_k\}$ if no distortion is present and the correct timing phase ε is chosen.

To reflect the behavior of a typical differential receiver, the sample sequence $\{Z_k(\varepsilon)\}$ should be compensated for carrier frequency drift. Therefore, the sequence $\{Z_k(\varepsilon)\}$ is multiplied by a factor W^{-k} in which $W = e^{j\omega T}$ accounts for the frequency offset ω. A constant value of ω is used for each DEVM block of N = 50 symbols, but ω may vary between DEVM blocks (note that the values of ω can be used to measure carrier frequency drift.

In addition, $\{Z_k(\varepsilon)\}$ is compensated for the ideal phase changes between symbols by multiplying it with the complex conjugate of the symbol sequence $\{S_k\}$. However, it is not necessary to compensate $\{Z_k(\varepsilon)\}$ for initial carrier phase or output power of the transmitter.

Let $\{Q_k(\varepsilon,\omega)\}$ denote the compensated sequence $\{Z_k(\varepsilon)\}$, where the ideal phase changes have been removed and ε and ω are chosen optimally to minimize the DEVM, (i.e. remove time and frequency uncertainty). For a transmitter with no distortions other than a constant frequency error, $\{Q_k(\varepsilon,\omega)\}$ is a complex constant that depends on the initial carrier phase and the output power of the transmitter.

The differential error sequence $\{E_k(\varepsilon,\omega)\}$ is defined as the difference between $\{Q_k(\varepsilon,\omega)\}$ and $\{Q_{k-1}(\varepsilon,\omega)\}$. This reflects the modulation errors that would be perceived by a differential receiver. For a transmitter with no distortions other than a constant frequency error, $\{E_k(\varepsilon,\omega)\}$ is zero.

The definitions of the DEVM measures are based upon this differential error sequence $\{E_k(\varepsilon,\omega)\}$. The generation of the error sequence is depicted in Figure 7.2.

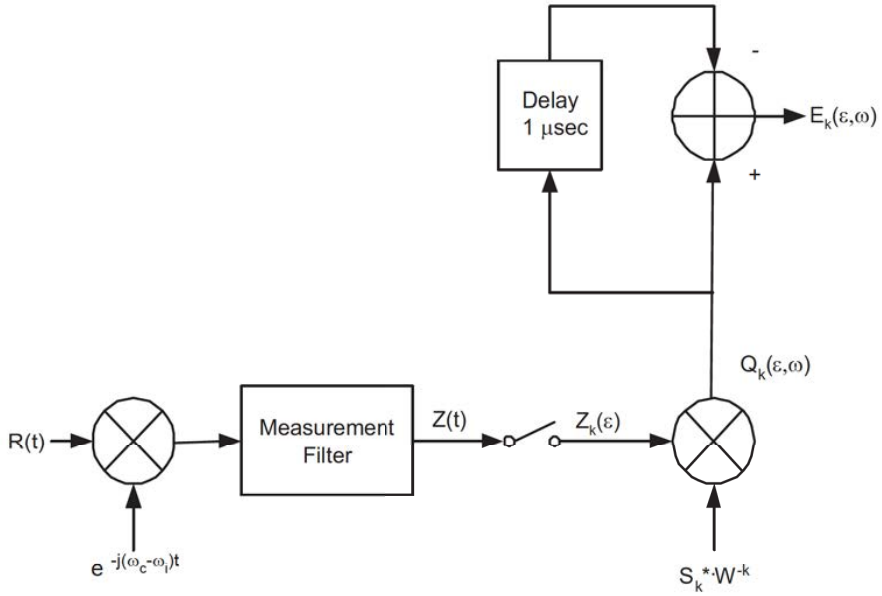


Figure 7.2: Error sequence generation.

RMS DEVM

The root mean squared DEVM (RMS DEVM) computed over N = 50 symbols is defined as:

$$RMS\ DEVM = \min_{\varepsilon,\omega} \left\{ \sqrt{ \sum_{k=1}^{N} \left| E_k(\varepsilon,\omega) \right|^2 \Big/ \sum_{k=1}^{N} \left| Q_k(\varepsilon,\omega) \right|^2 } \right\}$$

As can be seen from the expression above, the RMS DEVM is the square-root of the normalized power of the error.

Peak DEVM

The DEVM at symbol k is defined as

$$DEVM(k) = \sqrt{\frac{\left|E_k(\varepsilon_0, \omega_0)\right|^2}{\sum_{j=1}^{N}\left|Q_j(\varepsilon_0, \omega_0)\right|^2 / N}} \quad \text{(EQ 6)}$$

where ε_0 and ω_0 are the values for ε and ω used to calculate the RMS DEVM.

The peak DEVM is defined as:

$$Peak\ DEVM = \max_{k}\{\text{DEVM (k)}\} \quad \text{(EQ 7)}$$



BASEBAND SPECIFICATION

This document describes the specification of the Bluetooth link controller which carries out the baseband protocols and other low-level link routines.

CONTENTS

1 General Description 63
1.1 Bluetooth Clock 64
1.2 Bluetooth Device Addressing 66
1.2.1 Reserved addresses 66
1.3 Access Codes 67
2 Physical Channels 69
2.1 Physical Channel Definition 70
2.2 Basic Piconet Physical Channel 70
2.2.1 Master-slave definition 70
2.2.2 Hopping characteristics 71
2.2.3 Time slots 71
2.2.4 Piconet clocks 72
2.2.5 Transmit/receive timing 72
2.2.5.1 Piconet physical channel timing 73
2.2.5.2 Piconet physical channel re-synchronization 74
2.3 Adapted Piconet Physical Channel 75
2.3.1 Hopping characteristics 75
2.4 Page Scan Physical Channel 76
2.4.1 Clock estimate for paging 76
2.4.2 Hopping characteristics 76
2.4.3 Paging procedure timing 77
2.4.4 Page response timing 78
2.5 Inquiry Scan Physical Channel 80
2.5.1 Clock for inquiry 80
2.5.2 Hopping characteristics 80
2.5.3 Inquiry procedure timing 80
2.5.4 Inquiry response timing 80
2.6 Hop Selection 82
2.6.1 General selection scheme 82
2.6.2 Selection kernel 86
2.6.2.1 First addition operation 86
2.6.2.2 XOR operation 87
2.6.2.3 Permutation operation 87
2.6.2.4 Second addition operation 88
2.6.2.5 Register bank 88
2.6.3 Adapted hop selection kernel 89
2.6.3.1 Channel re-mapping function 89
2.6.4 Control word 90

2.6.4.1 Page scan and inquiry scan hopping sequences 91
2.6.4.2 Page hopping sequence 92
2.6.4.3 Slave page response hopping sequence 92
2.6.4.4 Master page response hopping sequence 93
2.6.4.5 Inquiry hopping sequence 93
2.6.4.6 Inquiry response hopping sequence 94
2.6.4.7 Basic and adapted channel hopping sequence 94

3 Physical Links 95
3.1 Link Supervision 95

4 Logical Transports 97
4.1 General 97
4.2 Logical Transport Address (LT_ADDR) 97
4.3 Synchronous Logical Transports 98
4.4 Asynchronous Logical Transport 98
4.5 Transmit/Receive Routines 99
4.5.1 TX Routine 99
4.5.1.1 ACL traffic 100
4.5.1.2 SCO traffic 101
4.5.1.3 Mixed data/voice traffic 101
4.5.1.4 eSCO Traffic 102
4.5.1.5 Default packet types 102
4.5.2 RX routine 102
4.5.3 Flow control 103
4.5.3.1 Destination control 104
4.5.3.2 Source control 104
4.6 Active Slave Broadcast Transport 104
4.7 Parked Slave Broadcast Transport 105
4.7.1 Parked member address (PM_ADDR) 105
4.7.2 Access request address (AR_ADDR) 105

5 Logical Links 107
5.1 Link Control Logical Link (LC) 107
5.2 ACL Control Logical Link (ACL-C) 107
5.3 User Asynchronous/Isochronous Logical Link (ACL-U) 107
5.3.1 Pausing the ACL-U logical link 108
5.4 User Synchronous Data Logical Link (SCO-S) 108
5.5 User Extended Synchronous Data Logical Link (eSCO-S) 108
5.6 Logical Link Priorities 108

6 Packets 109
6.1 General Format 109
6.1.1 Basic Rate 109

6.1.2 Enhanced Data Rate 109
6.2 Bit Ordering 110
6.3 Access Code 111
6.3.1 Access code types 111
6.3.2 Preamble 112
6.3.3 Sync word 112
6.3.3.1 Synchronization word definition 112
6.3.3.2 Pseudo-random noise sequence generation 115
6.3.4 Trailer 115
6.4 Packet Header 116
6.4.1 LT_ADDR 116
6.4.2 TYPE 116
6.4.3 FLOW 117
6.4.4 ARQN 117
6.4.5 SEQN 117
6.4.6 HEC 117
6.5 Packet Types 118
6.5.1 Common packet types 119
6.5.1.1 ID packet 119
6.5.1.2 NULL packet 120
6.5.1.3 POLL packet 120
6.5.1.4 FHS packet 120
6.5.1.5 DM1 packet 122
6.5.2 SCO packets 123
6.5.2.1 HV1 packet 123
6.5.2.2 HV2 packet 123
6.5.2.3 HV3 packet 123
6.5.2.4 DV packet 123
6.5.3 eSCO packets 124
6.5.3.1 EV3 packet 124
6.5.3.2 EV4 packet 124
6.5.3.3 EV5 packet 124
6.5.3.4 2-EV3 packet 124
6.5.3.5 2-EV5 packet 125
6.5.3.6 3-EV3 packet 125
6.5.3.7 3-EV5 packet 125
6.5.4 ACL packets 126
6.5.4.1 DM1 packet 126
6.5.4.2 DH1 packet 126
6.5.4.3 DM3 packet 126
6.5.4.4 DH3 packet 126
6.5.4.5 DM5 packet 126
6.5.4.6 DH5 packet 127

6.5.4.7 AUX1 packet 127
6.5.4.8 2-DH1 packet 127
6.5.4.9 2-DH3 packet 127
6.5.4.10 2-DH5 packet 127
6.5.4.11 3-DH1 packet 127
6.5.4.12 3-DH3 packet 128
6.5.4.13 3-DH5 packet 128
6.6 Payload Format 128
6.6.1 Synchronous data field 128
6.6.2 Asynchronous data field 130
6.7 Packet Summary 134
7 Bitstream Processing 137
7.1 Error Checking 138
7.1.1 HEC generation 138
7.1.2 CRC generation 139
7.2 Data Whitening 141
7.3 Error Correction 142
7.4 FEC Code: Rate 1/3 142
7.5 FEC Code: Rate 2/3 143
7.6 ARQ Scheme 144
7.6.1 Unnumbered ARQ 144
7.6.2 Retransmit filtering 147
7.6.2.1 Initialization of SEQN at start of new connection 148
7.6.2.2 ACL and SCO retransmit filtering 148
7.6.2.3 eSCO retransmit filtering 149
7.6.2.4 FHS retransmit filtering 149
7.6.2.5 Packets without CRC retransmit filtering 149
7.6.3 Flushing payloads 150
7.6.4 Multi-slave considerations 150
7.6.5 Broadcast packets 150
8 Link Controller Operation 153
8.1 Overview of States 153
8.2 Standby State 154
8.3 Connection Establishment Substates 154
8.3.1 Page scan substate 154
8.3.2 Page substate 156
8.3.3 Page response substates 159
8.3.3.1 Slave response substate 160
8.3.3.2 Master response substate 162
8.4 Device Discovery Substates 163
8.4.1 Inquiry scan substate 164

8.4.2 Inquiry substate 165
8.4.3 Inquiry response substate 166
8.5 Connection State 167
8.6 Active Mode 168
8.6.1 Polling in the active mode 169
8.6.2 SCO 169
8.6.3 eSCO 171
8.6.4 Broadcast scheme 173
8.6.5 Role switch 175
8.6.6 Scatternet 177
8.6.6.1 Inter-piconet communications 177
8.6.7 Hop sequence switching 178
8.6.8 Channel classification and channel map selection 181
8.6.9 Power Management 182
8.6.9.1 Packet handling 182
8.6.9.2 Slot occupancy 182
8.6.9.3 Recommendations for low-power operation 182
8.6.9.4 Enhanced Data Rate 183
8.7 sniff Mode 183
8.7.1 Sniff Transition Mode 184
8.8 Hold Mode 185
8.9 Park State 185
8.9.1 Beacon train 186
8.9.2 Beacon access window 189
8.9.3 Parked slave synchronization 190
8.9.4 Parking 191
8.9.5 Master-initiated unparking 192
8.9.6 Slave-initiated unparking 192
8.9.7 Broadcast scan window 193
8.9.8 Polling in the park state 193

9 Audio 195
9.1 LOG PCM CODEC 195
9.2 CVSD CODEC 195
9.3 Error Handling 198
9.4 General Audio Requirements 198
9.4.1 Signal levels 198
9.4.2 CVSD audio quality 198

10 List of Figures 199

11 List of Tables 203

12 Appendix.....203

1 GENERAL DESCRIPTION

This part specifies the normal operation of a Bluetooth baseband.

