# Specification
# of the Bluetooth System

Wireless connections made easy

Core

**Bluetooth**™

v1.0 B
December 1st 1999

Samsung Ex. 1019 p. 2

| BLUETOOTH DOC | Date / Day-Month-Year<br>01 Dec 99 | N.B. | Document No.<br>1.C.47/1.0 B |
|---|---|---|---|
| Responsible | e-mail address | | Status |

**Bluetooth.**

# Specification
# of the Bluetooth System

## Version 1.0 B

**Bluetooth.**

## Revision History

The Revision History is shown in Appendix I on page 868

## Contributors

The persons who contributed to this specification are listed in Appendix II on page 879.

## Web Site

This specification can also be found on the Bluetooth website:
http://www.bluetooth.com

## Disclaimer and copyright notice

THIS SPECIFICATION IS PROVIDED "AS IS" WITH NO WARRANTIES WHATSOEVER, INCLUDING ANY WARRANTY OF MERCHANTABILITY, NONINFRINGEMENT, FITNESS FOR ANY PARTICULAR PURPOSE, OR ANY WARRANTY OTHERWISE ARISING OUT OF ANY PROPOSAL, SPECIFICATION OR SAMPLE. All liability, including liability for infringement of any proprietary rights, relating to use of information in this document is disclaimed.

No license, express or implied, by estoppel or otherwise, to any intellectual property rights are granted herein.

Copyright © 1999

Telefonaktiebolaget LM Ericsson,
International Business Machines Corporation,
Intel Corporation,
Nokia Corporation,
Toshiba Corporation .

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

**Bluetooth.**

# MASTER TABLE OF CONTENTS

For the Bluetooth Profiles, *See Volume 2.*

**Part C**                                                    **Volume 1 (1:2)**

## LINK MANAGER PROTOCOL

**Part D**                                                    **Volume 1 (1:2)**

## LOGICAL LINK CONTROL AND ADAPTATION PROTOCOL SPECIFICATION

**Bluetooth.**

---

**Part E**                                                                    **Volume 1 (1:2)**

---

SERVICE DISCOVERY PROTOCOL (SDP)

---

**Part F:1**                                                                  **Volume 1 (1:2)**

---

RFCOMM WITH TS 07.10

---

**Part F:2**                                                                  **Volume 1 (1:2)**

---

IrDA INTEROPERABILITY

---

**Part F:3**                                                    **Volume 1 (1:2)**

## TELEPHONY CONTROL PROTOCOL SPECIFICATION

**Part F:4**                                                    **Volume 1 (1:2)**

## INTEROPERABILITY REQUIREMENTS FOR BLUETOOTH AS A WAP BEARER

**Bluetooth.**

| Part H:1 | Volume 1 (2:2) |
|---|---|

## HOST CONTROLLER INTERFACE FUNCTIONAL SPECIFICATION

| Part H:2 | Volume 1 (2:2) |
|---|---|

## HCI USB TRANSPORT LAYER

| Part H:3 | Volume 1 (2:2) |
|---|---|

## HCI RS232 TRANSPORT LAYER

AFFLT0293237

**Samsung Ex. 1019 p. 9**

**Part H:4**                                                          **Volume 1 (2:2)**

## HCI UART TRANSPORT LAYER

**Part I:1**                                                          **Volume 1 (2:2)**

## BLUETOOTH TEST MODE

**Part I:2**                                                          **Volume 1 (2:2)**

## BLUETOOTH COMPLIANCE REQUIREMENTS

**Bluetooth.**

---

**Part I:3** | **Volume 1 (2:2)**

---

## TEST CONTROL INTERFACE

---

**Part K** | **Profiles - see Volume 2**

---

**Appendix I** | **Volume 1 (2:2)**

---

**Appendix II** | **Volume 1 (2:2)**

---

**Appendix III** | **Volume 1 (2:2)**

---

**Appendix IV** | **Volume 1 (2:2)**

## SAMPLE DATA

---

| **Appendix V** | **Volume 1 (2:2)** |
|---|---|

## BLUETOOTH AUDIO

| **Appendix VI** | **Volume 1 (2:2)** |
|---|---|

## BASEBAND TIMERS

| **Appendix VII** | **Volume 1 (2:2)** |
|---|---|

## OPTIONAL PAGING SCHEMES

| **Appendix VIII** | **Volume 1 (2:2)** |
|---|---|

## BLUETOOTH ASSIGNED NUMBERS

**Appendix IX**                                                  **Volume 1 (2:2)**

## MESSAGE SEQUENCE CHARTS

## Part A

# RADIO SPECIFICATION

Samsung Ex. 1019 p. 16

## CONTENTS

# 1 SCOPE

The Bluetooth transceiver is operating in the 2.4 GHz ISM band. This specification defines the requirements for a Bluetooth transceiver operating in this unlicensed band.

Requirements are defined for two reasons:

- Provide compatibility between the radios used in the system

- Define the quality of the system

The Bluetooth transceiver shall fulfil the stated requirements under the operating conditions specified in Appendix A and Appendix B. The Radio parameters must 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** (except France and Spain):

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

**France:**

Approval Standards: La Reglementation en France por les Equipements fonctionnant dans la bande de frequences 2.4 GHz "RLAN-Radio Local Area Network"
Documents: SP/DGPT/ATAS/23, ETS 300-328, ETS 300-826
Approval Authority: Direction Generale des Postes et Telecommunications
**Note:** A new R&TTE EU Directive will be in effect by March 2000, with consequent effects on the manufacturer's declaration of conformity and free circulation of products within the EU.

**Spain:**

Approval Standards: Supplemento Del Numero 164 Del Boletin Oficial Del Estado (Published 10 July 91, Revised 25 June 93)
Documents: ETS 300-328, ETS 300-826
Approval Authority: Cuadro Nacional De Atribucion De Frecuesias

**Japan:**

Approval Standards: Association of Radio Industries and Businesses, ARIB
Documents: RCR STD-33A
Approval Authority: Ministry of Post and Telecommunications, MPT
Note: The Japanese rules are in revision. Decisions on the revision will take place in Q2 1999.

**North Americas:**

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

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

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

*Radio Specification*

**Bluetooth.**

# 2 FREQUENCY BANDS AND CHANNEL ARRANGEMENT

The Bluetooth system is operating in the 2.4 GHz ISM (Industrial Scientific Medicine) band. In a vast majority of countries around the world the range of this frequency band is 2400 - 2483.5 MHz. Some countries have however national limitations in the frequency range. In order to comply with these national limitations, special frequency hopping algorithms have been specified for these countries. It should be noted that products implementing the reduced frequency band will not work with products implementing the full band. The products implementing the reduced frequency band must therefore be considered as local versions for a single market. The Bluetooth SIG has launched a campaign to overcome these difficulties and reach total harmonization of the frequency band.

| Geography | Regulatory Range | RF Channels |
|---|---|---|
| USA, Europe and most other countries[1] | 2.400-2.4835 GHz | f=2402+k MHz, k=0,...,78 |
| Spain[2] | 2.445-2.475 GHz | f=2449+k MHz, k=0,...,22 |
| France[3] | 2.4465-2.4835 GHz | f=2454+k MHz, k=0,...,22 |

*Table 2.1: Operating frequency bands*

Note 1.   Japan, the MPT announced at the beginning of October 1999 that the Japanese frequency band would be extended to 2400-2483.5 MHz, effective immediately. Testing of devices by TELEC may however need some time to change. The previously specified special frequency-hopping algorithm covering 2471-2497 MHz remains as an option.

Note 2.   There is a proposal in Spain to extend the national frequency band to 2403-2483.5 MHz. The Bluetooth SIG has approached the authorities in Spain to get a full harmonization. The outcome is expected by the beginning of year 2000.

Note 3.   The Bluetooth SIG has established good contacts with the French authorities and are closely following the development of harmonization.

Channel spacing is 1 MHz. In order to comply with out-of-band regulations in each country, a guard band is used at the lower and upper band edge.

| Geography | Lower Guard Band | Upper Guard Band |
|---|---|---|
| USA | 2 MHz | 3.5 MHz |
| Europe (except Spain and France) | 2 MHz | 3.5 MHz |
| Spain | 4 MHz | 26 MHz |
| France | 7.5 MHz | 7.5 MHz |
| Japan | 2 MHz | 2 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 equipment. If the equipment does not have a connector, a reference antenna with 0 dBi gain is assumed.

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

If transmitting antennas of directional gain greater than 0 dBi are used, the applicable paragraphs in ETSI 300 328 and FCC part 15 must be compensated for.

The equipment 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<br>Optional:<br>Pmin[2] to Pmax |
| 2 | 2.5 mW (4 dBm) | 1 mW (0 dBm) | 0.25 mW (-6 dBm) | Optional:<br>Pmin[2] to Pmax |
| 3 | 1 mW (0 dBm) | N/A | N/A | Optional:<br>Pmin[2] to Pmax |

*Table 3.1: Power classes*

Note 1. Minimum output power at maximum power setting.

Note 2. The lower power limit Pmin<-30dBm is suggested but is not mandatory, and may be chosen according to application needs.

A power control is required for power class 1 equipment. The power control is used for limiting the transmitted power over 0 dBm. Power control capability under 0 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 equipment with a maximum transmit power of +20 must be able to control its transmit power down to 4 dBm or less.

Equipment with power control capability optimizes the output power in a link with LMP commands (see Link Manager Protocol). It is done by measuring RSSI and report back if the power should be increased or decreased.

**Bluetooth.**

## 3.1  MODULATION CHARACTERISTICS

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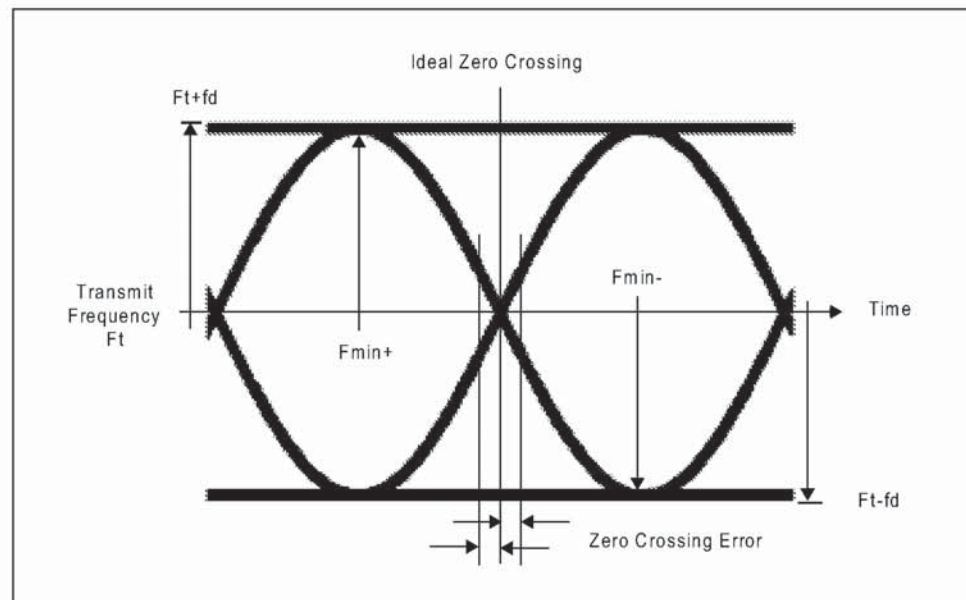


*Figure 3.1:  Figure 3-1 Actual transmit modulation.*

For each transmit channel, the minimum frequency deviation (Fmin = the lesser of {Fmin+, Fmin-}) which corresponds to 1010 sequence shall be no smaller than ±80% of the frequency deviation (fd) which corresponds to a 00001111 sequence.
In addition, the minimum deviation shall never be smaller than 115 kHz.

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.

## 3.2  SPURIOUS EMISSIONS

The spurious emission, in-band and out-of-band, is measured with a frequency hopping transmitter hopping on a single frequency; this means that the synthesizer must change frequency between receive slot and transmit slot, but always returns to the same transmit frequency.

For the USA, FCC parts 15.247, 15.249, 15.205 and 15.209 are applicable regulations. For Japan, RCR STD-33 applies and, for Europe, ETSI 300 328.

*Radio Specification*

**Bluetooth.**

### 3.2.1 In-band Spurious Emission

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

| Frequency offset | Transmit Power |
|---|---|
| ± 550 kHz | -20 dBc |
| |M-N| = 2 | -20 dBm |
| |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.