The Bluetooth system provides a point-to-point connection or a point-to-multi-point connection, see (a) and (b) in Figure 1.1 on page 63. In a point-to-point connection the physical channel is shared between two Bluetooth devices. In a point-to-multipoint connection, the physical channel is shared among several Bluetooth devices. Two or more devices sharing the same physical channel form a *piconet*. One Bluetooth device acts as the master of the piconet, whereas the other device(s) act as slave(s). Up to seven slaves can be active in the piconet. Additionally, many more slaves can remain connected in a parked state. These parked slaves are not active on the channel, but remain synchronized to the master and can become active without using the connection establishment procedure. Both for active and parked slaves, the channel access is controlled by the master.

Piconets that have common devices are called a *scatternet*, see (c) in Figure 1.1 on page 63. Each piconet only has a single master, however, slaves can participate in different piconets on a time-division multiplex basis. In addition, a master in one piconet can be a slave in other piconets. Piconets shall not be frequency synchronized and each piconet has its own hopping sequence.

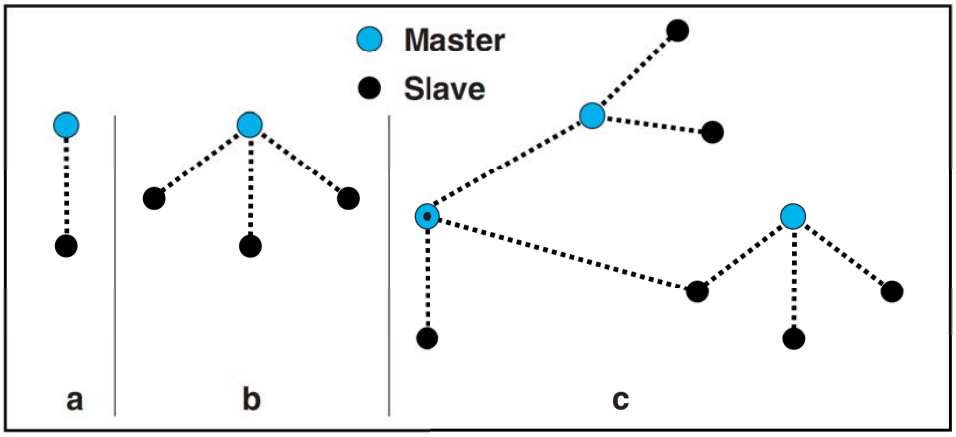


Figure 1.1: Piconets with a single slave operation (a), a multi-slave operation (b) and a scatternet operation (c).

Data is transmitted over the air in packets. Two modulation modes are defined: a mandatory mode called Basic Rate and an optional mode called Enhanced Data Rate. The symbol rate for all modulation schemes is 1 Ms/s. The gross air data rate is 1 Mbps for Basic Rate. Enhanced Data Rate has a primary modulation mode that provides a gross air data rate of 2 Mbps, and a secondary modulation mode that provides a gross air data rate of 3 Mbps.

The general Basic Rate packet format is shown in Figure 1.2. Each packet consists of 3 entities: the access code, the header, and the payload.

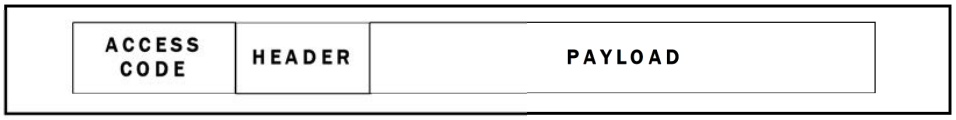


Figure 1.2: Standard Basic Rate packet format.

The general Enhanced Data Rate packet format is shown in Standard Enhanced Data Rate packet format. Each packet consists of 6 entities: the access code, the header, the guard period, the synchronization sequence, the Enhanced Data Rate payload and the trailer. The access code and header use the same modulation scheme as for Basic Rate packets while the synchronization sequence, the Enhanced Data Rate payload and the trailer use the Enhanced Data Rate modulation scheme. The guard time allows for the transition between the modulation schemes.

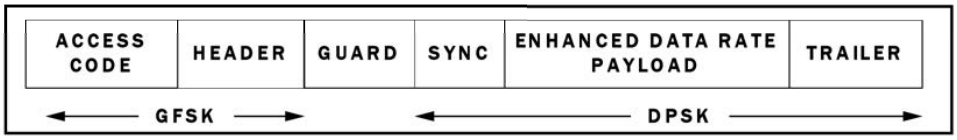


Figure 1.3: Standard Enhanced Data Rate packet format

1.1 BLUETOOTH CLOCK

Every Bluetooth device shall have a native clock that shall be derived from a free running system clock. For synchronization with other devices, offsets are used that, when added to the native clock, provide temporary Bluetooth clocks that are mutually synchronized. It should be noted that the Bluetooth clock has no relation to the time of day; it may therefore be initialized to any value. The clock has a cycle of about a day. If the clock is implemented with a counter, a 28-bit counter is required that shall wrap around at 2^{28}-1. The least significant bit (LSB) shall tick in units of 312.5 μs (i.e. half a time slot), giving a clock rate of 3.2 kHz.

The clock determines critical periods and triggers the events in the device. Four periods are important in the Bluetooth system: 312.5 μs, 625 μs, 1.25 ms, and 1.28 s; these periods correspond to the timer bits CLK_0, CLK_1, CLK_2, and CLK_{12}, respectively, see Figure 1.4 on page 65.

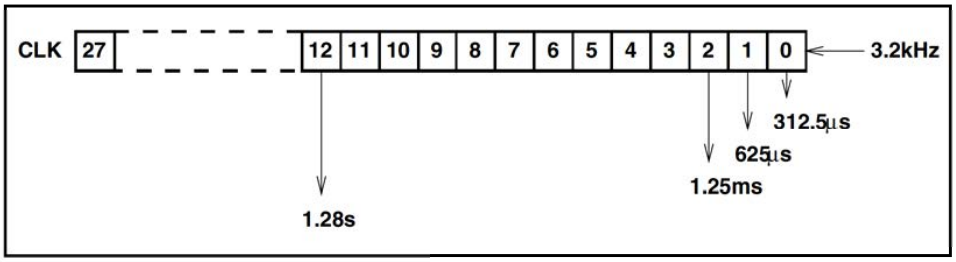


Figure 1.4: Bluetooth clock.

In the different modes and states a device can reside in, the clock has different appearances:

- CLKN native clock
- CLKE estimated clock
- CLK master clock

CLKN is the native clock and shall be the reference to all other clock appearances. In STANDBY and in Park, Hold and Sniff mode the native clock may be driven by a low power oscillator (LPO) with worst case accuracy (+/-250ppm). Otherwise, the native clock shall be driven by the reference crystal oscillator with worst case accuracy of +/-20ppm.

See Section 2.2.4 on page 72 for the definition of CLK and Section 2.4.1 on page 76 for the definition of CLKE.

The master shall never adjust its native clock during the existence of the piconet.

1.2 BLUETOOTH DEVICE ADDRESSING

Each Bluetooth device shall be allocated a unique 48-bit Bluetooth device address (BD_ADDR). This address shall be obtained from the IEEE Registration Authority. The address is divided into the following three fields:

- LAP field: lower address part consisting of 24 bits
- UAP field: upper address part consisting of 8 bits
- NAP field: non-significant address part consisting of 16 bits

The LAP and UAP form the significant part of the BD_ADDR. The bit pattern in Figure 1.5 is an example BD_ADDR.

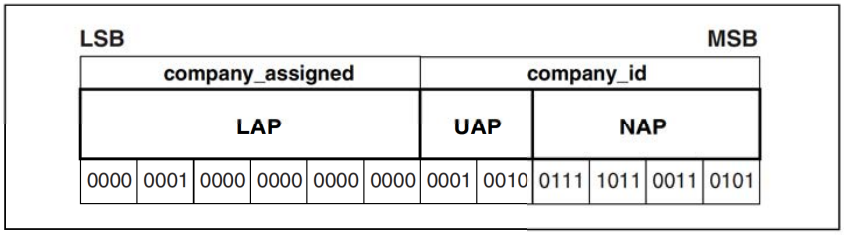


Figure 1.5: Format of BD_ADDR.

The BD_ADDR may take any values except the 64 reserved LAP values for general and dedicated inquiries (see Section 1.2.1 on page 66).

1.2.1 Reserved addresses

A block of 64 contiguous LAPs is reserved for inquiry operations; one LAP common to all devices is reserved for general inquiry, the remaining 63 LAPs are reserved for dedicated inquiry of specific classes of devices (see Assigned Numbers on the web site[1]). The same LAP values are used regardless of the contents of UAP and NAP. Consequently, none of these LAPs can be part of a user BD_ADDR.

The reserved LAP addresses are 0x9E8B00-0x9E8B3F. The general inquiry LAP is 0x9E8B33. All addresses have the LSB at the rightmost position, hexadecimal notation. The default check initialization (DCI) is used as the UAP whenever one of the reserved LAP addresses is used. The DCI is defined to be 0x00 (hexadecimal).

1. https://www.bluetooth.org/foundry/assignnumb/document/assigned_numbers

1.3 ACCESS CODES

In the Bluetooth system all transmissions over the physical channel begin with an access code. Three different access codes are defined, see also Section 6.3.1 on page 111:

- device access code (DAC)
- channel access code (CAC)
- inquiry access code (IAC)

All access codes are derived from the LAP of a device address or an inquiry address. The device access code is used during **page**, **page scan** and **page response** substates and shall be derived from the paged device's BD_ADDR. The channel access code is used in the **CONNECTION** state and forms the beginning of all packets exchanged on the piconet physical channel. The channel access code shall be derived from the LAP of the master's BD_ADDR. Finally, the inquiry access code shall be used in the **inquiry** substate. There is one general IAC (GIAC) for general inquiry operations and there are 63 dedicated IACs (DIACs) for dedicated inquiry operations.

The access code also indicates to the receiver the arrival of a packet. It is used for timing synchronization and offset compensation. The receiver correlates against the entire synchronization word in the access code, providing very robust signalling.

2 PHYSICAL CHANNELS

The lowest architectural layer in the Bluetooth system is the physical channel. A number of types of physical channels are defined. All Bluetooth physical channels are characterized by the combination of a pseudo-random frequency hopping sequence, the specific slot timing of the transmissions, the access code and packet header encoding. These aspects, together with the range of the transmitters, define the signature of the physical channel. For the basic and adapted piconet physical channels frequency hopping is used to change frequency periodically to reduce the effects of interference and to satisfy local regulatory requirements.

Two devices that wish to communicate use a shared physical channel for this communication. To achieve this, their transceivers must be tuned to the same RF frequency at the same time, and they must be within a nominal range of each other.

Given that the number of RF carriers is limited and that many Bluetooth devices may be operating independently within the same spatial and temporal area there is a strong likelihood of two independent Bluetooth devices having their transceivers tuned to the same RF carrier, resulting in a physical channel collision. To mitigate the unwanted effects of this collision each transmission on a physical channel starts with an access code that is used as a correlation code by devices tuned to the physical channel. This channel access code is a property of the physical channel. The access code is always present at the start of every transmitted packet.

Four Bluetooth physical channels are defined. Each is optimized and used for a different purpose. Two of these physical channels (the basic piconet channel and adapted piconet channel) are used for communication between connected devices and are associated with a specific piconet. The remaining physical channels are used for discovering (the inquiry scan channel) and connecting (the page scan channel) Bluetooth devices.

A Bluetooth device can only use one of these physical channels at any given time. In order to support multiple concurrent operations the device uses time-division multiplexing between the channels. In this way a Bluetooth device can appear to operate simultaneously in several piconets, as well as being discoverable and connectable.

Whenever a Bluetooth device is synchronized to the timing, frequency and access code of a physical channel it is said to be 'connected' to this channel (whether or not it is actively involved in communications over the channel.) At a minimum, a device need only be capable of connection to one physical channel at a time, however, advanced devices may be capable of connecting simultaneously to more than one physical channel, but the specification does not assume that this is possible.

2.1 PHYSICAL CHANNEL DEFINITION

Physical channels are defined by a pseudo-random RF channel hopping sequence, the packet (slot) timing and an access code. The hopping sequence is determined by the UAP and LAP of a Bluetooth device address and the selected hopping sequence. The phase in the hopping sequence is determined by the Bluetooth clock. All physical channels are subdivided into time slots whose length is different depending on the physical channel. Within the physical channel, each reception or transmission event is associated with a time slot or time slots. For each reception or transmission event an RF channel is selected by the hop selection kernel (see Section 2.6 on page 82).The maximum hop rate is 1600 hops/s in the **CONNECTION** state and the maximum is 3200 hops/s in the **inquiry** and **page** substates.

The following physical channels are defined:

- basic piconet physical channel
- adapted piconet physical channel
- page scan physical channel
- inquiry scan physical channel

2.2 BASIC PICONET PHYSICAL CHANNEL

During the **CONNECTION** state the basic piconet physical channel is used by default. The adapted piconet physical channel may also be used. The adapted piconet physical channel is identical to the basic piconet physical channel except for the differences listed in Section 2.3 on page 75.

2.2.1 Master-slave definition

The basic piconet physical channel is defined by the master of the piconet. The master controls the traffic on the piconet physical channel by a polling scheme. (see Section 8.5 on page 167)

By definition, the device that initiates a connection by paging is the master. Once a piconet has been established, master-slave roles may be exchanged. This is described in Section 8.6.5 on page 175.

2.2.2 Hopping characteristics

The basic piconet physical channel is characterized by a pseudo-random hopping through all 79 RF channels. The frequency hopping in the piconet physical channel is determined by the Bluetooth clock and BD_ADDR of the master. When the piconet is established, the master clock is communicated to the slaves. Each slave shall add an offset to its native clock to synchronize with the master clock. Since the clocks are independent, the offsets must be updated regularly. All devices participating in the piconet are time-synchronized and hop-synchronized to the channel.

The basic piconet physical channel uses the basic channel hopping sequence and is described in Section 2.6 on page 82.

2.2.3 Time slots

The basic piconet physical channel is divided into time slots, each 625 μs in length. The time slots are numbered according to the most significant 27 bits of the Bluetooth clock CLK_{28-1} of the piconet master. The slot numbering ranges from 0 to 2^{27}-1 and is cyclic with a cycle length of 2^{27}. The time slot number is denoted as k.

A TDD scheme is used where master and slave alternatively transmit, see Figure 2.1 on page 71. The packet start shall be aligned with the slot start. Packets may extend over up to five time slots.

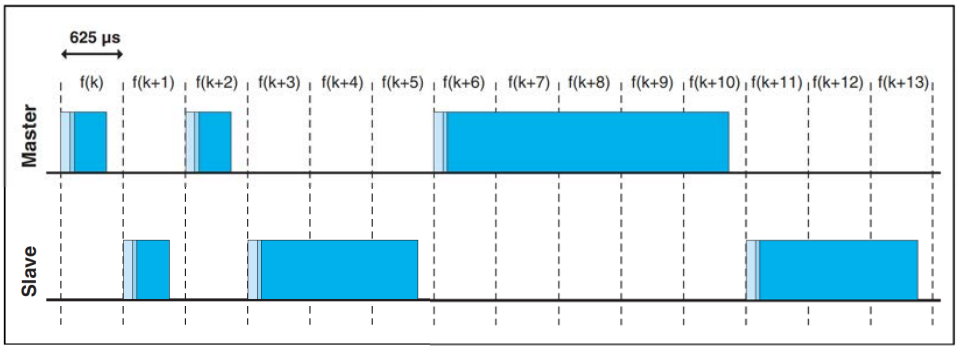


Figure 2.1: Multi-slot packets

The term *slot pairs* is used to indicate two adjacent time slots starting with a master-to-slave transmission slot.

2.2.4 Piconet clocks

CLK is the master clock of the piconet. It shall be used for all timing and scheduling activities in the piconet. All devices shall use the CLK to schedule their transmission and reception. The CLK shall be derived from the native clock CLKN (see Section 1.1 on page 64) by adding an offset, see Figure 2.2 on page 72. The offset shall be zero for the master since CLK is identical to its own native clock CLKN. Each slave shall add an appropriate offset to its CLKN such that the CLK corresponds to the CLKN of the master. Although all CLKNs in the devices run at the same nominal rate, mutual drift causes inaccuracies in CLK. Therefore, the offsets in the slaves must be regularly updated such that CLK is approximately CLKN of the master.

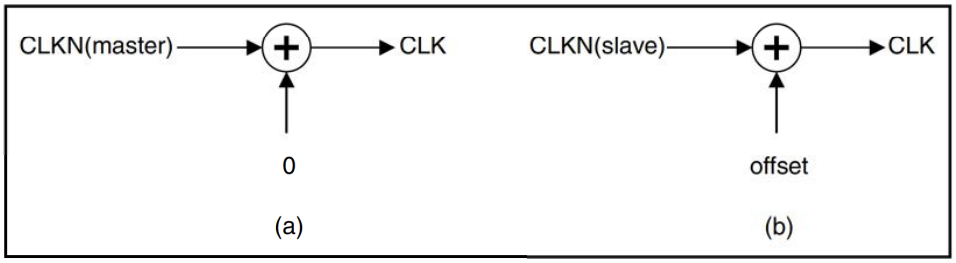


Figure 2.2: Derivation of CLK in master (a) and in slave (b).

2.2.5 Transmit/receive timing

The master transmission shall always start at even numbered time slots (CLK_1=0) and the slave transmission shall always start at odd numbered time slots (CLK_1=1). Due to packet types that cover more than a single slot, master transmission may continue in odd numbered slots and slave transmission may continue in even numbered slots, see Figure 2.1 on page 71.

All timing diagrams shown in this chapter are based on the signals as present at the antenna. The term “exact” when used to describe timing refers to an ideal transmission or reception and neglects timing jitter and clock frequency imperfections.

The average timing of packet transmission shall not drift faster than 20 ppm relative to the ideal slot timing of 625 µs. The instantaneous timing shall not deviate more than 1 µs from the average timing. Thus, the absolute packet transmission timing t_k of slot boundary k shall fulfill the equation:

$$t_k - \left(\sum_{i=1}^{k} (1 + d_i) T_N \right) + j_k + \text{offset}, \qquad \text{(EQ 1)}$$

where T_N is the nominal slot length (625 µs), j_k denotes jitter ($|j_k| \leq 1$ µs) at the start of slot k, and, d_k, denotes the drift ($|d_k| \leq 20$ ppm) within slot k. The jitter and drift may vary arbitrarily within the given limits for every slot, while *offset* is an arbitrary but fixed constant. For hold, park and sniff the drift and jitter parameters specified in Link Manager Protocol [Part C] Section 4.3.1 on page 262 apply.

2.2.5.1 Piconet physical channel timing

In the figures, only single-slot packets are shown as an example.

The master TX/RX timing is shown in Figure 2.3 on page 73. In Figure 2.3 and Figure 2.4 the channel hopping frequencies are indicated by *f(k)* where k is the time slot number. After transmission, a return packet is expected N × 625 µs after the start of the TX packet where N is an odd, integer larger than 0. N depends on the type of the transmitted packet.

To allow for some time slipping, an uncertainty window is defined around the exact receive timing. During normal operation, the window length shall be 20 µs, which allows the RX packet to arrive up to 10 µs too early or 10 µs too late. It is recommended that slaves implement variable sized windows or time tracking to accommodate a master's absence of more than 250ms.

During the beginning of the RX cycle, the access correlator shall search for the correct channel access code over the uncertainty window. If an event trigger does not occur the receiver may go to sleep until the next RX event. If in the course of the search, it becomes apparent that the correlation output will never exceed the final threshold, the receiver may go to sleep earlier. If a trigger event occurs, the receiver shall remain open to receive the rest of the packet unless the packet is for another device, a non-recoverable header error is detected, or a non-recoverable payload error is detected.

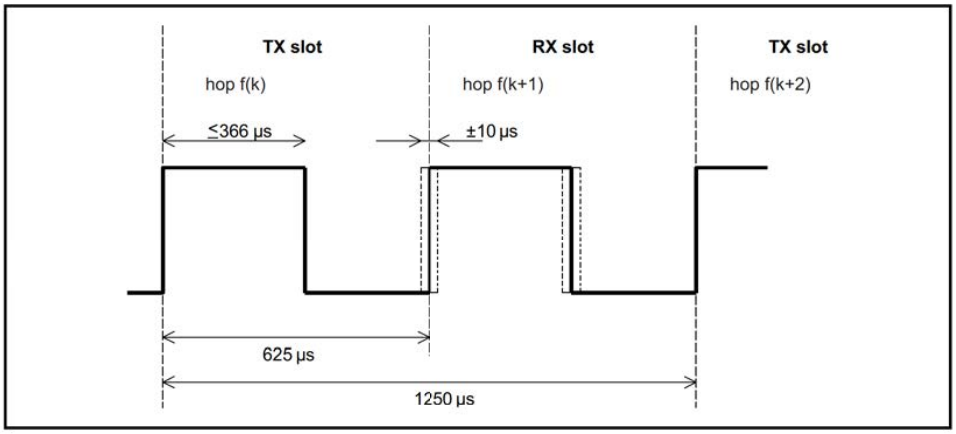


Figure 2.3: RX/TX cycle of master transceiver in normal mode for single-slot packets.

Each master transmission shall be derived from bit 2 of the Master's native Bluetooth clock, thus the current transmission will be scheduled Mx1250µs after the start of the previous master TX burst where M depends on the transmitted and received packet type and is an even, integer larger than 0. The master TX timing shall be derived from the master's native Bluetooth clock, and thus it will not be affected by time drifts in the slave(s).

Slaves maintain an estimate of the master's native clock by adding a timing offset to the slave's native clock (see Section 2.2.4 on page 72). This offset shall be updated each time a packet is received from the master. By comparing the exact RX timing of the received packet with the estimated RX timing, slaves shall correct the offset for any timing misalignments. Since only the channel access code is required to synchronize the slave, slave RX timing can be corrected with any packet sent in the master-to-slave transmission slot.

The slave's TX/RX timing is shown in Figure 2.4 on page 74. The slave's transmission shall be scheduled N × 625µs after the start of the slave's RX packet where N is an odd, positive integer larger than 0. If the slave's RX timing drifts, so will its TX timing. During periods when a slave is in the active mode (see Section 8.6 on page 168) and is not able to receive any valid channel access codes from the master, the slave may increase its receive uncertainty window and/or use predicted timing drift to increase the probability of receiving the master's bursts when reception resumes.