"In any 100 kHz bandwidth outside the frequency band in which the spread spectrum intentional radiator is operating, the radio frequency power that is produced by the intentional radiator shall be at least 20 dB below that in the 100 kHz bandwidth within the band that contains the highest level of the desired power, based on either an RF conducted or a radiated measurement. Attenuation below the general limits specified in § 15.209(a) is not required. In addition, radiated emissions which fall in the restricted bands, as defined in § 15.205(a), must also comply with the radiated emission limits specified in § 15.209(a) (see § 15.205(c))."

FCC Part 15.247c

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 must, however, comply with an absolute value of –20 dBm.

### 3.2.2 Out-of-Band Spurious Emission

The measured power should be measured in a 100 kHz bandwidth.

| Frequency Band | Operation mode | Idle mode |
|---|---|---|
| 30 MHz - 1 GHz | -36 dBm | -57 dBm |
| 1 GHz – 12.75 GHz | -30 dBm | -47 dBm |
| 1.8 GHz – 1.9 GHz | -47 dBm | -47 dBm |
| 5.15 GHz – 5.3 GHz | -47 dBm | -47 dBm |

*Table 3.3: Out-of-band spurious emission requirement*

**Bluetooth.**

## 3.3  RADIO FREQUENCY TOLERANCE

The transmitted initial center frequency accuracy must be ±75 kHz from $F_c$.
The initial frequency accuracy is defined as being the frequency accuracy before any information is transmitted. Note that the frequency drift requirement is not included in the ±75 kHz.

The transmitter center frequency drift in a packet is specified in Table 3.4. The different packets are defined in the Baseband Specification.

| Type of Packet | Frequency Drift |
|---|---|
| One-slot packet | ±25 kHz |
| Three-slot packet | ±40 kHz |
| Five-slot packet | ±40 kHz |
| Maximum drift rate[1) | 400 Hz/μs |

*Table 3.4: Frequency drift in a package*

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

# 4 RECEIVER CHARACTERISTICS

In order to measure the bit error rate performance; the equipment must have a "loop back" facility. The equipment sends back the decoded information. This facility is specified in the Test Mode Specification.

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

## 4.1 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 requirement for a Bluetooth receiver is an actual sensitivity level of –70 dBm or better. The receiver must achieve the –70 dBm sensitivity level with any Bluetooth transmitter compliant to the transmitter specification specified in Section 3 on page 20.

## 4.2 INTERFERENCE PERFORMANCE

The interference performance on Co-channel and adjacent 1 MHz and 2 MHz are measured with the wanted signal 10 dB over the reference sensitivity level. On all other frequencies the wanted signal shall be 3 dB over the reference sensitivity level. Should the frequency of an interfering signal lie outside of the band 2400-2497 MHz, the out-of-band blocking specification (see Section 4.3 on page 25) shall apply. The interfering signal shall be Bluetooth-modulated (see section 4.8 on page 27). The BER shall be ≤ 0.1%. The signal to interference ratio shall be:

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

*Table 4.1: Interference performance*

Note 1. These specifications are tentative and will be fixed within 18 months after the release of the Bluetooth specification version 1.0. Implementations have to fulfil the final specification after a 3-years' convergence period starting at the release of the Bluetooth specification version 1.0. During the convergence period, devices need to achieve a co-channel interference resistance of +14 dB, an ACI (@1MHz) resistance of +4 dB, Image frequency interference resistance of –6 dB and an ACI to in-band image frequency resistance of –16 dB.

Note 2. In-band image frequency

Note 3. If the image frequency ≠ n*1 MHz, than the image reference frequency is defined as the closest n*1 MHz frequency.

Note 4. If two adjacent channel specifications from Table 4.1 are applicable to the same channel, the more relaxed specification applies.

**Bluetooth.**

These specifications are only to be tested at nominal temperature conditions with a receiver hopping on one frequency, meaning that the synthesizer must change frequency between receive slot and transmit slot, but always return 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 $\geq 2$ MHz from the wanted signal. On these spurious response frequencies a relaxed interference requirement C/I = -17 dB shall be met.

## 4.3  OUT-OF-BAND BLOCKING

The Out of band blocking is 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 $\leq 0.1\%$. 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 |
| 2498 – 3000 MHz | -27 dBm |
| 3000 MHz – 12.75 GHz | -10 dBm |

*Table 4.2:  Out of Band blocking requirements*

24 exceptions are permitted which are dependent upon the given receive channel frequency and are centered at a frequency which is an integer multiple of 1 MHz. At 19 of these spurious response frequencies a relaxed power level -50 dBm of the interferer may used to achieve a BER of 0.1%. At the remaining 5 spurious response frequencies the power level is arbitrary.

## 4.4  INTERMODULATION CHARACTERISTICS

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

*   The wanted signal at frequency $f_0$ with a power level 6 dB over the reference sensitivity level.

*   A static sine wave signal at $f_1$ with a power level of $-39$ dBm

*   A Bluetooth modulated signal (see Section 4.8 on page 27) at $f_2$ with a power level of -39 dBm

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 must fulfil one of the three alternatives.

## 4.5　MAXIMUM USABLE LEVEL

The maximum usable input level the receiver shall operate at shall be better than −20 dBm. The BER shall be less or equal to 0,1% at −20* dBm input power.

## 4.6　SPURIOUS EMISSIONS

The spurious emission for a Bluetooth receiver shall not be more than:

| Frequency Band | Requirement |
|---|---|
| 30 MHz - 1 GHz | -57 dBm |
| 1 GHz – 12.75 GHz | -47 dBm |

*Table 4.3: Out-of-band spurious emission*

The measured power should be measured in a 100 kHz bandwidth.

## 4.7　RECEIVER SIGNAL STRENGTH INDICATOR (OPTIONAL)

A transceiver that wishes to take part in a power-controlled link must be able to measure its own receiver signal strength and determine if the transmitter on the other side of the link should increase or decrease its output power level. A Receiver Signal Strength Indicator (RSSI) makes this possible.

The way the power control is specified is to have a golden receive power. This golden receive power is defined as a range with a low limit and a high limit. The RSSI must have a minimum dynamic range equal to this range. The RSSI must have an absolute accuracy of ±4dB or better when the receive signal power is −60 dBm. In addition, a minimum range of 20±6 dB must be covered, starting from −60 dB and up (see ).
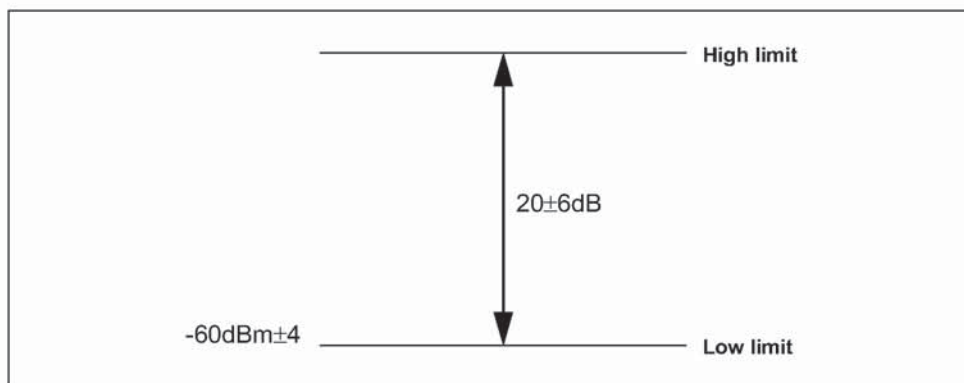


*Figure 4.1: RSSI dynamic range and accuracy*

**Bluetooth.**

## 4.8   REFERENCE INTERFERENCE-SIGNAL DEFINITION

A Bluetooth modulated interfering signal is defined as:

Modulation = GFSK

Modulation index = 0.32±1%

BT= 0.5±1%

Bit Rate = 1 Mbps ±1 ppm

Modulating Data = PRBS9

Frequency accuracy better than ±1 ppm.

# 5  APPENDIX A

## 5.1  NOMINAL TEST CONDITIONS (NTC)

### 5.1.1  Nominal temperature

The nominal temperature conditions for tests shall be +15 to +35 $^{\circ}$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 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.

**Bluetooth.**

## 5.2   EXTREME TEST CONDITIONS

### 5.2.1   Extreme temperatures

The extreme temperature range is defined as 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 the 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 Radio parameters shall be tested in the following conditions
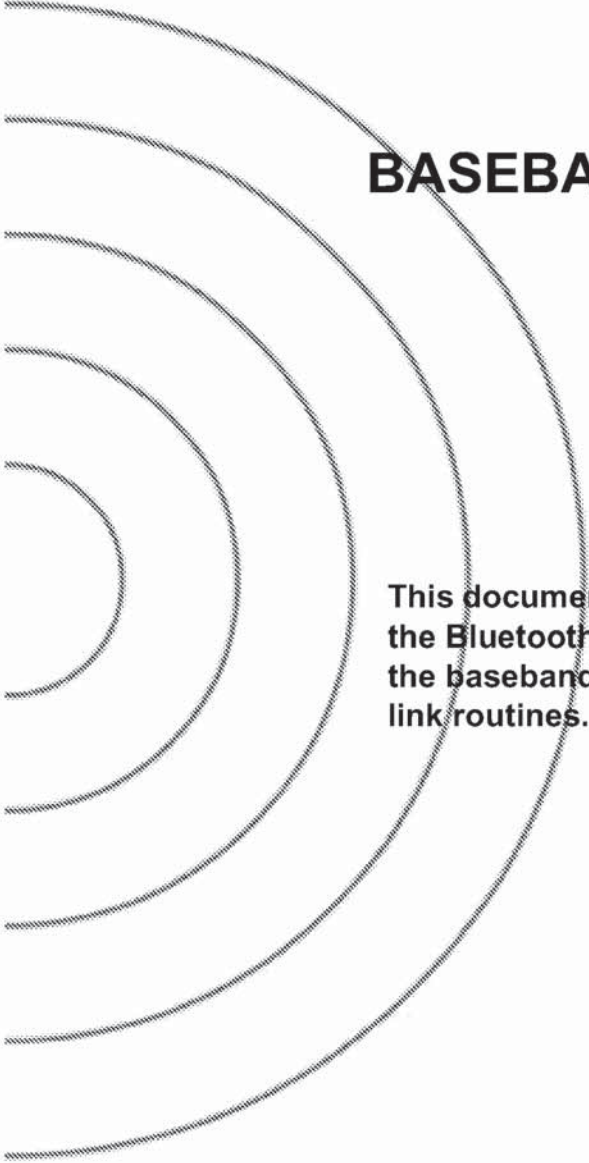
| Parameter | Temperature | Power source |
|---|---|---|
| Output Power | ETC | ETC |
| Power control | NTC | NTC |
| Modulation index | ETC | ETC |
| Initial Carrier Frequency accuracy | ETC | ETC |
| Carrier Frequency drift | ETC | ETC |
| In-band spurious emissions | ETC | ETC |
| Out-of-band Spurious Emissions | ETC | ETC |
| 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

# Part B

# BASEBAND SPECIFICATION

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

**Bluetooth.**

## CONTENTS

**Samsung Ex. 1019 p. 37**

**Bluetooth.**

# 1 GENERAL DESCRIPTION

Bluetooth is a short-range radio link intended to replace the cable(s) connecting portable and/or fixed electronic devices. Key features are robustness, low complexity, low power, and low cost.

Bluetooth operates in the unlicensed ISM band at 2.4 GHz. A frequency hop transceiver is applied to combat interference and fading. A shaped, binary FM modulation is applied to minimize transceiver complexity. The symbol rate is 1 Ms/s. A slotted channel is applied with a nominal slot length of 625 μs. For full duplex transmission, a Time-Division Duplex (TDD) scheme is used. On the channel, information is exchanged through packets. Each packet is transmitted on a different hop frequency. A packet nominally covers a single slot, but can be extended to cover up to five slots.

The Bluetooth protocol uses a combination of circuit and packet switching. Slots can be reserved for synchronous packets. Bluetooth can support an asynchronous data channel, up to three simultaneous synchronous voice channels, or a channel which simultaneously supports asynchronous data and synchronous voice. Each voice channel supports a 64 kb/s synchronous (voice) channel in each direction. The asynchronous channel can support maximal 723.2 kb/s asymmetric (and still up to 57.6 kb/s in the return direction), or 433.9 kb/s symmetric.