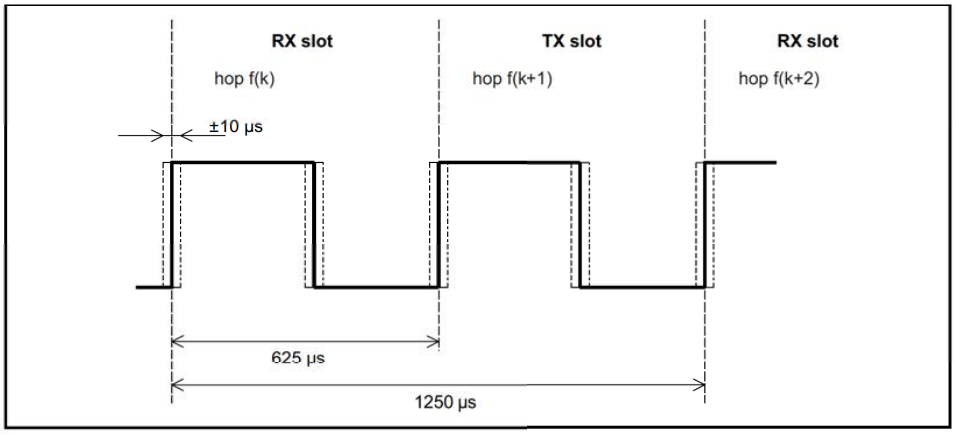


Figure 2.4: RX/TX cycle of slave transceiver in normal mode for single-slot packets.

2.2.5.2 Piconet physical channel re-synchronization

In the piconet physical channel, a slave may loose synchronization if it does not receive a packet from the master at least every 250ms (or less if the low power clock is used). This may occur in sniff, hold, park, in a scatternet or due to interference. When re-synchronizing to the piconet physical channel a slave device shall listen for the master before it may send information. In this case, the length of the search window in the slave device may be increased from 20 µs to a larger value X µs as illustrated in Figure 2.5 on page 75. Note that only RX hop frequencies are used. The hop frequency used in the master-to-slave (RX) slot shall also be used in the uncertainty window, even when it is extended into the preceding time interval normally used for the slave-to-master (TX) slot.

If the length of search window, X, exceeds 1250 μs, consecutive windows shall avoid overlapping search windows. Consecutive windows should instead be centered at *f(k), f(k+4),... f(k+4i)* (where 'i' is an integer), which gives a maximum value X=2500 μs, or even at *f(k), f(k+6),...f(k+6i)* which gives a maximum value X=3750 μs. The RX hop frequencies used shall correspond to the master-to-slave transmission slots.

It is recommended that single slot packets are transmitted by the master during slave re-synchronization.

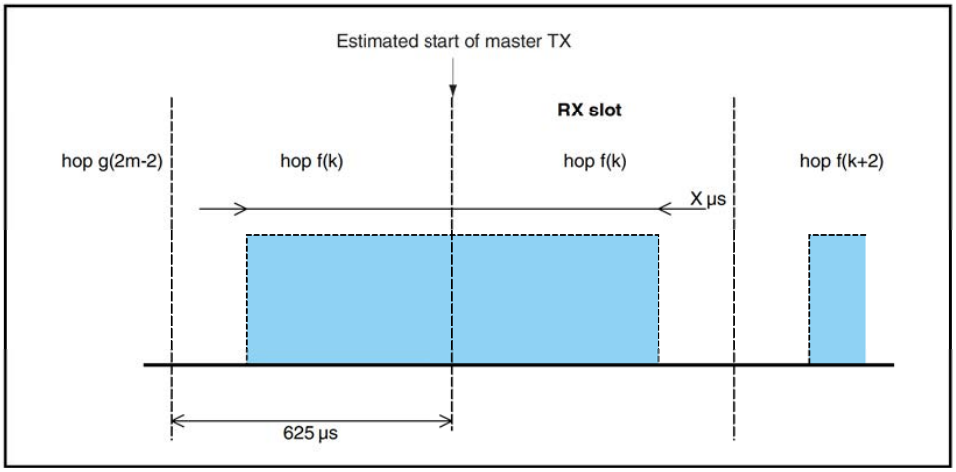


Figure 2.5: RX timing of slave returning from hold mode.

2.3 ADAPTED PICONET PHYSICAL CHANNEL

2.3.1 Hopping characteristics

The adapted piconet physical channel shall use at least N_{min} RF channels (where N_{min} is 20).

The adapted piconet physical channel uses the adapted channel hopping sequence described in Section 2.6 on page 82.

Adapted piconet physical channels can be used for connected devices that have adaptive frequency hopping (AFH) enabled. There are two distinctions between basic and adapted piconet physical channels. The first is that the same channel mechanism that makes the slave frequency the same as the preceding master transmission. The second aspect is that the adapted piconet physical channel may be based on less than the full 79 frequencies of the basic piconet physical channel.

2.4 PAGE SCAN PHYSICAL CHANNEL

Although master and slave roles are not defined prior to a connection, the term *master* is used for the paging device (that becomes a master in the **CONNECTION** state) and *slave* is used for the page scanning device (that becomes a slave in the **CONNECTION** state).

2.4.1 Clock estimate for paging

A paging device uses an estimate of the native clock of the page scanning device, CLKE; i.e. an offset shall be added to the CLKN of the pager to approximate the CLKN of the recipient, see Figure 2.6 on page 76. CLKE shall be derived from the reference CLKN by adding an offset. By using the CLKN of the recipient, the pager might be able to speed up the connection establishment.

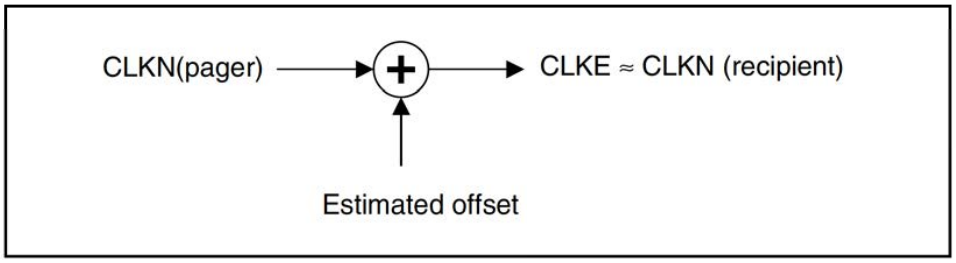


Figure 2.6: Derivation of CLKE.

2.4.2 Hopping characteristics

The page scan physical channel follows a slower hopping pattern than the basic piconet physical channel and is a short pseudo-random hopping sequence through the RF channels. The timing of the page scan channel shall be determined by the native Bluetooth clock of the scanning device. The frequency hopping sequence is determined by the Bluetooth address of the scanning device.

The page scan physical channel uses the page, master page response, slave page response, and page scan hopping sequences specified in Section 2.6 on page 82.

2.4.3 Paging procedure timing

During the paging procedure, the master shall transmit paging messages (see Table 8.3 on page 159) corresponding to the slave to be connected. Since the paging message is a very short packet, the hop rate is 3200 hops/s. In a single TX slot interval, the paging device shall transmit on two different hop frequencies. In Figure 2.7 through Figure 2.11, *f(k)* is used for the frequencies of the page hopping sequence and *f'(k)* denotes the corresponding page response sequence frequencies. The first transmission starts where $CLK_0 = 0$ and the second transmission starts where $CLK_0 = 1$.

In a single RX slot interval, the paging device shall listen for the slave page response message on two different hop frequencies. Similar to transmission, the nominal reception starts where $CLK_0 = 0$ and the second reception nominally starts where $CLK_0 = 1$; see Figure 2.7 on page 77. During the TX slot, the paging device shall send the paging message at the TX hop frequencies *f(k)* and *f(k+1)*. In the RX slot, it shall listen for a response on the corresponding RX hop frequencies *f'(k)* and *f'(k+1)*. The listening periods shall be exactly timed 625 µs after the corresponding paging packets, and shall include a ±10 µs uncertainty window.

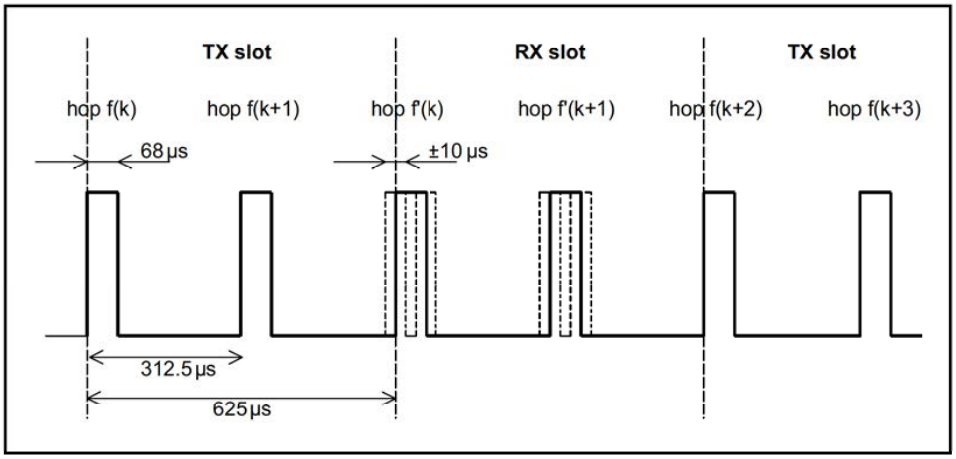


Figure 2.7: RX/TX cycle of transceiver in PAGE mode.

2.4.4 Page response timing

At connection setup a master page response packet is transmitted from the master to the slave (see Table 8.3 on page 159). This packet establishes the timing and frequency synchronization. After the slave device has received the page message, it shall return a response message that consists of the slave page response packet and shall follow 625 µs after the receipt of the page message. The master shall send the master page response packet in the TX slot following the RX slot in which it received the slave response, according to the RX/TX timing of the master. The time difference between the slave page response and master page response message will depend on the timing of the page message the slave received. In Figure 2.8 on page 78, the slave receives the paging message sent **first** in the master-to-slave slot. It then responds with a first slave page response packet in the first half of the slave-to-master slot. The timing of the master page response packet is based on the timing of the page message sent first in the preceding master-to-slave slot: there is an exact 1250 µs delay between the first page message and the master page response packet. The packet is sent at the hop frequency *f(k+1)* which is the hop frequency following the hop frequency *f(k)* the page message was received in.

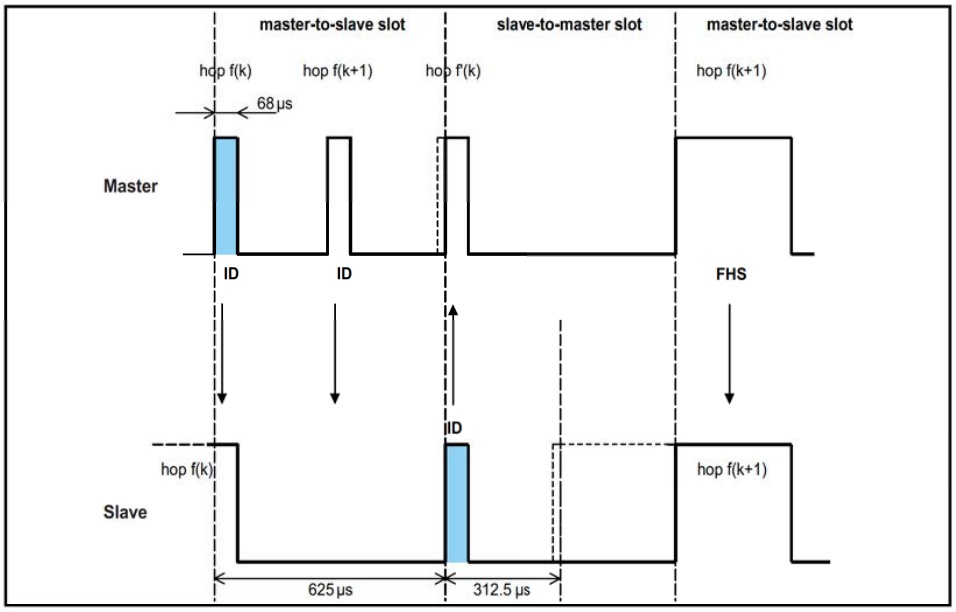


Figure 2.8: Timing of page response packets on successful page in first half slot

In Figure 2.9 on page 79, the slave receives the paging message sent **second** in the master-to-slave slot. It then responds with a slave page response packet in the second half of the slave-to-master slot exactly 625 µs after the receipt of the page message. The timing of the master page response packet is still based on the timing of the page message sent **first** in the preceding master-to-slave slot: there is an exact 1250 µs delay between the **first** page message and the master page response packet. The packet is sent at the hop frequency *f(k+2)* which is the hop frequency following the hop frequency *f(k+1)* the page message was received in.

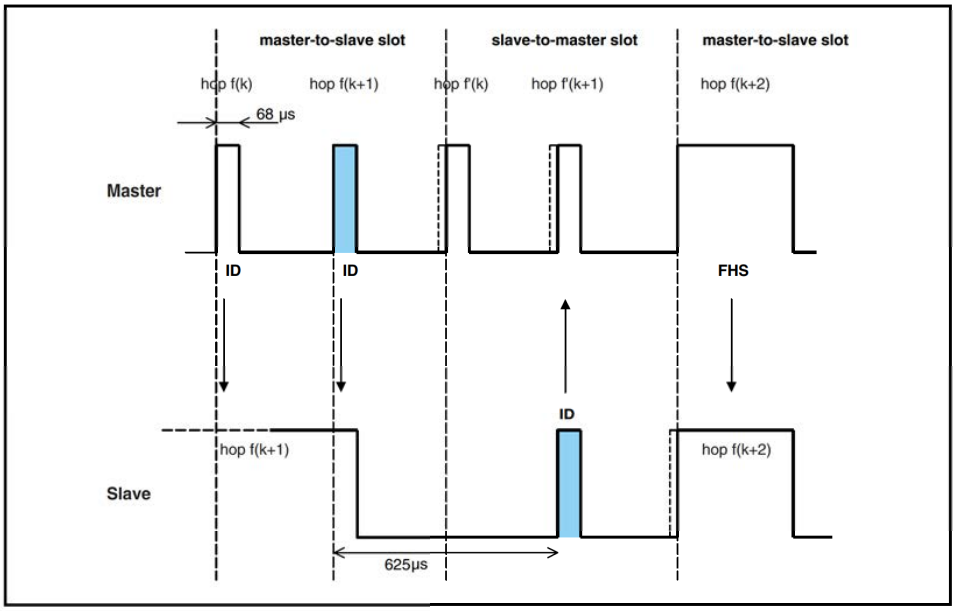


Figure 2.9: Timing of page response packets on successful page in second half slot

The slave shall adjust its RX/TX timing according to the reception of the master page response packet (and not according to the reception of the page message). That is, the second slave page response message that acknowledges the reception of the master page response packet shall be transmitted 625 µs after the start of the master page response packet.

2.5 INQUIRY SCAN PHYSICAL CHANNEL

Although master and slave roles are not defined prior to a connection, the term *master* is used for the inquiring device and *slave* is used for the inquiry scanning device.

2.5.1 Clock for inquiry

The clock used for inquiry and inquiry scan shall be the device's native clock.

2.5.2 Hopping characteristics

The inquiry scan channel follows a slower hopping pattern than the piconet physical channel and is a short pseudo-random hopping sequence through the RF channels. The timing of the inquiry scan channel is determined by the native Bluetooth clock of the scanning device while the frequency hopping sequence is determined by the general inquiry access code.

The inquiry scan physical channel uses the inquiry, inquiry response, and inquiry scan hopping sequences described in Section 2.6 on page 82.

2.5.3 Inquiry procedure timing

During the inquiry procedure, the master shall transmit inquiry messages with the general or dedicated inquiry access code. The timing for inquiry is the same as for paging (see Section 2.4.3 on page 77).

2.5.4 Inquiry response timing

An inquiry response packet is transmitted from the slave to the master after the slave has received an inquiry message (see Table 8.5 on page 167). This packet contains information necessary for the inquiring master to page the slave (see definition of the FHS packet in Section 6.5.1.4 on page 120) and follows 625µs after the receipt of the inquiry message. In Figure 2.10 and Figure 2.11, *f(k)* is used for the frequencies of the inquiry hopping sequence and f'(k) denotes the corresponding inquiry response sequence frequency. The packet is received by the master at the hop frequency *f'(k)* when the inquiry message received by the slave was first in the master-to-slave slot.

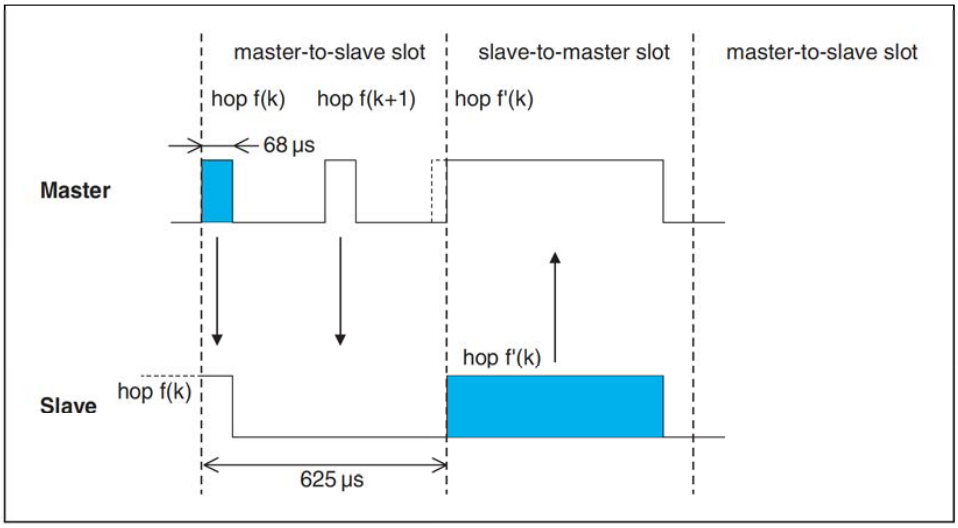


Figure 2.10: Timing of inquiry response packet on successful inquiry in first half slot

When the inquiry message received by the slave was the second in the master-to-slave slot the packet is received by the master at the hop frequency *f'(k+1)*.

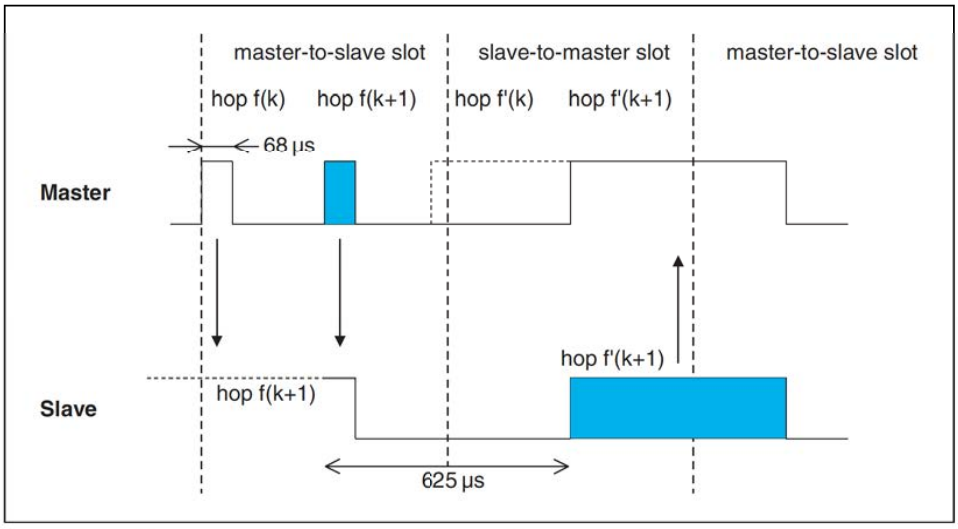


Figure 2.11: Timing of inquiry response packet on successful inquiry in second half slot

2.6 HOP SELECTION

Bluetooth devices shall use the hopping kernel as defined in the following sections.

In total, six types of hopping sequence are defined – five for the basic hop system and one for an adapted set of hop locations used by adaptive frequency hopping (AFH). These sequences are:

- A **page hopping sequence** with 32 wake-up frequencies distributed equally over the 79 MHz, with a period length of 32;
- A **page response hopping sequence** covering 32 response frequencies that are in a one-to-one correspondence to the current page hopping sequence. The master and slave use different rules to obtain the same sequence;
- An **inquiry hopping sequence** with 32 wake-up frequencies distributed equally over the 79 MHz, with a period length of 32;
- An **inquiry response hopping sequence** covering 32 response frequencies that are in a one-to-one correspondence to the current inquiry hopping sequence.
- A **basic channel hopping sequence** which has a very long period length, which does not show repetitive patterns over a short time interval, and which distributes the hop frequencies equally over the 79 MHz during a short time interval.
- An **adapted channel hopping sequence** derived from the basic channel hopping sequence which uses the same channel mechanism and may use fewer than 79 frequencies. The adapted channel hopping sequence is only used in place of the basic channel hopping sequence. All other hopping sequences are not affected by hop sequence adaptation.

2.6.1 General selection scheme

The selection scheme consists of two parts:

- selecting a sequence;
- mapping this sequence onto the hop frequencies;

The general block diagram of the hop selection scheme is shown in Figure 2.12 on page 83. The mapping from the input to a particular RF channel index is performed in the selection box.

The inputs to the selection box are the selected clock, frozen clock, N, k_{offset}, address, sequence selection and AFH_channel_map. The source of the clock input depends on the hopping sequence selected. Additionally, each hopping sequence uses different bits of the clock (see Table 2.2 on page 91). N and k_{offset} are defined in Section 2.6.4 on page 90.

The *sequence selection* input can be set to the following values:

- page scan
- inquiry scan
- page
- inquiry
- master page response
- slave page response
- inquiry response
- basic channel
- adapted channel

The address input consists of 28 bits including the entire LAP and the 4 LSBs of the UAP. This is designated as the UAP/LAP. When the basic or adapted channel hopping sequence is selected, the Bluetooth device address of the master (BD_ADDR) shall be used. When the page, master page response, slave page response, or page scan hopping sequences are selected the BD_ADDR given by the Host of the paged device shall be used (see HCI Create Connection Command [Part E] Section 7.1.5 on page 406). When the inquiry, inquiry response, or inquiry scan hopping sequences are selected, the UAP/LAP corresponding to the GIAC shall be used even if it concerns a DIAC. Whenever one of the reserved BD_ADDRs (see Section 1.2.1 on page 66) is used for generating a frequency hop sequence, the UAP shall be replaced by the default check initialization (DCI, see Section 7.1 on page 138). The hopping sequence is selected by the sequence selection input to the selection box.

When the adapted channel hopping sequence is selected, the *AFH_channel_map* is an additional input to the selection box. The *AFH_channel_map* indicates which channels shall be *used* and which shall be *unused*. These terms are defined in Section 2.6.3 on page 89.

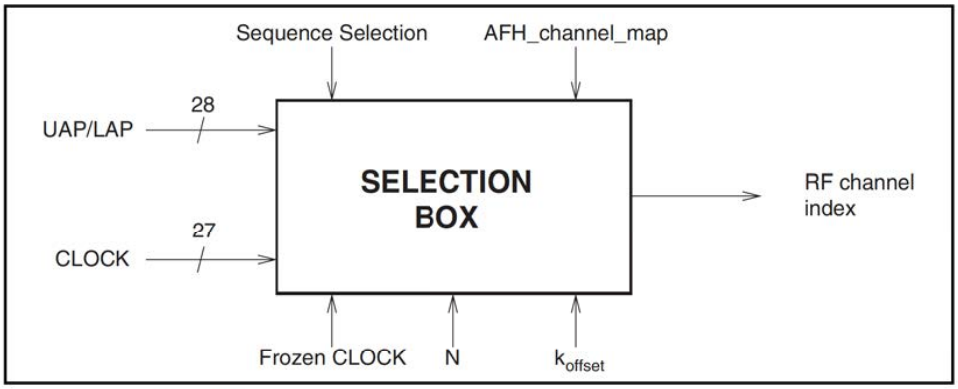


Figure 2.12: General block diagram of hop selection scheme.

The output, *RF channel index*, constitutes a pseudo-random sequence. The RF channel index is mapped to RF channel frequencies using the equation in Table 2.1 on page 29 in the Radio Specification.