The Bluetooth system consists of a radio unit (see Radio Specification), a link control unit, and a support unit for link management and host terminal interface functions, see Figure 1.1 on page 41. The current document describes the specifications of the Bluetooth link controller, which carries out the baseband protocols and other low-level link routines. Link layer messages for link set-up and control are defined in the Link Manager Protocol on page 185.
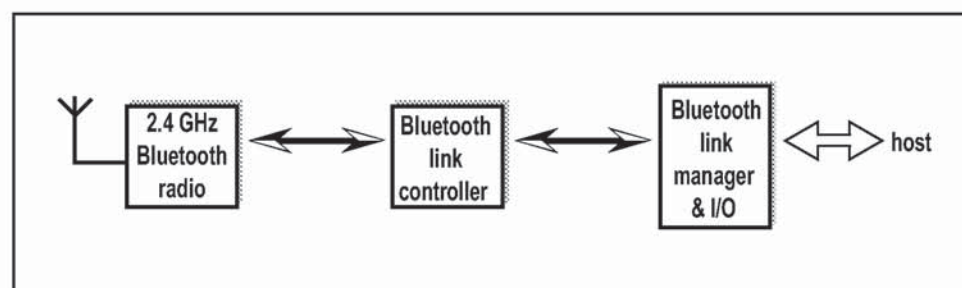


Figure 1.1: Different functional blocks in the Bluetooth system

The Bluetooth system provides a point-to-point connection (only two Bluetooth units involved), or a point-to-multipoint connection, see Figure 1.2 on page 42. In the point-to-multipoint connection, the channel is shared among several Bluetooth units. Two or more units sharing the same channel form a *piconet*. One Bluetooth unit acts as the master of the piconet, whereas the other unit(s)

**Bluetooth.**

acts as slave(s). Up to seven slaves can be active in the piconet. In addition, many more slaves can remain locked to the master in a so-called parked state. These parked slaves cannot be active on the channel, but remain synchronized to the master. Both for active and parked slaves, the channel access is controlled by the master.

Multiple piconets with overlapping coverage areas form a ***scatternet***. Each piconet can only have 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 another piconet. The piconets shall not be time- or frequency-synchronized. Each piconet has its own hopping channel.
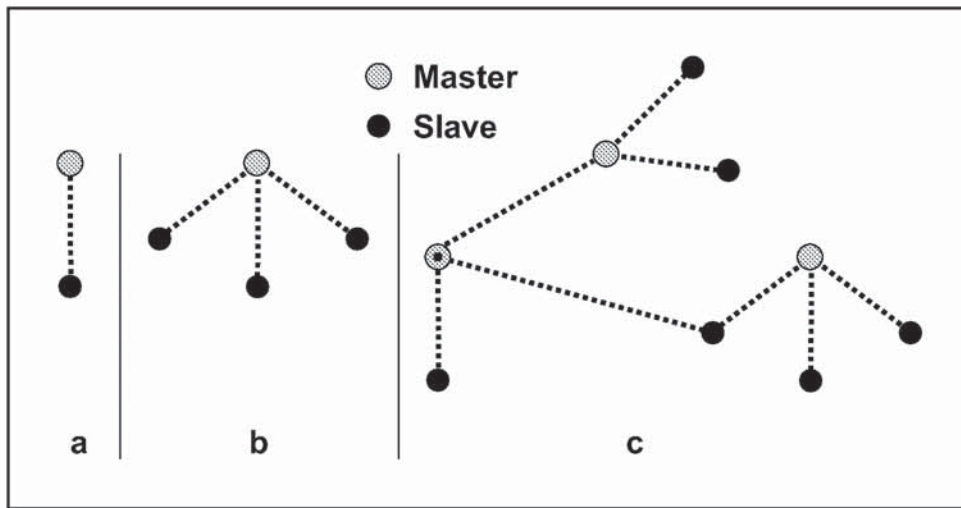


*Figure 1.2: Piconets with a single slave operation (a), a multi-slave operation (b) and a scatternet operation (c).*

**Bluetooth.**

# 2 PHYSICAL CHANNEL

## 2.1 FREQUENCY BAND AND RF CHANNELS

Bluetooth operates in the 2.4 GHz ISM band. Although globally available, the exact location and the width of the band may differ by country. In the US and Europe, a band of 83.5 MHz width is available; in this band, 79 RF channels spaced 1 MHz apart are defined. In Japan, Spain, and France, a smaller band is available; in this band, 23 RF channels spaced 1 MHz apart are defined.

| Country | Frequency Range | RF Channels | |
|---|---|---|---|
| Europe[*] & USA | 2400 - 2483.5 MHz | $f = 2402 + k$ MHz | $k = 0,...,78$ |
| Japan | 2471 - 2497 MHz | $f = 2473 + k$ MHz | $k = 0,...,22$ |
| Spain | 2445 - 2475 MHz | $f = 2449 + k$ MHz | $k = 0,...,22$ |
| France | 2446.5 - 2483.5 MHz | $f = 2454 + k$ MHz | $k = 0,...,22$ |

*Table 2.1: Available RF channels*

[*]. except Spain and France

## 2.2 CHANNEL DEFINITION

The channel is represented by a pseudo-random hopping sequence hopping through the 79 or 23 RF channels. The hopping sequence is unique for the piconet and is determined by the Bluetooth device address of the master; the phase in the hopping sequence is determined by the Bluetooth clock of the master. The channel is divided into time slots where each slot corresponds to an RF hop frequency. Consecutive hops correspond to different RF hop frequencies. The nominal hop rate is 1600 hops/s. All Bluetooth units participating in the piconet are time- and hop-synchronized to the channel.

## 2.3 TIME SLOTS

The channel is divided into time slots, each 625 μs in length. The time slots are numbered according to the Bluetooth clock of the piconet master. The slot numbering ranges from 0 to $2^{27}-1$ and is cyclic with a cycle length of $2^{27}$.

In the time slots, master and slave can transmit packets.

A TDD scheme is used where master and slave alternatively transmit, see Figure 2.1 on page 44. The master shall start its transmission in even-numbered time slots only, and the slave shall start its transmission in odd-numbered time slots only. The packet start shall be aligned with the slot start. Packets transmitted by the master or the slave may extend over up to five time slots.

The RF hop frequency shall remain fixed for the duration of the packet. For a single packet, the RF hop frequency to be used is derived from the current Bluetooth clock value. For a multi-slot packet, the RF hop frequency to be used for the entire packet is derived from the Bluetooth clock value in the first slot of the packet. The RF hop frequency in the first slot after a multi-slot packet shall use the frequency as determined by the current Bluetooth clock value. Figure 2.2 on page 44 illustrates the hop definition on single- and multi-slot packets. If a packet occupies more than one time slot, the hop frequency applied shall be the hop frequency as applied in the time slot where the packet transmission was started.
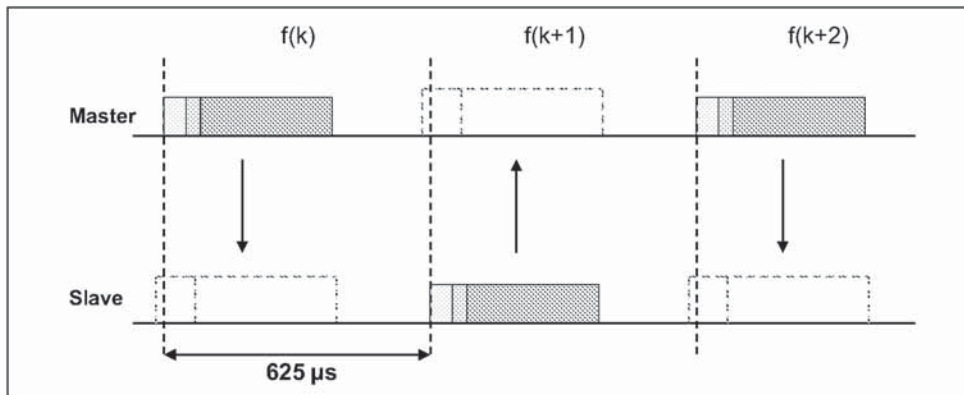


Figure 2.1: TDD and timing
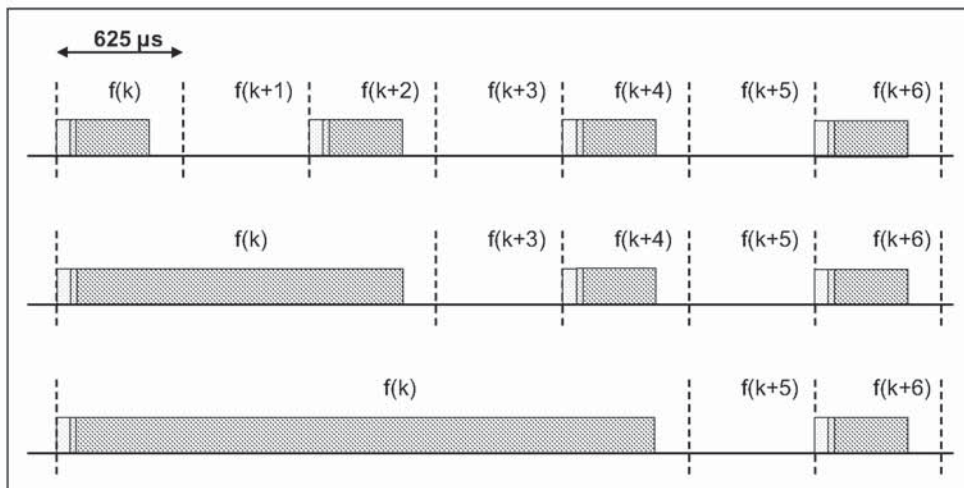


Figure 2.2: Multi-slot packets

## 2.4 MODULATION AND BIT RATE

The data transmitted has a symbol rate of 1 Ms/s. A Gaussian-shaped, binary FSK modulation is applied with a *BT* product of 0.5. A binary one is represented by a positive frequency deviation, a binary zero by a negative frequency deviation. The maximum frequency deviation shall be between 140 kHz and 175 kHz.

# 3 PHYSICAL LINKS

## 3.1 GENERAL

Between master and slave(s), different types of links can be established. Two link types have been defined:

- Synchronous Connection-Oriented (SCO) link
- Asynchronous Connection-Less (ACL) link

The SCO link is a point-to-point link between a master and a single slave in the piconet. The master maintains the SCO link by using reserved slots at regular intervals. The ACL link is a point-to-multipoint link between the master and all the slaves participating on the piconet. In the slots not reserved for the SCO link(s), the master can establish an ACL link on a per-slot basis to any slave, including the slave(s) already engaged in an SCO link.

## 3.2 SCO LINK

The SCO link is a symmetric, point-to-point link between the master and a specific slave. The SCO link reserves slots and can therefore be considered as a circuit-switched connection between the master and the slave. The SCO link typically supports time-bounded information like voice. The master can support up to three SCO links to the same slave or to different slaves. A slave can 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 master will send SCO packets at regular intervals, the so-called SCO interval $T_{SCO}$ (counted in slots) to the slave in the reserved master-to-slave slots. The SCO slave is always allowed to respond with an SCO packet in the following slave-to-master slot unless a different slave was addressed in the previous master-to-slave slot. If the SCO slave fails to decode the slave address in the packet header, it is still allowed to return an SCO packet in the reserved SCO slot.

The SCO link is established by the master sending an SCO setup message via the LM protocol. This message will contain timing parameters such as the SCO interval $T_{SCO}$ and the offset $D_{SCO}$ to specify the reserved slots.

In order to prevent clock wrap-around problems, an initialization flag in the LMP setup message indicates whether initialization procedure 1 or 2 is being used. The slave shall apply the initialization method as indicated by the initialization flag. The master uses initialization 1 when the MSB of the current master clock ($CLK_{27}$) is 0; it uses initialization 2 when the MSB of the current master clock ($CLK_{27}$) is 1. The master-to-slave SCO slots reserved by the master and the slave shall be initialized on the slots for which the clock satisfies the following equation:

**Bluetooth.**

$$CLK_{27-1} \bmod T_{SCO} = D_{SCO} \qquad \text{for initialization 1}$$

$$(\overline{CLK_{27}}, CLK_{26-1}) \bmod T_{SCO} = D_{SCO} \qquad \text{for initialization 2}$$

The slave-to-master SCO slots shall directly follow the reserved master-to-slave SCO slots. After initialization, the clock value CLK(k+1) for the next master-to-slave SCO slot is found by adding the fixed interval $T_{SCO}$ to the clock value of the current master-to-slave SCO slot:

$$CLK(k+1) = CLK(k) + T_{SCO}$$

## 3.3  ACL LINK

In the slots not reserved for SCO links, the master can exchange packets with any slave on a per-slot basis. The ACL link 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 link can exist. For most ACL packets, packet retransmission is applied to assure data integrity.

A slave is permitted to return an ACL packet in the slave-to-master slot if and only if it has been addressed in the preceding master-to-slave slot. If the slave fails to decode the slave address in the packet header, it is not allowed to transmit.