The selection scheme chooses a segment of 32 hop frequencies spanning about 64 MHz and visits these hops in a pseudo-random order. Next, a different 32-hop segment is chosen, etc. In the page, master page response, slave page response, page scan, inquiry, inquiry response and inquiry scan hopping sequences, the same 32-hop segment is used all the time (the segment is selected by the address; different devices will have different paging segments). When the basic channel hopping sequence is selected, the output constitutes a pseudo-random sequence that slides through the 79 hops. The principle is depicted in Figure 2.13 on page 84.

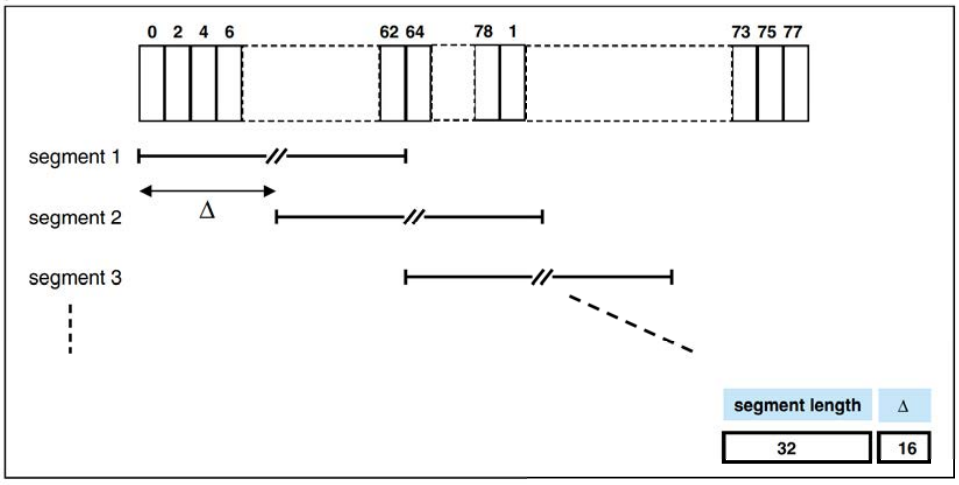


Figure 2.13: Hop selection scheme in CONNECTION state.

The RF frequency shall remain fixed for the duration of the packet. The RF frequency for the packet shall be derived from the Bluetooth clock value in the first slot of the packet. The RF frequency in the first slot after a multi-slot packet shall use the frequency as determined by the Bluetooth clock value for that slot. Figure 2.14 on page 85 illustrates the hop definition on single- and multi-slot packets.

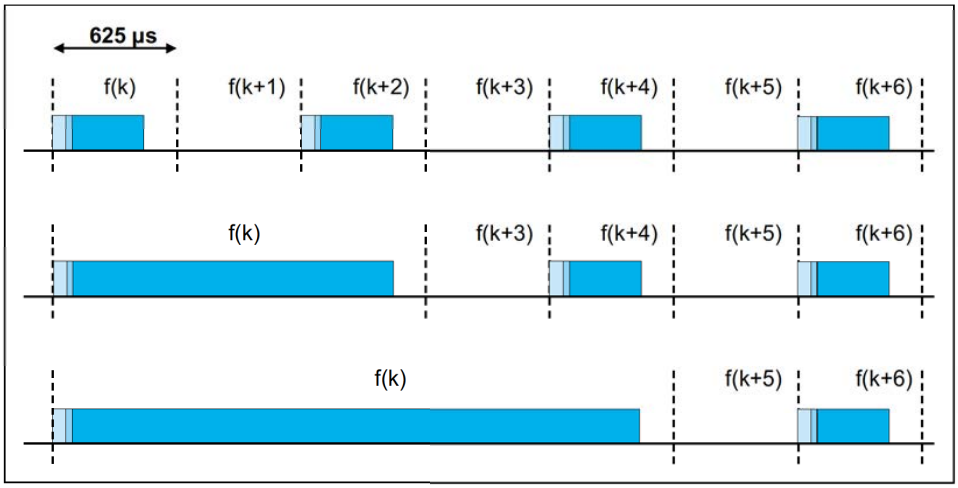


Figure 2.14: Single- and multi-slot packets.

When the adapted channel hopping sequence is used, the pseudo-random sequence contains only frequencies that are in the RF channel set defined by the *AFH_channel_map* input. The adapted sequence has similar statistical properties to the non-adapted hop sequence. In addition, the slave responds with its packet on the same RF channel that was used by the master to address that slave (or would have been in the case of a synchronous reserved slot without a validly received master-to-slave transmission). This is called the *same channel mechanism* of AFH. Thus, the RF channel used for the master to slave packet is also used for the immediately following slave to master packet. An example of the same channel mechanism is illustrated in Figure 2.15 on page 85. The same channel mechanism shall be used whenever the adapted channel hopping sequence is selected.

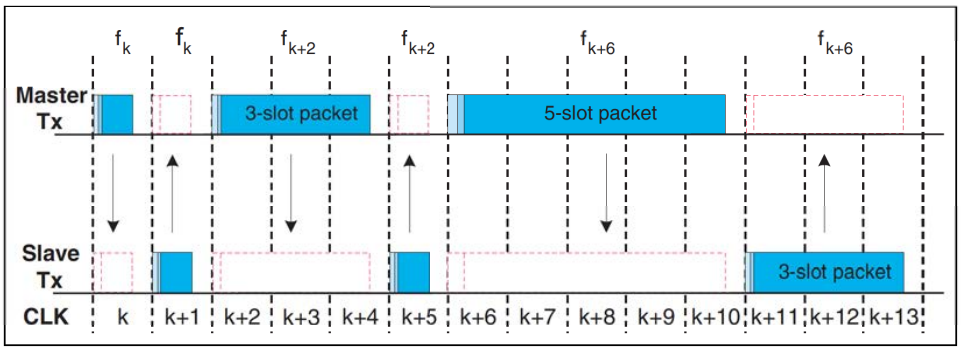


Figure 2.15: Example of the same channel mechanism.

2.6.2 Selection kernel

The basic hop selection kernel shall be as shown in Figure 2.16 on page 86 and is used for the page, page response, inquiry, inquiry response and basic channel hopping selection kernels. In these substates the AFH_channel_map input is unused. The adapted channel hopping selection kernel is described in Section 2.6.3 on page 89. The X input determines the phase in the 32-hop segment, whereas Y1 and Y2 selects between master-to-slave and slave-to-master. The inputs A to D determine the ordering within the segment, the inputs E and F determine the mapping onto the hop frequencies. The kernel addresses a register containing the RF channel indices. This list is ordered so that first all even RF channel indices are listed and then all odd hop frequencies. In this way, a 32-hop segment spans about 64 MHz.

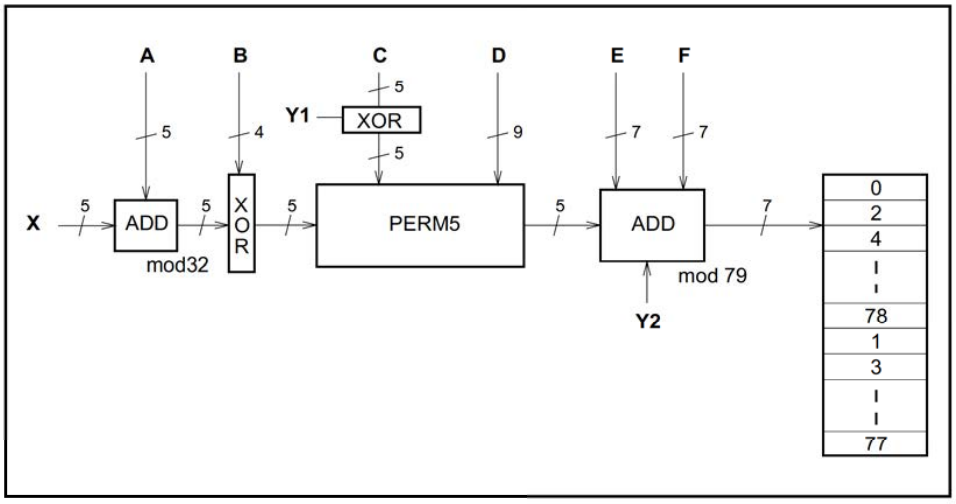


Figure 2.16: Block diagram of the basic hop selection kernel for the hop system.

The selection procedure consists of an addition, an XOR operation, a permutation operation, an addition, and finally a register selection. In the remainder of this chapter, the notation A_i is used for bit i of the BD_ADDR.

2.6.2.1 First addition operation

The first addition operation only adds a constant to the phase and applies a modulo 32 operation. For the page hopping sequence, the first addition is redundant since it only changes the phase within the segment. However, when different segments are concatenated (as in the basic channel hopping sequence), the first addition operation will have an impact on the resulting sequence.

2.6.2.2 XOR operation

Let Z' denote the output of the first addition. In the XOR operation, the four LSBs of Z' are modulo-2 added to the address bits $A_{22\text{-}19}$. The operation is illustrated in Figure 2.17 on page 87.

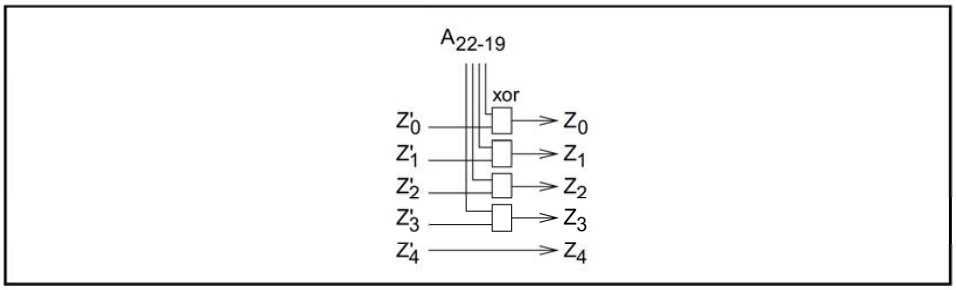


Figure 2.17: XOR operation for the hop system.

2.6.2.3 Permutation operation

The permutation operation involves the switching from 5 inputs to 5 outputs for the hop system, controlled by the control word. The permutation or switching box shall be as shown in Figure 2.18 on page 88. It consists of 7 stages of butterfly operations. The control of the butterflies by the control signals P is shown in Table 2.1. $P_{0\text{-}8}$ corresponds to $D_{0\text{-}8}$, and, P_{i+9} corresponds to $C_i \oplus Y1$ for $i = 0 \ldots 4$ in Figure 2.16.

Control signal	Butterfly		Control signal	Butterfly
P_0	$\{Z_0,Z_1\}$		P_8	$\{Z_1,Z_4\}$
P_1	$\{Z_2,Z_3\}$		P_9	$\{Z_0,Z_3\}$
P_2	$\{Z_1,Z_2\}$		P_{10}	$\{Z_2,Z_4\}$
P_3	$\{Z_3,Z_4\}$		P_{11}	$\{Z_1,Z_3\}$
P_4	$\{Z_0,Z_4\}$		P_{12}	$\{Z_0,Z_3\}$
P_5	$\{Z_1,Z_3\}$		P_{13}	$\{Z_1,Z_2\}$
P_6	$\{Z_0,Z_2\}$			
P_7	$\{Z_3,Z_4\}$			

Table 2.1: Control of the butterflies for the hop system

The Z input is the output of the XOR operation as described in the previous section. The butterfly operation can be implemented with multiplexers as depicted in Figure 2.19 on page 88.

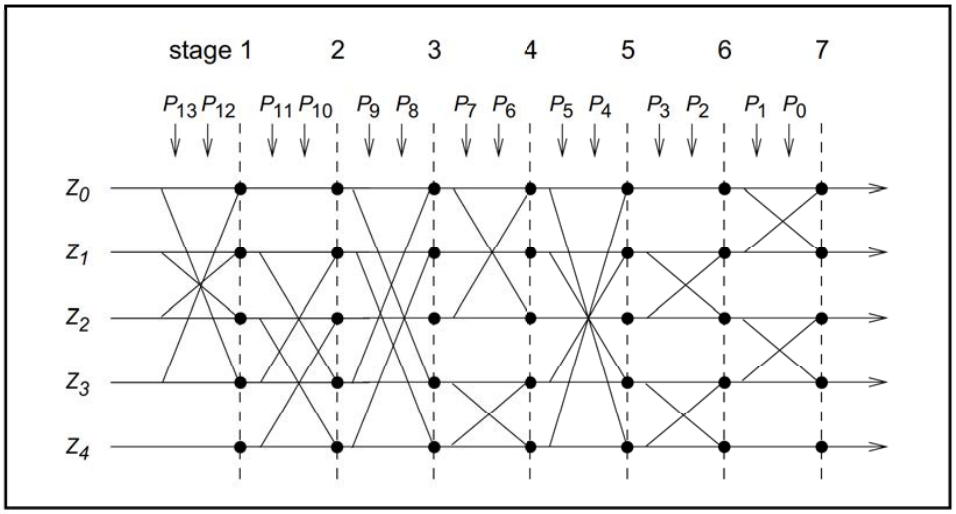


Figure 2.18: Permutation operation for the hop system.