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

# 4 PACKETS

## 4.1 GENERAL FORMAT

The bit ordering when defining packets and messages in the *Baseband Specification*, follows the *Little Endian format*, i.e., the following rules apply:

- The *least significant bit* (LSB) corresponds to $b_0$;

- The LSB is the first bit sent over the air;

- In illustrations, the LSB is shown on the left side;

The baseband controller interprets the first bit arriving from a higher software layer as $b_0$; i.e. this is the first bit to be sent over the air. Furthermore, data fields generated internally at baseband level, such as the packet header fields and payload header length, are transmitted with the LSB first. For instance, a 3-bit parameter X=3 is sent as $b_0 b_1 b_2 = 110$ over the air where 1 is sent first and 0 is sent last.

The data on the piconet channel is conveyed in packets. The general packet format is shown in Figure 4.1 on page 47. Each packet consists of 3 entities: the access code, the header, and the payload. In the figure, the number of bits per entity is indicated.

| LSB   72 | 54 | 0 - 2745 | MSB |
|---|---|---|---|
| **ACCESS CODE** | **HEADER** | **PAYLOAD** | |
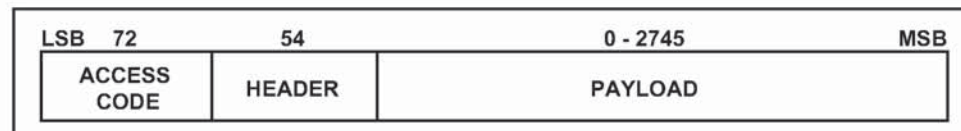
Figure 4.1: Standard packet format.

The access code and header are of fixed size: 72 bits and 54 bits respectively. The payload can range from zero to a maximum of 2745 bits. Different packet types have been defined. Packets may consist of the (shortened) access code only (see ID packet on page 55), of the access code – header, or of the access code – header – payload.

**Bluetooth.**

## 4.2  ACCESS CODE

Each packet starts with an access code. If a packet header follows, the access code is 72 bits long, otherwise the access code is 68 bits long. This access code is used for synchronization, DC offset compensation and identification. The access code identifies all packets exchanged on the channel of the piconet: all packets sent in the same piconet are preceded by the same channel access code. In the receiver of the Bluetooth unit, a sliding correlator correlates against the access code and triggers when a threshold is exceeded. This trigger signal is used to determine the receive timing.

The access code is also used in paging and inquiry procedures. In this case, the access code itself is used as a signalling message and neither a header nor a payload is present.

The access code consists of a preamble, a sync word, and possibly a trailer, see Figure 4.2 on page 48. For details see Section 4.2.1 on page 48.

| LSB  4 | 64 | 4  MSB |
|---|---|---|
| PREAMBLE | SYNC WORD | TRAILER |
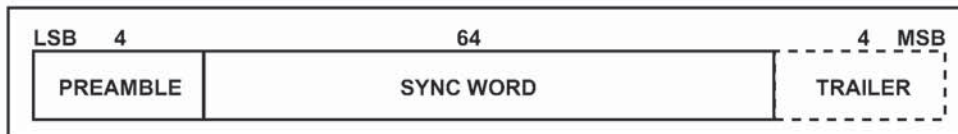
*Figure 4.2:  Access code format*

### 4.2.1 Access code types

There are three different types of access codes defined:

- Channel Access Code (CAC)

- Device Access Code (DAC)

- Inquiry Access Code (IAC)

The respective access code types are used for a Bluetooth unit in different operating modes. The channel access code identifies a piconet. This code is included in all packets exchanged on the piconet channel. The device access code is used for special signalling procedures, e.g., paging and response to paging. For the inquiry access code there are two variations. A general inquiry access code (GIAC) is common to all devices. The GIAC can be used to discover which other Bluetooth units are in range. The dedicated inquiry access code (DIAC) is common for a dedicated group of Bluetooth units that share a common characteristic. The DIAC can be used to discover only these dedicated Bluetooth units in range.

The CAC consists of a **preamble**, **sync word**, and **trailer** and its total length is 72 bits. When used as self-contained messages without a header, the DAC and IAC do not include the trailer bits and are of length 68 bits.

**Samsung Ex. 1019 p. 48**

The different access code types use different Lower Address Parts (LAPs) to construct the sync word. The LAP field of the BD address is explained in Section 13.1 on page 143. A summary of the different access code types can be found in Table 4.1 on page 49.

| Code type | LAP | Code length | Comments |
|---|---|---|---|
| CAC | Master | 72 | |
| DAC | Paged unit | 68/72* | See also Section 13.2 on page 143 |
| GIAC | Reserved | 68/72* | |
| DIAC | Dedicated | 68/72* | |

*Table 4.1: Summary of access code types.*

*. length 72 is only used in combination with FHS packets

### 4.2.2 Preamble

The preamble is a fixed zero-one pattern of 4 symbols used to facilitate DC compensation. The sequence is either 1010 or 0101, depending whether the LSB of the following sync word is 1 or 0, respectively. The preamble is shown in Figure 4.3 on page 49.



*Figure 4.3: Preamble*

### 4.2.3 Sync Word

The sync word is a 64-bit code word derived from a 24 bit address (LAP); for the CAC the master's LAP is used; for the GIAC and the DIAC, reserved, dedicated LAPs are used; for the DAC, the slave unit LAP is used. The construction guarantees large Hamming distance between sync words based on different LAPs. In addition, the good autocorrelation properties of the sync word improve on the timing synchronization process. The derivation of the sync word is described in Section 13.2 on page 143

### 4.2.4 Trailer

The trailer is appended to the sync word as soon as the packet header follows the access code. This is typically the case with the CAC, but the trailer is also used in the DAC and IAC when these codes are used in FHS packets exchanged during page response and inquiry response procedures.

The trailer is a fixed zero-one pattern of four symbols. The trailer together with the three MSBs of the syncword form a 7-bit pattern of alternating ones and zeroes which may be used for extended DC compensation. The trailer sequence is either 1010 or 0101 depending on whether the MSB of the sync word is 0 or 1, respectively. The choice of trailer is illustrated in Figure 4.4 on page 50.



Figure 4.4: Trailer in CAC when MSB of sync word is 0 (a), and when MSB of sync word is 1 (b).

**Bluetooth.**

## 4.3 PACKET HEADER

The header contains link control (LC) information and consists of 6 fields:

- AM_ADDR:        3- bit active member address
- TYPE:           4-bit type code
- FLOW:           1-bit flow control
- ARQN:           1-bit acknowledge indication
- SEQN:           1-bit sequence number
- HEC:            8-bit header error check

The total header, including the HEC, consists of 18 bits, see Figure 4.5 on page 51, and is encoded with a rate 1/3 FEC (not shown but described in Section 5.1 on page 67) resulting in a 54-bit header. Note that the AM_ADDR and TYPE fields are sent with their LSB first. The function of the different fields will be explained next.

| LSB 3 | 4 | 1 | 1 | 1 | 8 | MSB |
|---|---|---|---|---|---|---|
| AM_ADDR | TYPE | FLOW | ARQN | SEQN | HEC | |
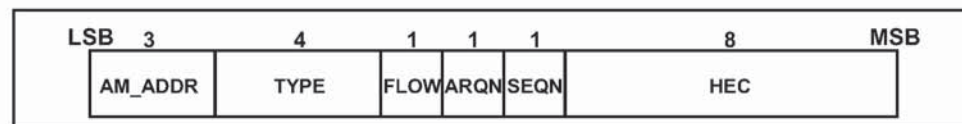
*Figure 4.5: Header format.*

### 4.3.1 AM_ADDR

The AM_ADDR represents a member address and is used to distinguish between the active members participating on the piconet. In a piconet, one or more slaves are connected to a single master. To identify each slave separately, each slave is assigned a temporary 3-bit address to be used when it is active. Packets exchanged between the master and the slave all carry the AM_ADDR of this slave; that is, the AM_ADDR of the slave is used in both master-to-slave packets and in the slave-to-master packets. The all-zero address is reserved for broadcasting packets from the master to the slaves. An exception is the FHS packet which may use the all-zero member address but is *not* a broadcast message (Section 4.4.1.4 on page 56). Slaves that are disconnected or parked give up their AM_ADDR. A new AM_ADDR has to be assigned when they re-enter the piconet.

### 4.3.2 TYPE

Sixteen different types of packets can be distinguished. The 4-bit TYPE code specifies which packet type is used. Important to note is that the interpretation of the TYPE code depends on the physical link type associated with the packet. First, it shall be determined whether the packet is sent on an SCO link or an ACL link. Then it can be determined which type of SCO packet or ACL packet has been received. The TYPE code also reveals how many slots the current packet will occupy. This allows the non-addressed receivers to refrain

**Bluetooth.**

from listening to the channel for the duration of the remaining slots. In Section 4.4 on page 54, each packet type will be described in more detail.

### 4.3.3 FLOW

This bit is used for flow control of packets over the ACL link. When the RX buffer for the ACL link in the recipient is full and is not emptied, a STOP indication (FLOW=0) is returned to stop the transmission of data temporarily. Note, that the STOP signal only concerns ACL packets. Packets including only link control information (ID, POLL and NULL packets) or SCO packets can still be received. When the RX buffer is empty, a GO indication (FLOW=1) is returned. When no packet is received, or the received header is in error, a GO is assumed implicitly.

### 4.3.4 ARQN

The 1-bit acknowledgment indication ARQN is used to inform the source of a successful transfer of payload data with CRC, and can be positive acknowledge ACK or negative acknowledge NAK. If the reception was successful, an ACK (ARQN=1) is returned, otherwise a NAK (ARQN=0) is returned. When no return message regarding acknowledge is received, a NAK is assumed implicitly. NAK is also the default return information.

The ARQN is piggy-backed in the header of the return packet. The success of the reception is checked by means of a cyclic redundancy check (CRC) code. An unnumbered ARQ scheme which means that the ARQN relates to the latest received packet from the same source, is used. See Section 5.3 on page 68 for initialization and usage of this bit.

### 4.3.5 SEQN

The SEQN bit provides a sequential numbering scheme to order the data packet stream. For each new transmitted packet that contains data with CRC, the SEQN bit is inverted. This is required to filter out retransmissions at the destination; if a retransmission occurs due to a failing ACK, the destination receives the same packet twice. By comparing the SEQN of consecutive packets, correctly received retransmissions can be discarded. The SEQN has to be added due to a lack of packet numbering in the unnumbered ARQ scheme. See section 5.3.2 on page 70 for initialization and usage of the SEQN bit. For broadcast packets, a modified sequencing method is used, see Section 5.3.5 on page 72.

### 4.3.6 HEC

Each header has a header-error-check to check the header integrity. The HEC consists of an 8-bit word generated by the polynomial 647 (octal representation). Before generating the HEC, the HEC generator is initialized with an 8-bit value. For FHS packets sent in **master page response** state, the slave upper

address part (UAP) is used. For FHS packets sent in **inquiry response**, the default check initialization (DCI, see Section 5.4) is used. In all other cases, the UAP of the master device is used. For the definition of Bluetooth device addresses, see Section 13.1 on page 143.

After the initialization, a HEC is calculated for the 10 header bits. Before checking the HEC, the receiver must initialize the HEC check circuitry with the proper 8-bit UAP (or DCI). If the HEC does not check, the entire packet is disregarded. More information can be found in Section 5.4 on page 73.

AFFLT0293281

**Samsung Ex. 1019 p. 53**

**Bluetooth.**

## 4.4  PACKET TYPES

The packets used on the piconet are related to the physical links they are used in. Up to now, two physical links are defined: the SCO link and the ACL link. For each of these links, 12 different packet types can be defined. Four control packets will be common to all link types: their TYPE code is unique irrespective of the link type.

To indicate the different packets on a link, the 4-bit TYPE code is used. The packet types have been divided into four segments. The first segment is reserved for the four control packets common to all physical link types; all four packet types have been defined. The second segment is reserved for packets occupying a single time slot; six packet types have been defined. The third segment is reserved for packets occupying three time slots; two packet types have been defined. The fourth segment is reserved for packets occupying five time slots; two packet types have been defined. The slot occupancy is reflected in the segmentation and can directly be derived from the type code. Table 4.2 on page 54 summarizes the packets defined so far for the SCO and ACL link types.

| Segment | TYPE code $b_3b_2b_1b_0$ | Slot occupancy | SCO link | ACL link |
|---------|--------------------------|----------------|----------|----------|
| 1 | 0000 | 1 | NULL | NULL |
|   | 0001 | 1 | POLL | POLL |
|   | 0010 | 1 | FHS | FHS |
|   | 0011 | 1 | DM1 | DM1 |
| 2 | 0100 | 1 | undefined | DH1 |
|   | 0101 | 1 | HV1 | undefined |
|   | 0110 | 1 | HV2 | undefined |
|   | 0111 | 1 | HV3 | undefined |
|   | 1000 | 1 | DV | undefined |
|   | 1001 | 1 | undefined | AUX1 |
| 3 | 1010 | 3 | undefined | DM3 |
|   | 1011 | 3 | undefined | DH3 |
|   | 1100 | 3 | undefined | undefined |
|   | 1101 | 3 | undefined | undefined |
| 4 | 1110 | 5 | undefined | DM5 |
|   | 1111 | 5 | undefined | DH5 |

Table 4.2:  *Packets defined for SCO and ACL link types*

**Bluetooth.**

### 4.4.1 Common packet types

There are five common packets. In addition to the types listed in segment 1 of the previous table, there is the ID packet not listed. Each packet will now be examined in more detail.

#### 4.4.1.1 ID packet

The identity or ID packet consists of the device access code (DAC) or inquiry access code (IAC). It has a fixed length of 68 bits. It is a very robust packet since the receiver uses a bit correlator to match the received packet to the known bit sequence of the ID packet. The packet is used, for example, in paging, inquiry, and response routines.

#### 4.4.1.2 NULL packet

The NULL packet has no payload and therefore consists of the channel access code and packet header only. Its total (fixed) length is 126 bits. The NULL packet is used to return link information to the source regarding the success of the previous transmission (ARQN), or the status of the RX buffer (FLOW). The NULL packet itself does not have to be acknowledged.

#### 4.4.1.3 POLL packet

The POLL packet is very similar to the NULL packet. It does not have a payload either. In contrast to the NULL packet, it requires a confirmation from the recipient. It is not a part of the ARQ scheme. The POLL packet does not affect the ARQN and SEQN fields. Upon reception of a POLL packet the slave must respond with a packet. This return packet is an implicit acknowledgement of the POLL packet. This packet can be used by the master in a piconet to poll the slaves, which must then respond even if they do not have information to send.

**Samsung Ex. 1019 p. 55**

**Bluetooth.**

### 4.4.1.4 FHS packet

The FHS packet is a special control packet revealing, among other things, the Bluetooth device address and the clock of the sender. The payload contains 144 information bits plus a 16-bit CRC code. The payload is coded with a rate 2/3 FEC which brings the gross payload length to 240 bits. The FHS packet covers a single time slot.

Figure 4.6 on page 56 illustrates the format and contents of the FHS payload. The payload consists of eleven fields. The FHS packet is used in page master response, inquiry response and in master slave switch. In page master response or master slave switch, it is retransmitted until its reception is acknowledged or a timeout has exceeded. In inquiry response, the FHS packet is not acknowledged. The FHS packet contains real-time clock information. This clock information is updated before each retransmission. The retransmission of the FHS payload is thus somewhat different from the retransmission of ordinary data payloads where the same payload is used for each retransmission. The FHS packet is used for frequency hop synchronization before the piconet channel has been established, or when an existing piconet changes to a new piconet. In the former case, the recipient has not been assigned an active member address yet, in which case the AM_ADDR field in the FHS packet header is set to all-zeroes; however, the FHS packet should not be considered as a broadcast packet. In the latter case the slave already has an AM_ADDR in the existing piconet, which is then used in the FHS packet header.

| LSB | | | | | | | | | | MSB |
|---|---|---|---|---|---|---|---|---|---|---|
| 34 | 24 | 2 | 2 | 2 | 8 | 16 | 24 | 3 | 26 | 3 |
| Parity bits | LAP | Un-defined | SR | SP | UAP | NAP | Class of device | AM_ADDR | $CLK_{27-2}$ | Page scan mode |
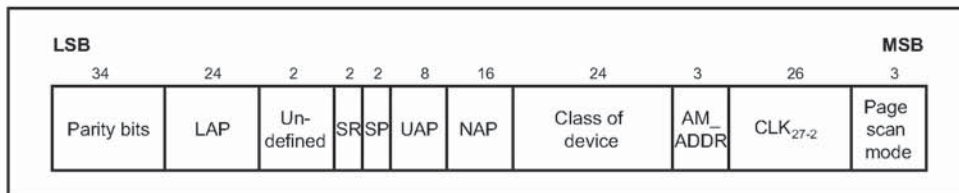
*Figure 4.6: Format of the FHS payload*

Each field is described in more detail below:

| Parity bits | This 34-bit field contains the parity bits that form the first part of the sync word of the access code of the unit that sends the FHS packet. These bits are derived from the LAP as described in section 13.2 on page 143. |
|---|---|
| LAP | This 24-bit field contains the lower address part of the unit that sends the FHS packet. |
| Undefined | This 2-bit field is reserved for future use and shall be set to zero. |
| SR | This 2-bit field is the scan repetition field and indicates the interval between two consecutive page scan windows, see also Table 4.4 and Table 10.1 on page 101 |

*Table 4.3: Description of the FHS payload*

**Bluetooth.**

| | |
|---|---|
| **SP** | This 2-bit field is the scan period field and indicates the period in which the mandatory page scan mode is applied after transmission of an inquiry response message, see also Table 4.5 and Table 10.6 on page 112. |
| **UAP** | This 8-bit field contains the upper address part of the unit that sends the FHS packet. |
| **NAP** | This 16-bit field contains the non-significant address part of the unit that sends the FHS packet (see also section 13.1 on page 143 for LAP, UAP, and NAP). |
| **Class of device** | This 24-bit field contains the class of device of the unit that sends the FHS packet. The class of device has not been defined yet. |
| **AM_ADDR** | This 3-bit field contains the member address the recipient shall use if the FHS packet is used at call setup or master-slave switch. A slave responding to a master or a unit responding to an inquiry request message shall include an all-zero AM_ADDR field if it sends the FHS packet. |
| **$CLK_{27-2}$** | This 26-bit field contains the value of the native system clock of the unit that sends the FHS packet, sampled at the beginning of the transmission of the access code of this FHS packet. This clock value has a resolution of 1.25ms (two-slot interval). For each new transmission, this field is updated so that it accurately reflects the real-time clock value. |
| **Page scan mode** | This 3-bit field indicates which scan mode is used by default by the sender of the FHS packet. The interpretation of the page scan mode is illustrated in Table 4.6. Currently, the standard supports one mandatory scan mode and up to three optional scan modes (see also "Appendix VII" on page 999). |

Table 4.3: Description of the FHS payload

| SR bit format $b_1b_0$ | SR mode |
|---|---|
| 00 | R0 |
| 01 | R1 |
| 10 | R2 |
| 11 | reserved |

Table 4.4: Contents of SR field

| SP bit format $b_1b_0$ | SP mode |
|---|---|
| 00 | P0 |
| 01 | P1 |
| 10 | P2 |
| 11 | reserved |

Table 4.5: Contents of SP field

| Bit format $b_2 b_1 b_0$ | Page scan mode |
|---|---|
| 000 | Mandatory scan mode |
| 001 | Optional scan mode I |
| 010 | Optional scan mode II |
| 011 | Optional scan mode III |
| 100 | Reserved for future use |
| 101 | Reserved for future use |
| 110 | Reserved for future use |
| 111 | Reserved for future use |

*Table 4.6: Contents of page scan mode field*

The LAP, UAP, and NAP together form the 48-bit IEEE address of the unit that sends the FHS packet. Using the parity bits and the LAP, the recipient can directly construct the channel access code of the sender of the FHS packet.

### 4.4.1.5 DM1 packet

DM1 serves as part of segment 1 in order to support control messages in any link type. However, it can also carry regular user data. Since the DM1 packet is recognized on the SCO link, it can interrupt the synchronous information to send control information. Since the DM1 packet can be regarded as an ACL packet, it will be discussed in .

### 4.4.2 SCO packets

SCO packets are used on the synchronous SCO link. The packets do not include a CRC and are never retransmitted. SCO packets are routed to the synchronous I/O (voice) port. Up to now, three pure SCO packets have been defined. In addition, an SCO packet is defined which carries an asynchronous data field in addition to a synchronous (voice) field. The SCO packets defined so far are typically used for 64 kb/s speech transmission.

### 4.4.2.1 HV1 packet

The **HV1** packet carries 10 information bytes. The bytes are protected with a rate 1/3 FEC. No CRC is present. The payload length is fixed at 240 bits. There is no payload header present.

HV packets are typically used for voice transmission. HV stands for High-quality Voice. The voice packets are never retransmitted and need no CRC.

An HV1 packet can carry 1.25ms of speech at a 64 kb/s rate. In that case, an HV1 packet has to be sent every two time slots ($T_{SCO}$=2).

### 4.4.2.2 HV2 packet

The **HV2** packet carries 20 information bytes. The bytes are protected with a rate 2/3 FEC. No CRC is present. The payload length is fixed at 240 bits. There is no payload header present.

If the HV2 packet is used for voice at a 64 kb/s rate, it can carry 2.5ms of speech. In that case, an HV2 packet has to be sent every four time slots ($T_{SCO}$=4).

### 4.4.2.3 HV3 packet

The **HV3** packet carries 30 information bytes. The bytes are not protected by FEC. No CRC is present. The payload length is fixed at 240 bits. There is no payload header present.

If the HV3 packet is used for voice at a 64 kb/s rate, it can carry 3.75ms of speech. In that case, an HV3 packet has to be sent every six time slots ($T_{SCO}$=6).

### 4.4.2.4 DV packet

The **DV** packet is a combined data - voice packet. The payload is divided into a voice field of 80 bits and a data field containing up to 150 bits, see Figure 4.7. The voice field is not protected by FEC. The data field contains up to 10 information bytes (including the 1-byte payload header) and includes a 16-bit CRC. The data field is encoded with a rate 2/3 FEC. If necessary, extra zeroes are appended to assure that the total number of payload bits is a multiple of 10 prior to FEC encoding. Since the **DV** packet has to be sent at regular intervals due to its synchronous (voice) contents, it is listed under the SCO packet types. The voice and data fields are treated completely separate. The voice field is handled like normal SCO data and is never retransmitted; that is, the voice field is always new. The data field is checked for errors and is retransmitted if necessary.

| LSB 72 | 54 | 80 | 32 - 150 MSB |
|---|---|---|---|
| ACCESS CODE | HEADER | VOICE FIELD | DATA FIELD |
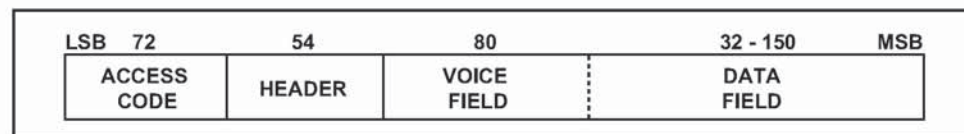
*Figure 4.7: DV packet format*

**Bluetooth.**

### 4.4.3 ACL packets

ACL packets are used on the asynchronous links. The information carried can be user data or control data. Including the DM1 packet, seven ACL packets have been defined. Six of the ACL packets contain a CRC code and retransmission is applied if no acknowledgement of proper reception is received (except in case a flush operation is carried out, see Section 5.3.3 on page 71). The 7th ACL packet, the AUX1 packet, has no CRC and is not retransmitted.

#### 4.4.3.1 DM1 packet

The DM1 packet is a packet that carries data information only. DM stands for Data – Medium rate. The payload contains up to 18 information bytes (including the 1-byte payload header) plus a 16-bit CRC code. The DM1 packet may cover up to a single time slot. The information plus CRC bits are coded with a rate 2/3 FEC which adds 5 parity bits to every 10-bit segment. If necessary, extra zeros are appended after the CRC bits to get the total number of bits (information bits, CRC bits, and tail bits) equal a multiple of 10. The payload header in the DM1 packet is only 1 byte long, see Figure 4.8 on page 62. The length indicator in the payload header specifies the number of user bytes (excluding payload header and the CRC code).

#### 4.4.3.2 DH1 packet

This packet is similar to the DM1 packet, except that the information in the payload is not FEC encoded. As a result, the DH1 packet can carry up to 28 information bytes plus a 16-bit CRC code. DH stands for Data – High rate. The DH1 packet may cover up to a single time slot.

#### 4.4.3.3 DM3 packet

The DM3 packet is a DM1 packet with an extended payload. The DM3 packet may cover up to three time slots. The payload contains up to 123 information bytes (including the 2-bytes payload header) plus a 16-bit CRC code. The payload header in the DM3 packet is 2 bytes long, see Figure 4.9 on page 62. The length indicator in the payload header specifies the number of user bytes (excluding payload header and the CRC code). When a DM3 packet is sent or received, the RF hop frequency shall not change for a duration of three time slots (the first time slot being the slot where the channel access code was transmitted).