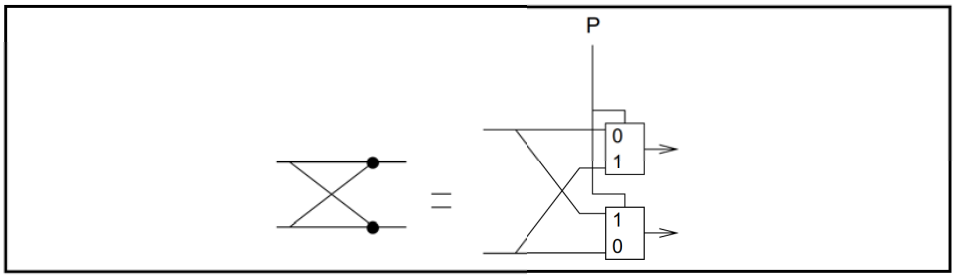


Figure 2.19: Butterfly implementation.

2.6.2.4 Second addition operation

The addition operation only adds a constant to the output of the permutation operation. The addition is applied modulo 79.

2.6.2.5 Register bank

The output of the adder addresses a bank of 79 registers. The registers are loaded with the synthesizer code words corresponding to the hop frequencies 0 to 78. Note that the upper half of the bank contains the even hop frequencies, whereas the lower half of the bank contains the odd hop frequencies.

2.6.3 Adapted hop selection kernel

The adapted hop selection kernel is based on the basic hop selection kernel defined in the preceding sections.

The inputs to the adapted hop selection kernel are the same as for the basic hop system kernel except that the input AFH_channel_map (defined in Link Manager Protocol [Part C] Section 5.2 on page 303) is used. The *AFH_channel_map* indicates which RF channels shall be *used* and which shall be *unused*. When hop sequence adaptation is enabled, the number of *used* RF channels may be reduced from 79 to some smaller value N. All devices shall be capable of operating on an adapted hop sequence (AHS) with $N_{min} \leq N \leq 79$, with any combination of *used* RF channels within the *AFH_channel_map* that meets this constraint. N_{min} is defined in Section 2.3.1 on page 75.

Adaptation of the hopping sequence is achieved through two additions to the basic channel hopping sequence according to Figure 2.16 on page 86:

- *Unused* RF channels are re-mapped uniformly onto *used* RF channels. That is, if the hop selection kernel of the basic system generates an *unused* RF channel, an alternative RF channel out of the set of *used* RF channels is selected pseudo-randomly.
- The *used* RF channel generated for the master-to-slave packet is also used for the immediately following slave-to-master packet (see Section 2.6.1 on page 82).

2.6.3.1 Channel re-mapping function

When the adapted hop selection kernel is selected, the basic hop selection kernel according to Figure 2.16 on page 86 is initially used to determine an RF channel. If this RF channel is *unused* according to the *AFH_channel_map*, the *unused* RF channel is re-mapped by the re-mapping function to one of the *used* RF channels. If the RF channel determined by the basic hop selection kernel is already in the set of *used* RF channels, no adjustment is made. The hop sequence of the (non-adapted) basic hop equals the sequence of the adapted selection kernel on all locations where *used* RF channels are generated by the basic hop. This property facilitates non-AFH slaves remaining synchronized while other slaves in the piconet are using the adapted hopping sequence.

A block diagram of the re-mapping mechanism is shown in Figure 2.20 on page 90. The re-mapping function is a post-processing step to the selection kernel from Figure 2.16 on page 86, denoted as 'Hop selection of the basic hop'. The output f_k of the basic hop selection kernel is an RF channel number that ranges between 0 and 78. This RF channel will either be in the set of *used* RF channels or in the set of *unused* RF channels.

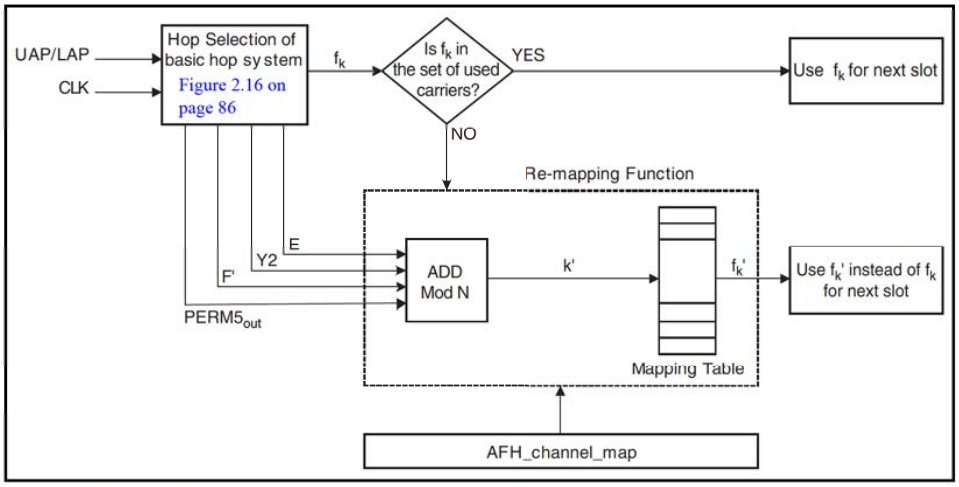


Figure 2.20: Block diagram of adaptive hop selection mechanism

When an unused RF channel is generated by the basic hop selection mechanism, it is re-mapped to the set of *used* RF channels as follows. A new index *k'* ∈ {0, 1,..., *N*-1} is calculated using some of the parameters from the basic hop selection kernel:

$$k' = (PERM5_{out} + E + F' + Y2) \bmod N$$

where *F'* is defined in Table 2.2 on page 91. The index *k'* is then used to select the re-mapped channel from a mapping table that contains all of the even *used* RF channels in ascending order followed by all the odd *used* RF channels in ascending order (i.e., the mapping table of Figure 2.16 on page 86 with all the *unused* RF channels removed).

2.6.4 Control word

In the following section X_{j-i}, $i<j$, will denote bits i, $i+1$,...,j of the bit vector X. By convention, X_0 is the least significant bit of the vector X.

The control word of the kernel is controlled by the overall control signals X, Y1, Y2, A to F, and F' as illustrated in Figure 2.16 on page 86 and Figure 2.20 on page 90. During paging and inquiry, the inputs A to E use the address values as given in the corresponding columns of Table 2.2 on page 91. In addition, the inputs X, Y1 and Y2 are used. The F and F' inputs are unused. The clock bits CLK_{6-2} (i.e., input X) specifies the phase within the length 32 sequence. CLK_1 (i.e., inputs Y1 and Y2) is used to select between TX and RX. The address inputs determine the sequence order within segments. The final mapping onto the hop frequencies is determined by the register contents.

During the **CONNECTION** state (see Section 8.5 on page 167), the inputs A, C and D shall be derived from the address bits being bit-wise XORed with the

clock bits as shown in the “Connection state” column of Table 2.2 on page 91 (the two most significant bits, MSBs, are XORed together, the two second MSBs are XORed together, etc.).

	Page scan / Interlaced Page Scan / Inquiry scan / Interlaced Inquiry Scan	Page/Inquiry	Master/Slave page response and Inquiry response	Connection state
X	$CLKN_{16-12}$ / $(CLKN_{16-12}+16) mod 32$ / Xir_{4-0} / $Xir_{4-0}+16) mod 32$	Xp_{4-0}/Xi_{4-0}	$Xprm_{4-0}$ / $Xprs_{4-0}$ / Xir_{4-0}	CLK_{6-2}
Y1	0	$CLKE_1/CLKN_1$	$CLKE_1/CLKN_1/1$	CLK_1
Y2	0	$32 \times CLKE_1$ / $32 \times CLKN_1$	$32 \times CLKE_1$ / $32 \times CLKN_1$ / 32×1	$32 \times CLK_1$
A	A_{27-23}	A_{27-23}	A_{27-23}	$A_{27-23} \oplus CLK_{25-21}$
B	A_{22-19}	A_{22-19}	A_{22-19}	A_{22-19}
C	$A_{8,6,4,2,0}$	$A_{8,6,4,2,0}$	$A_{8,6,4,2,0}$	$A_{8,6,4,2,0} \oplus CLK_{20-16}$
D	A_{18-10}	A_{18-10}	A_{18-10}	$A_{18-10} \oplus CLK_{15-7}$
E	$A_{13,11,9,7,5,3,1}$	$A_{13,11,9,7,5,3,1}$	$A_{13,11,9,7,5,3,1}$	$A_{13,11,9,7,5,3,1}$
F	0	0	0	$16 \times CLK_{27-7} \bmod 79$
F’	n/a	n/a	n/a	$16 \times CLK_{27-7} \bmod N$

Table 2.2: Control for hop system.

The five X input bits vary depending on the current state of the device. In the **page scan** and **inquiry scan** substates, the native clock (CLKN) shall be used. In **CONNECTION** state the master clock (CLK) shall be used as input. The situation is somewhat more complicated for the other states.

2.6.4.1 Page scan and inquiry scan hopping sequences

When the sequence selection input is set to page scan, the Bluetooth device address of the scanning device shall be used as address input. When the sequence selection input is set to inquiry scan, the GIAC LAP and the four LSBs of the DCI (as A_{27-24}), shall be used as address input for the hopping sequence. For the transmitted access code and in the receiver correlator, the appropriate GIAC or DIAC shall be used. The application decides which inquiry access code to use depending on the purpose of the inquiry.

2.6.4.2 Page hopping sequence

When the sequence selection input is set to page, the paging device shall start using the **A**-train, i.e., $\{f(k-8), \ldots, f(k), \ldots, f(k+7)\}$, where $f(k)$ is the source's estimate of the current receiver frequency in the paged device. The index k is a function of all the inputs in Figure 2.16. There are 32 possible paging frequencies within each 1.28 second interval. Half of these frequencies belong to the **A**-train, the rest (i.e., $\{f(k+8), \ldots, f(k+15), f(k-16), \ldots, f(k-9)\}$) belong to the **B**-train. In order to achieve the -8 offset of the **A**-train, a constant of 24 shall be added to the clock bits (which is equivalent to -8 due to the modulo 32 operation). The **B**-train is obtained by setting the offset to 8. A cyclic shift of the order within the trains is also necessary in order to avoid a possible repetitive mismatch between the paging and scanning devices. Thus,

$$Xp = [\mathrm{CLKE}_{16-12} + k_{offset} + (\mathrm{CLKE}_{4-2,0} - \mathrm{CLKE}_{16-12}) \bmod 16] \bmod 32, \quad \text{(EQ 2)}$$

where

$$k_{offset} = \begin{cases} 24 & \text{A-train,} \\ 8 & \text{B-train.} \end{cases} \quad \text{(EQ 3)}$$

Alternatively, each switch between the **A**- and **B**-trains may be accomplished by adding 16 to the current value of k_{offset} (originally initialized with 24).

2.6.4.3 Slave page response hopping sequence

When the sequence selection input is set to *slave page response,* in order to eliminate the possibility of losing the link due to discrepancies of the native clock CLKN and the master's clock estimate CLKE, the four bits CLKN_{16-12} shall be frozen at their current value. The value shall be frozen at the content it has in the slot where the recipient's access code is detected. The native clock shall *not* be stopped; it is merely the values of the bits used for creating the X-input that are kept fixed for a while. A frozen value is denoted by an asterisk (*) in the discussion below.