#### 4.4.3.4 DH3 packet

This packet is similar to the DM3 packet, except that the information in the payload is not FEC encoded. As a result, the DH3 packet can carry up to 185 information bytes (including the two bytes payload header) plus a 16-bit CRC code.

The DH3 packet may cover three time slots. When a DH3 packet is sent or received, the hop frequency shall not change for a duration of three time slots (the first time slot being the slot where the channel access code was transmitted).

### 4.4.3.5 DM5 packet

The DM5 packet is a DM1 packet with an extended payload. The DM5 packet may cover up to five time slots. The payload contains up to 226 information bytes (including the 2-bytes payload header) plus a 16-bit CRC code. The payload header in the DM5 packet is 2 bytes long. The length indicator in the payload header specifies the number of user bytes (excluding payload header and the CRC code). When a DM5 packet is sent or received, the hop frequency shall not change for a duration of five time slots (the first time slot being the slot where the channel access code was transmitted).

### 4.4.3.6 DH5 packet

This packet is similar to the DM5 packet, except that the information in the payload is not FEC encoded. As a result, the DH5 packet can carry up to 341 information bytes (including the two bytes payload header) plus a 16-bit CRC code. The DH5 packet may cover five time slots. When a DH5 packet is sent or received, the hop frequency shall not change for a duration of five time slots (the first time slot being the slot where the channel access code was transmitted).

### 4.4.3.7 AUX1 packet

This packet resembles a DH1 packet but has no CRC code. The AUX1 packet can carry up to 30 information bytes (including the 1-byte payload header). The AUX1 packet may cover up to a single time slot.

## 4.5  PAYLOAD FORMAT

In the previous packet overview, several payload formats were considered. In the payload, two fields are distinguished: the (synchronous) voice field and the (asynchronous) data field. The ACL packets only have the data field and the SCO packets only have the voice field – with the exception of the DV packets which have both.

### 4.5.1  Voice field

The voice field has a fixed length. For the HV packets, the voice field length is 240 bits; for the DV packet the voice field length is 80 bits. No payload header is present.

### 4.5.2  Data field

The data field consists of three segments: a payload header, a payload body, and possibly a CRC code (only the AUX1 packet does not carry a CRC code).

**1. Payload header**

Only data fields have a payload header. The payload header is one or two bytes long. Packets in segments one and two have a 1-byte payload header; packets in segments three and four have a 2-bytes payload header. The payload header specifies the logical channel (2-bit L_CH indication), controls the flow on the logical channels (1-bit FLOW indication), and has a payload length indicator (5 bits and 9 bits for 1-byte and 2-bytes payload header, respectively). In the case of a 2-byte payload header, the length indicator is extended by four bits into the next byte. The remaining four bits of the second byte are reserved for future use and shall be set to zero. The formats of the 1-byte and 2-bytes payload headers are shown in Figure 4.8 on page 62 and Figure 4.9 on page 62.
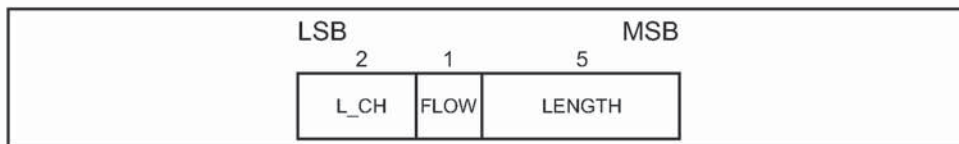


*Figure 4.8: Payload header format for single-slot packets.*
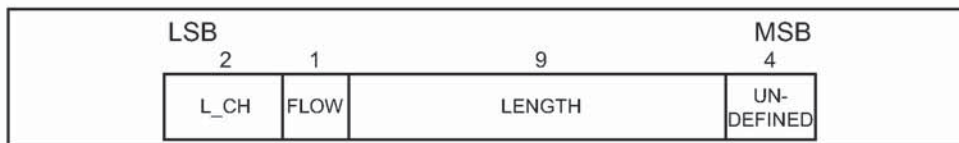


*Figure 4.9: Payload header format for multi-slot packets.*

The L_CH field is transmitted first, the length field last. In Table 4.7 on page 63, more details about the contents of the L_CH field are listed.

| L_CH code $b_1b_0$ | Logical Channel | Information |
|---|---|---|
| 00 | NA | undefined |
| 01 | UA/UI | Continuation fragment of an L2CAP message |
| 10 | UA/UI | Start of an L2CAP message or no fragmentation |
| 11 | LM | LMP message |

*Table 4.7: Logical channel L_CH field contents*

An L2CAP message can be fragmented into several packets. Code 10 is used for an L2CAP packet carrying the first fragment of such a message; code 01 is used for continuing fragments. If there is no fragmentation, code 10 is used for every packet. Code 11 is used for LMP messages. Code 00 is reserved for future use.

The flow indicator in the payload is used to control the flow at the L2CAP level. It is used to control the flow per logical channel (when applicable). FLOW=1 means flow-on ("OK to send") and FLOW=0 means flow-off ("stop"). There are no strict real-time requirements on the flow bit in the payload header. Flow bit in the last correctly received payload header determines flow status. The link manager is responsible for setting and processing the flow bit in the payload header. Real-time flow control is carried out at the packet level by the link controller via the flow bit in the packet header (see Section 4.3.3 on page 52). With the payload flow bit, traffic from the remote end can be controlled. It is allowed to generate and send an ACL packet with payload load length zero. L2CAP start- and continue-fragment indications (L_CH=10 and L_CH=01) also retain their meaning when the payload length is equal to zero (i.e. an empty start-fragment should not be sent in the middle of an on-going L2CAP packet transmission). It is always safe to send an ACL packet with payload length=0 and L_CH=10. The payload flow bit has its own meaning for each logical channel (UA/I or LM), see Table 4.8 on page 63. On the LM channel, no flow control is applied and the payload flow bit is always set at one.

| L_CH code $b_1b_0$ | Usage and semantics of the ACL payload header FLOW bit |
|---|---|
| 00 | Not defined, reserved for future use. |
| 01 or 10 | Flow control of the UA/I channels (which are used to send L2CAP messages) |
| 11 | Always set FLOW=1 on transmission and ignore the bit on reception |

*Table 4.8: Use of payload header flow bit on the logical channels.*

The length indicator indicates the number of bytes (i.e. 8-bit words) in the payload excluding the payload header and the CRC code; i.e. the payload body only. With reference to Figure 4.8 and Figure 4.9, the MSB of the length field in a 1-byte header is the last (right-most) bit in the payload

header; the MSB of the length field in a 2-byte header is the fourth bit (from left) of the second byte in the payload header.

### 2. Payload body

The payload body includes the user host information and determines the effective user throughput. The length of the payload body is indicated in the length field of the payload header.

### 3. CRC code generation

The 16-bit cyclic redundancy check code in the payload is generated by the CRC-CCITT polynomial `210041` (octal representation). It is generated in a way similar to the HEC. Before determining the CRC code, an 8-bit value is used to initialize the CRC generator. For the CRC code in the FHS packets sent in **master page response** state, the UAP of the slave is used. For the FHS packet sent in **inquiry response** state, the DCI (see Section 5.4) is used. For all other packets, the UAP of the master is used.

The 8 bits are loaded into the 8 least significant (left-most) positions of the LFSR circuit, see Figure 5.10 on page 76. The other 8 bits are at the same time reset to zero. Subsequently, the CRC code is calculated over the information. Then the CRC code is appended to the information; the UAP (or DCI) is disregarded. At the receive side, the CRC circuitry is in the same way initialized with the 8-bit UAP (DCI) before the received information is checked. More information can be found in Section 5.4 on page 73.

## 4.6 PACKET SUMMARY

A summary of the packets and their characteristics is shown in Table 4.9, Table 4.10 and Table 4.11. The user payload represents the packet payload excluding FEC, CRC, and payload header.

| Type | User Payload (bytes) | FEC | CRC | Symmetric Max. Rate | Asymmetric Max. Rate |
|------|----------------------|-----|-----|---------------------|----------------------|
| ID   | na | na | na | na | na |
| NULL | na | na | na | na | na |
| POLL | na | na | na | na | na |
| FHS  | 18 | 2/3 | yes | na | na |

Table 4.9: Link control packets

| Type | Payload Header (bytes) | User Payload (bytes) | FEC | CRC | Symmetric Max. Rate (kb/s) | Asymmetric Max. Rate (kb/s) | |
|------|------------------------|----------------------|-----|-----|----------------------------|-------------|---------|
| | | | | | | Forward | Reverse |
| DM1  | 1 | 0-17 | 2/3 | yes | 108.8 | 108.8 | 108.8 |
| DH1  | 1 | 0-27 | no | yes | 172.8 | 172.8 | 172.8 |
| DM3  | 2 | 0-121 | 2/3 | yes | 258.1 | 387.2 | 54.4 |
| DH3  | 2 | 0-183 | no | yes | 390.4 | 585.6 | 86.4 |
| DM5  | 2 | 0-224 | 2/3 | yes | 286.7 | 477.8 | 36.3 |
| DH5  | 2 | 0-339 | no | yes | 433.9 | 723.2 | 57.6 |
| AUX1 | 1 | 0-29 | no | no | 185.6 | 185.6 | 185.6 |

Table 4.10: ACL packets

| Type | Payload Header (bytes) | User Payload (bytes) | FEC | CRC | Symmetric Max. Rate (kb/s) |
|------|------------------------|----------------------|-----|-----|----------------------------|
| HV1  | na | 10 | 1/3 | no | 64.0 |
| HV2  | na | 20 | 2/3 | no | 64.0 |
| HV3  | na | 30 | no | no | 64.0 |
| DV*  | 1 D | 10+(0-9) D | 2/3 D | yes D | 64.0+57.6 D |

Table 4.11: SCO packets

*. Items followed by 'D' relate to data field only.

**Bluetooth.**

# 5 ERROR CORRECTION

There are three error correction schemes defined for Bluetooth:

- 1/3 rate FEC
- 2/3 rate FEC
- ARQ scheme for the data

The purpose of the FEC scheme on the data payload is to reduce the number of retransmissions. However, in a reasonable error-free environment, FEC gives unnecessary overhead that reduces the throughput. Therefore, the packet definitions given in Section 4 have been kept flexible to use FEC in the payload or not, resulting in the **DM** and **DH** packets for the ACL link and the **HV** packets for the SCO link. The packet header is always protected by a 1/3 rate FEC; it contains valuable link information and should be able to sustain more bit errors.

Correction measures to mask errors in the voice decoder are not included in this section. This matter is discussed in section Section 12.3 on page 142.

## 5.1 FEC CODE: RATE 1/3

A simple 3-times repetition FEC code is used for the header. The repetition code is implemented by repeating the bit three times, see the illustration in Figure 5.1 on page 67. The 3-bit repetition code is used for the entire header, and also for the voice field in the **HV1** packet.
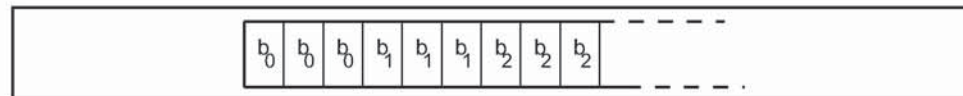


*Figure 5.1: Bit-repetition encoding scheme.*

## 5.2 FEC CODE: RATE 2/3

The other FEC scheme is a (15,10) shortened Hamming code. The generator polynomial is $g(D) = (D+1)(D^4+D+1)$. This corresponds to 65 in octal notation. The LFSR generating this code is depicted in Figure 5.2 on page 68. Initially all register elements are set to zero. The 10 information bits are sequentially fed into the LFSR with the switches S1 and S2 set in position 1. Then, after the final input bit, the switches S1 and S2 are set in position 2, and the five parity bits are shifted out. The parity bits are appended to the information bits. Consequently, each block of 10 information bits is encoded into a 15 bit codeword. This code can correct all single errors and detect all double errors in each codeword. This 2/3 rate FEC is used in the **DM** packets, in the data field of the **DV** packet, in the **FHS** packet, and in the **HV2** packet. Since the encoder operates with information segments of length 10, tail bits with

value zero may have to be appended after the CRC bits. The total number of bits to encode, i.e., payload header, user data, CRC, and tail bits, must be a multiple of 10. Thus, the number of tail bits to append is the least possible that achieves this (i.e., in the interval 0...9). These tail bits are not included in the payload length indicator.



*Figure 5.2: LFSR generating the (15,10) shortened Hamming code.*

## 5.3  ARQ SCHEME

With an automatic repeat request scheme, **DM, DH** and the data field of **DV** packets are transmitted and retransmitted until acknowledgement of a successful reception is returned by the destination (or timeout is exceeded). The acknowledgement information is included in the header of the return packet, so-called piggy-backing. To determine whether the payload is correct or not, a cyclic redundancy check (CRC) code is added to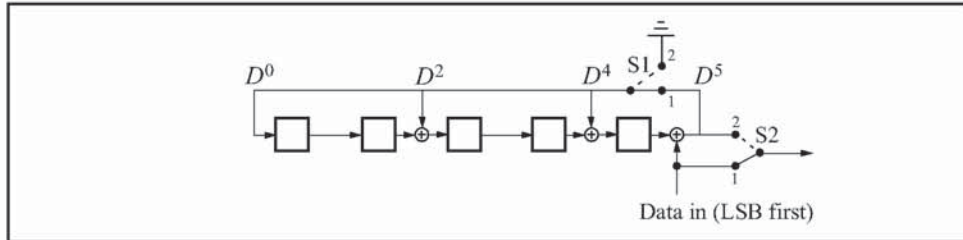 the packet. The ARQ scheme only works on the payload in the packet (only that payload which has a CRC). The packet header and the voice payload are not protected by the ARQ scheme.

### 5.3.1  Unnumbered ARQ

Bluetooth uses a fast, unnumbered acknowledgment scheme: an ACK (ARQN=1) or a NAK (ARQN=0) is returned in response to the receipt of previously received packet. The slave will respond in the slave-to-master slot directly following the master-to-slave slot; the master will respond at the next event it will address the same slave (the master may have addressed other slaves between the last received packet from the considered slave and the master response to this packet). For a packet reception to be successful, at least the HEC must check. In addition, the CRC must check if present.

At the start of a new connection which may be the result of a page, page scan, master-slave switch or unpark, the master sends a POLL packet to verify the connection. In this packet the master initializes the ARQN bit to NAK. The response packet sent by the slave also has the ARQN bit set to NAK. The subsequent packets use the following rules.

The ARQ bit is affected by data packets containing CRC and empty slots only. As shown in Fig. 5.3 on page 70, upon successful reception of a CRC packet, the ARQN bit is set to ACK. If, in any receive slot in the slave or in a receive

slot following transmission of a packet in the master, no access code is detected, and the HEC check or the CRC check of a CRC packet fails, then the ARQN bit is set to NAK. Packets that have correct HEC but that are addressed to other slaves, or packets other than DH, DM, or DV packets, do not affect the ARQN bit. In these cases the ARQN bit is left as it was prior to reception of the packet. If a CRC packet with a correct header has the same SEQN as the previously received CRC packet, the ARQN bit is set to ACK and the payload is disregarded without checking the CRC.

The ARQ bit in the FHS packet is not meaningful. Contents of the ARQN bit in the FHS packet should not be checked.

Broadcast packets are checked on errors using the CRC, but no ARQ scheme is applied. Broadcast packets are never acknowledged.

Inactive connection modes HOLD and SNIFF do not affect the ARQN scheme. After return from these modes, packets will continue using values from before the start of hold/sniff modes.

**Bluetooth.**
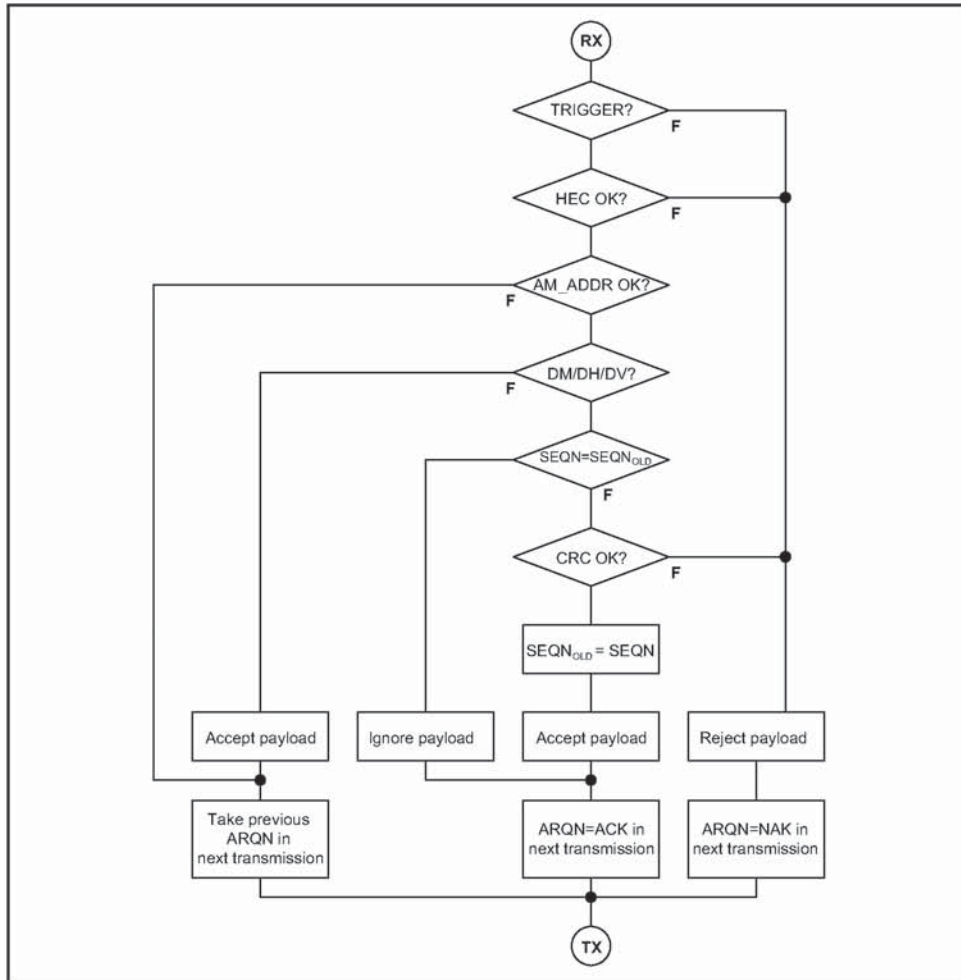


*Figure 5.3: Receive protocol for determining the ARQN bit.*

## 5.3.2 Retransmit filtering

The data payload is retransmitted until a positive acknowledgment is received (or a timeout is exceeded). A retransmission is carried out either because the packet transmission itself failed, or because the piggy-backed acknowledgment transmitted in the return packet failed (note that the latter has a lower failure probability since the header is more heavily coded). In the latter case, the destination keeps receiving the same payload over and over again. In order to filter out the retransmissions in the destination, the SEQN bit is added in the header. Normally, this bit is alternated for every new CRC data payload transmission. In case of a retransmission, this bit is not changed. So the destination can compare the SEQN bit with the previous SEQN value. If different, a new data payload has arrived; otherwise it is the same data payload and can be discarded. Only new data payloads are transferred to the link manager. Note that CRC data payloads can be carried only by **DM, DH** or **DV** packets.

**Bluetooth.**

At the start of a new connection which may be the result of a page, page scan, master slave switch or unpark, the master sends a POLL packet to verify the connection. The slave responds with a packet. The SEQN bit of the first CRC data packet, on both the master and the slave sides, is set to 1. The subsequent packets use the rules given below.

The SEQN bit is affected only by the CRC data packets as shown in Figure 5.4. It is inverted every time a new CRC data packet is sent. The CRC data packet is retransmitted with the same SEQN number until an ACK is received or the packet is flushed. When an ACK is received, the SEQN bit is inverted and a new payload is sent. When the packet is flushed (see Section 5.3.3 on page 71), a new payload is sent. The SEQN bit is not necessarily inverted. However, if an ACK is received before the new packet is sent, the SEQN bit is inverted. This procedure prevents loss of the first packet of a message (after the **flush** command has been given) due to the retransmit filtering.
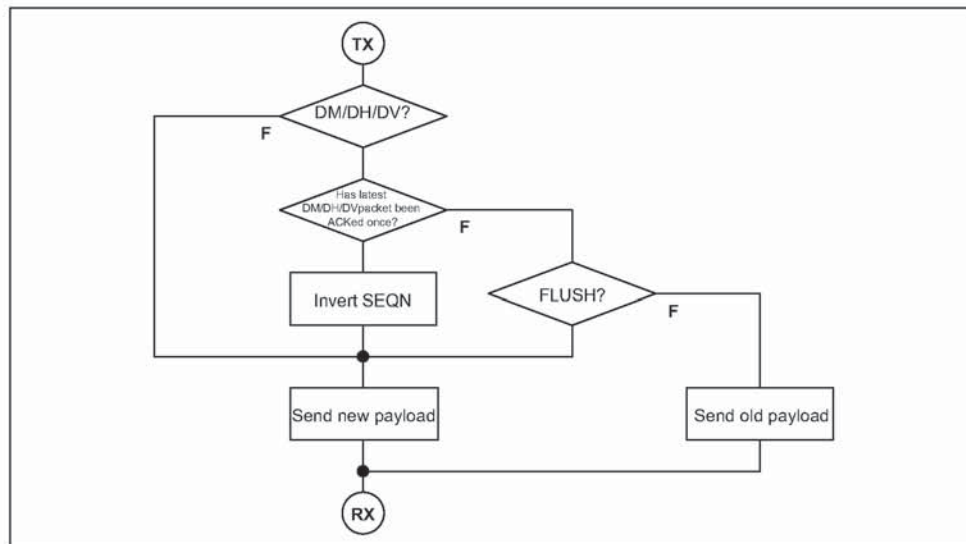


*Figure 5.4: Retransmit filtering for packets with CRC.*

The SEQN bit in the FHS packet is not meaningful. This bit can be set to any value. Contents of the SEQN bit in the FHS packet should not be checked. During transmission of all other packets the SEQN bit remains the same as it was in the previous packet.

Inactive connection modes HOLD and SNIFF do not affect the SEQN scheme. After return from these modes, packets will continue using values from before the start of hold/sniff modes.

### 5.3.3  Flushing payloads

The ARQ scheme can cause variable delay in the traffic flow since retransmissions are inserted to assure error-free data transfer. For certain communication

links, only a limited amount of delay is allowed: retransmissions are allowed up to a certain limit at which the current payload must be disregarded and the next payload must be considered. This data transfer is indicated as **isochronous traffic**. This means that the retransmit process must be overruled in order to continue with the next data payload. Aborting the retransmit scheme is accomplished by *flushing* the old data and forcing the Bluetooth controller to take the next data instead.

Flushing results in loss of remaining portions of an L2CAP message. Therefore, the packet following the flush will have a start packet indication of L_CH = 10 in the payload header for the next L2CAP message. This informs the destination of the flush. (see Section 4.5). Flushing will not necessarily result in a change in the SEQN bit value, see the previous section.

### 5.3.4 Multi-slave considerations

In case of a piconet with multiple slaves, the master carries out the ARQ protocol independently to each slave.

### 5.3.5 Broadcast packets

Broadcast packets are packets transmitted by the master to all the slaves simultaneously. A broadcast packet is indicated by the all-zero AM_ADDR (note; the FHS packet is the only packet which may have an all-zero address but is not a broadcast packet). Broadcast packets are not acknowledged (at least not at the LC level).

Since broadcast messages are not acknowledged, each broadcast packet is repeated for a fixed number of times. A broadcast packet is repeated $N_{BC}$ times before the next broadcast packet of the same broadcast message is repeated, see Figure 5.5 on page 73.

Broadcast packets with a CRC have their own sequence number. The SEQN of the first broadcast packet with a CRC is set to SEQN = 1 by the master and it is inverted for each new broadcast packet with CRC thereafter. Broadcast packets without a CRC have no influence on the sequence number. The slave accepts the SEQN of the first broadcast packet it receives in a connection and checks for change in SEQN for consequent broadcast packets. Since there is no acknowledgement of broadcast messages and there is no end packet indication, it is important to receive the start packets correctly. To ensure this, repetitions of the broadcast packets that are L2CAP start packets and LMP packets will not be filtered out. These packets are indicated by L_CH=1X in the payload header as explained in section 4.5 on page 62. Only repetitions of the L2CAP continuation packets will be filtered out.
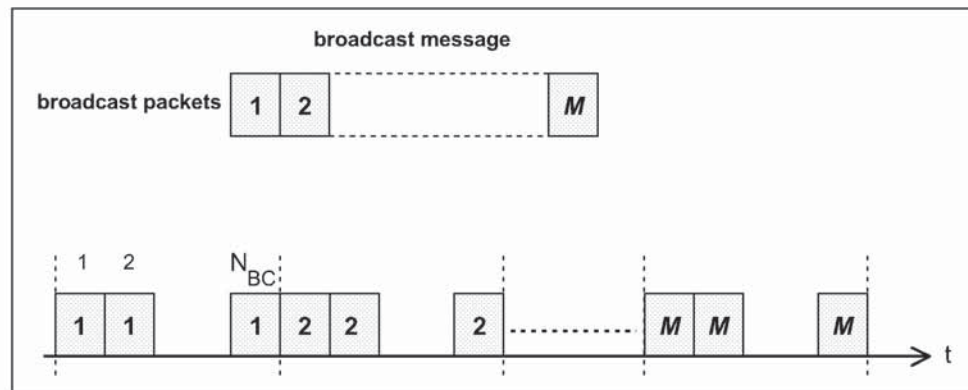
**Samsung Ex. 1019 p. 72**

*Figure 5.5: Broadcast repetition scheme*

## 5.4 ERROR CHECKING

We can check the packet for errors or wrong delivery using the channel access code, the HEC in the header, and the CRC in the payload. At packet reception, first the access code is checked. Since the 64-bit sync word in the channel access code is derived from the 24-bit master LAP, this checks if the LAP is correct, and prevents the receiver from accepting a packet of another piconet.