For each response slot the paged device shall use an X-input value one larger (modulo 32) than in the preceding response slot. However, the first response shall be made with the X-input kept at the same value as it was when the access code was recognized. Let N be a counter starting at zero. Then, the X-input in the $(N+1)$-th response slot (the first response slot being the one immediately following the page slot now responding to) of the **slave response** substate is:

$$Xprs = [\mathrm{CLKN}^*_{16-12} + N] \bmod 32, \quad \text{(EQ 4)}$$

The counter N shall be set to zero in the slot where the slave acknowledges the page (see Figure 8.3 on page 160 and Figure 8.4 on page 160). Then, the value of N shall be increased by one each time CLKN_1 is set to zero, which corresponds to the start of a master TX slot. The X-input shall be constructed this way until the first **FHS** packet is received *and* the immediately following response packet has been transmitted. After this the slave shall enter the **CONNECTION** state using the parameters received in the **FHS** packet.

2.6.4.4 Master page response hopping sequence

When the sequence selection input is set to *master page response*, the master shall freeze its estimated slave clock to the value that triggered a response from the paged device. It is equivalent to using the values of the clock estimate when receiving the slave response (since only CLKE_1 will differ from the corresponding page transmission). Thus, the values are frozen when the slave **ID** packet is received. In addition to the clock bits used, the current value of k_{offset} shall also be frozen. The master shall adjust its X-input in the same way the paged device does, i.e., by incrementing this value by one for each time CLKE_1 is set to zero. The first increment shall be done before sending the **FHS** packet to the paged device. Let N be a counter starting at one. The rule for forming the X-input is:

$$Xprm = [\mathrm{CLKE}^*_{16-12} + k_{offset}{}^* + (\mathrm{CLKE}^*_{4-2,0} - \mathrm{CLKE}^*_{16-12}) \bmod 16 + N] \bmod 32, \quad \text{(EQ 5)}$$

The value of N shall be increased each time CLKE_1 is set to zero, which corresponds to the start of a master TX slot.

2.6.4.5 Inquiry hopping sequence

When the sequence selection input is set to *inquiry*, the X-input is similar to that used in the *page hopping sequence*. Since no particular device is addressed, the native clock CLKN of the inquirer shall be used. Moreover, which of the two train offsets to start with is of no real concern in this state. Consequently,

$$Xi = [\mathrm{CLKN}_{16-12} + k_{offset} + (\mathrm{CLKN}_{4-2,0} - \mathrm{CLKN}_{16-12}) \bmod 16] \bmod 32, \quad \text{(EQ 6)}$$

where k_{offset} is defined by (EQ 3) on page 92. The initial choice of the offset is arbitrary.

The GIAC LAP and the four LSBs of the DCI (as A_{27-24}) shall be used as address input for the hopping sequence generator.

2.6.4.6 Inquiry response hopping sequence

The *inquiry response* hopping sequence is similar to the *slave page response* hopping sequence with respect to the X-input. The clock input shall not be frozen, thus the following equation apply:

$$Xir = [\mathrm{CLKN}_{16-12} + N] \mod 32, \qquad \text{(EQ 7)}$$

Furthermore, the counter N is increased not on CLKN_1 basis, but rather after each **FHS** packet has been transmitted in response to the inquiry. There is no restriction on the initial value of N as it is independent of the corresponding value in the inquiring unit.

The GIAC LAP and the four LSBs of the DCI (as A_{27-24}) shall be used as address input for the hopping sequence generator. The other input bits to the generator shall be the same as for page response.

2.6.4.7 Basic and adapted channel hopping sequence

In the *basic* and *adapted channel hopping sequences*, the clock bits to use in the basic or adapted hopping sequence generation shall always be derived from the master clock, CLK. The address bits shall be derived from the Bluetooth device address of the master.

3 PHYSICAL LINKS

A physical link represents a baseband connection between devices. A physical link is always associated with exactly one physical channel. Physical links have common properties that apply to all logical transports on the physical link.

The common properties of physical links are:

- Power control (see Link Manager Protocol Section 4.1.3 on page 235)
- Link supervision (see Section 3.1 on page 95 and Link Manager Protocol Section 4.1.6 on page 242)
- Encryption (see Security [Part H] Section 4 on page 787 and Link Manager Protocol [Part C] Section 4.2.5 on page 257)
- Channel quality-driven data rate change (see Link Manager Protocol Section 4.1.7 on page 243)
- Multi-slot packet control (see Link Manager Protocol Section 4.1.10 on page 247)

3.1 LINK SUPERVISION

A connection can break down due to various reasons such as a device moving out of range, encountering severe interference or a power failure condition. Since this may happen without any prior warning, it is important to monitor the link on both the master and the slave side to avoid possible collisions when the logical transport address (see Section 4.2 on page 97) or parked member address (see Section 4.7.1 on page 105) is reassigned to another slave.

To be able to detect link loss, both the master and the slave shall use a link supervision timer, $T_{supervision}$. Upon reception of a valid packet header with one of the slave's addresses (see Section 4.2 on page 97) on the physical link, the timer shall be reset. If at any time in **CONNECTION** state, the timer reaches the *supervisionTO* value, the connection shall be considered disconnected. The same link supervision timer shall be used for SCO, eSCO, and ACL logical transports.

The timeout period, *supervisionTO*, is negotiated by the Link Manager. Its value shall be chosen so that the supervision timeout will be longer than hold and sniff periods. Link supervision of a parked slave shall be done by unparking and re-parking the slave.

4 LOGICAL TRANSPORTS

4.1 GENERAL

Between master and slave(s), different types of logical transports may be established. Five logical transports have been defined:

- Synchronous Connection-Oriented (SCO) logical transport
- Extended Synchronous Connection-Oriented (eSCO) logical transport
- Asynchronous Connection-Oriented (ACL) logical transport
- Active Slave Broadcast (ASB) logical transport
- Parked Slave Broadcast (PSB) logical transport

The synchronous logical transports are point-to-point logical transports between a master and a single slave in the piconet. The synchronous logical transports typically support time-bounded information like voice or general synchronous data. The master maintains the synchronous logical transports by using reserved slots at regular intervals. In addition to the reserved slots the eSCO logical transport may have a retransmission window after the reserved slots.

The ACL logical transport is also a point-to-point logical transport between the master and a slave. In the slots not reserved for synchronous logical transport(s), the master can establish an ACL logical transport on a per-slot basis to any slave, including the slave(s) already engaged in a synchronous logical transport.

The ASB logical transport is used by a master to communicate with active slaves. The PSB logical transport is used by a master to communicate with parked slaves.

4.2 LOGICAL TRANSPORT ADDRESS (LT_ADDR)

Each slave active in a piconet is assigned a primary 3-bit logical transport address (LT_ADDR). The all-zero LT_ADDR is reserved for broadcast messages. The master does not have an LT_ADDR. A master's timing relative to the slaves distinguishes it from the slaves. A secondary LT_ADDR is assigned to the slave for each eSCO logical transport in use in the piconet. Only eSCO traffic (i.e. NULL, POLL, and one of the EV packet types as negotiated at eSCO logical transport setup) may be sent on these LT_ADDRs. ACL traffic (including LMP) shall always be sent on the primary LT_ADDR. A slave shall only accept packets with matching primary or secondary LT_ADDR and broadcast packets. The LT_ADDR is carried in the packet header (see Section 6.4 on page 116). The LT_ADDR shall only be valid for as long as a slave is in the active mode. As soon as it is disconnected or parked, the slave shall lose all of its LT_ADDRs.

The primary LT_ADDR shall be assigned by the master to the slave when the slave is activated. This is either at connection establishment, at role switch, or when the slave is unparked. At connection establishment and at role switch, the primary LT_ADDR is carried in the **FHS** payload. When unparking, the primary LT_ADDR is carried in the unpark message.

4.3 SYNCHRONOUS LOGICAL TRANSPORTS

The first type of synchronous logical transport, the SCO logical transport is a symmetric, point-to-point link between the master and a specific slave. The SCO logical transport reserves slots and can therefore be considered as a circuit-switched connection between the master and the slave. The master may support up to three SCO links to the same slave or to different slaves. A slave may support up to three SCO links from the same master, or two SCO links if the links originate from different masters. SCO packets are never retransmitted.

The second type of synchronous logical transport, the eSCO logical transport, is a point-to-point logical transport between the master and a specific slave. eSCO logical transports may be symmetric or asymmetric. Similar to SCO, eSCO reserves slots and can therefore be considered a circuit-switched connection between the master and the slave. In addition to the reserved slots, eSCO supports a retransmission window immediately following the reserved slots. Together, the reserved slots and the retransmission window form the complete eSCO window.

4.4 ASYNCHRONOUS LOGICAL TRANSPORT

In the slots not reserved for synchronous logical transports, the master may exchange packets with any slave on a per-slot basis. The ACL logical transport provides a packet-switched connection between the master and all active slaves participating in the piconet. Both asynchronous and isochronous services are supported. Between a master and a slave only a single ACL logical transport shall exist. For most ACL packets, packet retransmission is applied to assure data integrity.

ACL packets not addressed to a specific slave are considered as broadcast packets and should be read by every slave. If there is no data to be sent on the ACL logical transport and no polling is required, no transmission is required.

4.5 TRANSMIT/RECEIVE ROUTINES

This section describes the way to use the packets as defined in Section 6 on page 109 in order to support the traffic on the ACL, SCO and eSCO logical transports. Both single-slave and multi-slave configurations are considered. In addition, the use of buffers for the TX and RX routines are described.

The TX and RX routines described in sections 4.5.1 and 4.5.2 are informative only.

4.5.1 TX Routine

The TX routine is carried out separately for each asynchronous and synchronous link. Figure 4.1 on page 99 shows the asynchronous and synchronous buffers as used in the TX routine. In this figure, only a single TX asynchronous buffer and a single TX synchronous buffer are shown. In the master, there is a separate TX asynchronous buffer for each slave. In addition there may be one or more TX synchronous buffers for each synchronous slave (different SCO or eSCO logical transports may either reuse the same TX synchronous buffer, or each have their own TX synchronous buffer). Each TX buffer consists of two FIFO registers: one **current** register which can be accessed and read by the Link Controller in order to compose the packets, and one **next** register that can be accessed by the Baseband Resource Manager to load new information. The positions of the switches S1 and S2 determine which register is current and which register is next; the switches are controlled by the Link Controller. The switches at the input and the output of the FIFO registers can never be connected to the same register simultaneously.

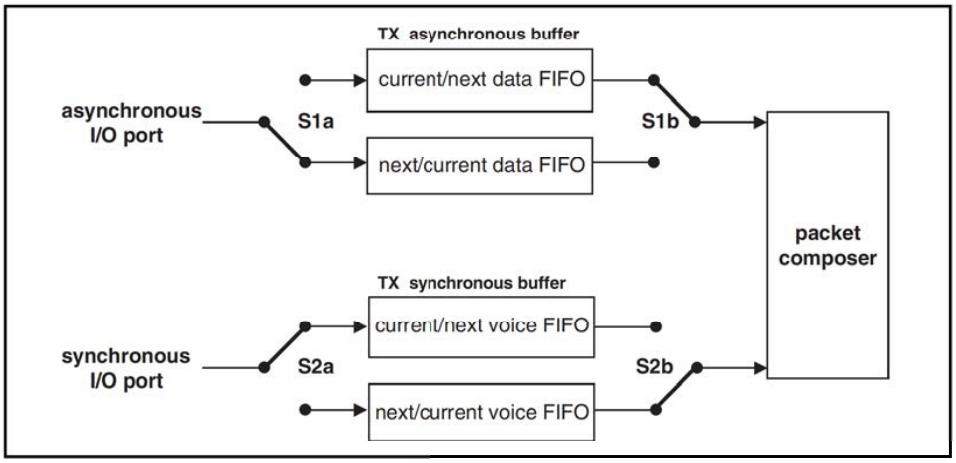


Figure 4.1: Functional diagram of TX buffering.

Of the packets common on the ACL and SCO logical transports (**NULL**, **POLL and DM1**) only the **DM1** packet carries a payload that is exchanged between the Link Controller and the Link Manager; this common packet makes use of the asynchronous buffer. All ACL packets make use of the asynchronous