The HEC and CRC are used to check both on errors and on a wrong address: to increase the address space with 8 bits, the UAP is normally included in the HEC and CRC checks. Then, even when a packet with the same access code – i.e., an access code of a device owning the same LAP but different UAP – passes the access code test, it will be discarded after the HEC and CRC tests when the UAP bits do not match. However, there is an exception where no common UAP is available in the transmitter and receiver. This is the case when the HEC and CRC are generated for the FHS packet in **inquiry response** state. In this case the default check initialization (DCI) value is used. The DCI is defined to be 0x00 (hexadecimal).

The generation and check of the HEC and CRC are summarized in Figure 5.8 on page 75 and Figure 5.11 on page 76. Before calculating the HEC or CRC, the shift registers in the HEC/CRC generators are initialized with the 8-bit UAP (or DCI) value. Then the header and payload information is shifted into the HEC and CRC generators, respectively (with the LSB first).

The HEC generating LFSR is depicted in Figure 5.6 on page 74. The generator polynomial is $g(D) = (D+1)(D^7 + D^4 + D^3 + D^2 + 1) = D^8 + D^7 + D^5 + D^2 + D + 1$ . Initially this circuit is pre-loaded with the 8-bit UAP such that the LSB of the UAP (denoted $UAP_0$) goes to the left-most shift register element, and, $UAP_7$ goes to the right-most element. The initial state of the HEC LFSR is depicted in Figure 5.7 on page 75. Then the data is shifted in with the switch S set in position 1. When the last data bit has been clocked into the LFSR, the switch S is set in position 2, and, the HEC can be read out from the register. The LFSR bits

are read out from right to left (i.e., the bit in position 7 is the first to be transmitted, followed by the bit in position 6, etc.).
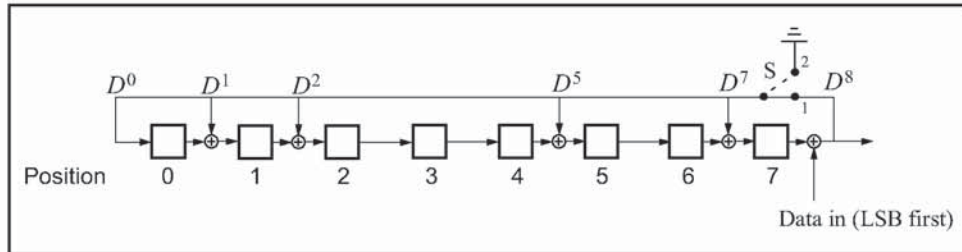


*Figure 5.6: The LFSR circuit generating the HEC.*
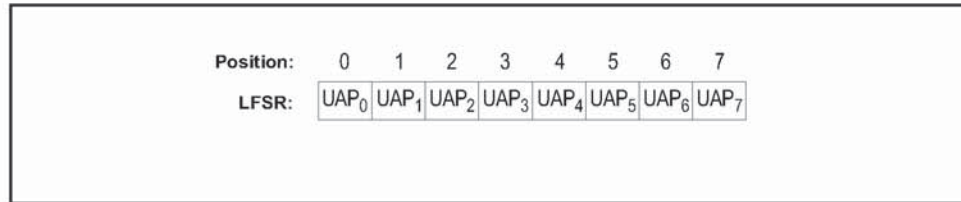
*Figure 5.7: Initial state of the HEC generating circuit.*
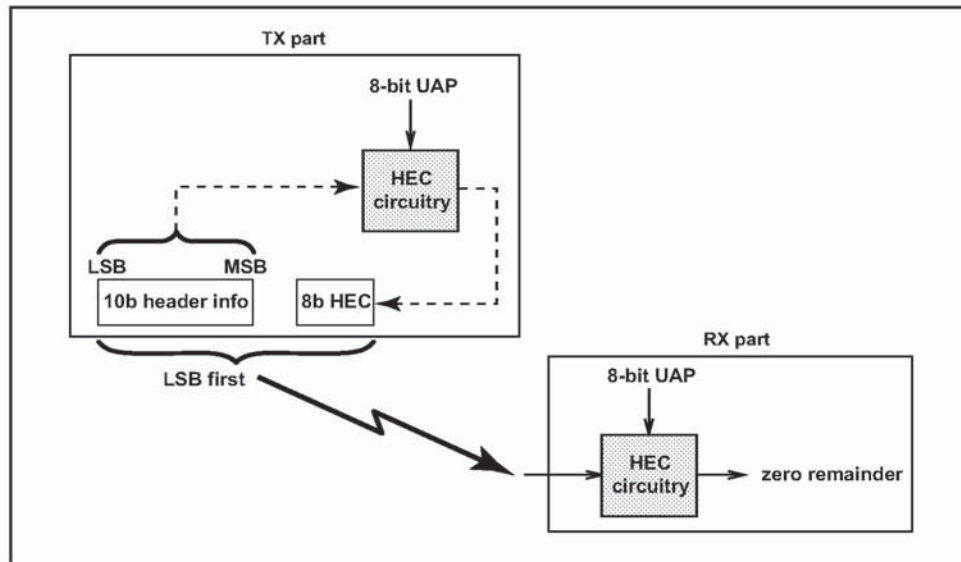


*Figure 5.8: HEC generation and checking.*

The 16 bit LFSR for the CRC is constructed similarly using the CRC-CCITT generator polynomial $g(D) = D^{16} + D^{12} + D^5 + 1$ (see Figure 5.9 on page 75). For this case, the 8 left-most bits are initially loaded with the 8-bit UAP ($UAP_0$ to the left and $UAP_7$ to the right) while the 8 right-most bits are reset to zero. The initial state of the 16 bit LFSR is depicted in Figure 5.10 on page 76. The switch S is set in position 1 while the data is shifted in. After the last bit has entered the LFSR, the switch is set in position 2, and, the register's contents are transmitted, from right to left (i.e., starting with position 15, then position 14, etc.).
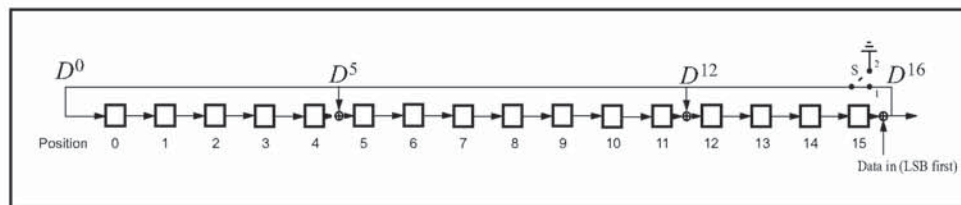


*Figure 5.9: The LFSR circuit generating the CRC.*

| Position: | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| LFSR: | $UAP_0$ | $UAP_1$ | $UAP_2$ | $UAP_3$ | $UAP_4$ | $UAP_5$ | $UAP_6$ | $UAP_7$ | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |

*Figure 5.10: Initial state of the CRC generating circuit.*
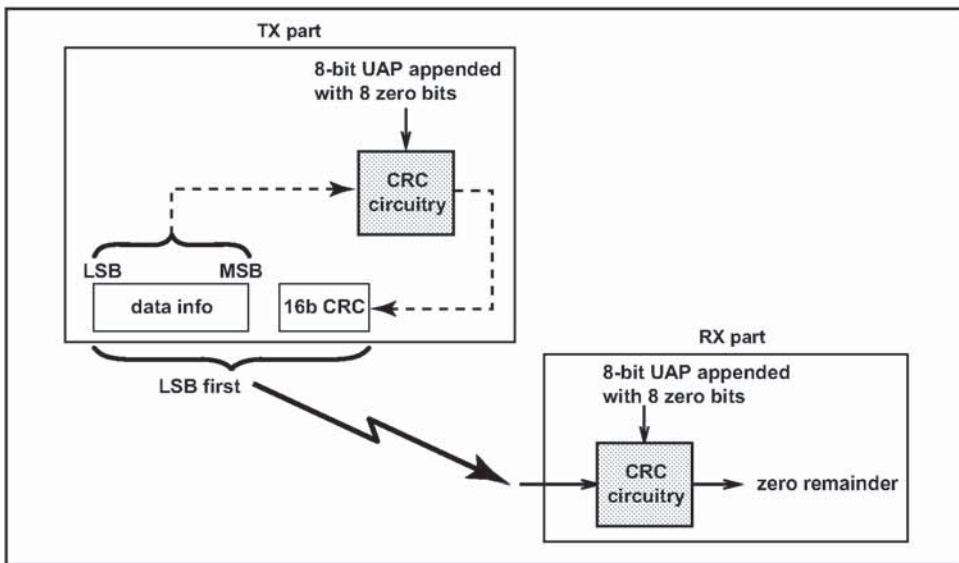


*Figure 5.11: CRC generation and checking*

**Bluetooth.**

# 6 LOGICAL CHANNELS

In the Bluetooth system, five logical channels are defined:

- LC control channel
- LM control channel
- UA user channel
- UI user channel
- US user channel

The control channels LC and LM are used at the link control level and link manager level, respectively. The user channels UA, UI, and US are used to carry asynchronous, isochronous, and synchronous user information, respectively. The LC channel is carried in the packet header; all other channels are carried in the packet payload. The LM, UA, and UI channels are indicated in the L_CH field in the payload header. The US channel is carried by the SCO link only; the UA and UI channels are normally carried by the ACL link; however, they can also be carried by the data in the DV packet on the SCO link. The LM channel can be carried either by the SCO or the ACL link.

## 6.1 LC CHANNEL (Link Control)

The LC control channel is mapped onto the packet header. This channel carries low level link control information like ARQ, flow control, and payload characterization. The LC channel is carried in every packet except in the **ID** packet which has no packet header.

## 6.2 LM CHANNEL (Link Manager)

The LM control channel carries control information exchanged between the link managers of the master and the slave(s). Typically, the LM channel uses protected **DM** packets. The LM channel is indicated by the L_CH code 11 in the payload header.

## 6.3 UA/UI CHANNEL (User Asynchronous/Isochronous Data)

The UA channel carries L2CAP transparent asynchronous user data. This data may be transmitted in one or more baseband packets. For fragmented messages, the start packet uses an L_CH code of 10 in the payload header. Remaining continuation packets use L_CH code 01. If there is no fragmentation, all packets use the L2CAP start code 10.

Isochronous data channel is supported by timing start packets properly at higher levels. At the baseband level, the L_CH code usage is the same as the UA channel.

**Bluetooth.**

## 6.4  US CHANNEL (User Synchronous Data)

The US channel carries transparent synchronous user data. This channel is carried over the SCO link.

## 6.5  CHANNEL MAPPING

The LC channel is mapped onto the packet header. All other channels are mapped onto the payload. The US channel can only be mapped onto the SCO packets. All other channels are mapped on the ACL packets, or possibly the SCO **DV** packet. The LM, UA, and UI channels may interrupt the US channel if it concerns information of higher priority.

# 7 DATA WHITENING

Before transmission, both the header and the payload are scrambled with a data whitening word in order to randomize the data from highly redundant patterns and to minimize DC bias in the packet. The scrambling is performed prior to the FEC encoding.

At the receiver, the received data is descrambled using the same whitening word generated in the recipient. The descrambling is performed after FEC decoding.

The whitening word is generated with the polynomial $g(D) = D^7 + D^4 + 1$ (i.e., 221 in octal representation) and is subsequently EXORed with the header and the payload. The whitening word is generated with the linear feedback shift register shown in Figure 7.1 on page 79. Before each transmission, the shift register is initialized with a portion of the master Bluetooth clock, $CLK_{6-1}$, extended with an MSB of value one. This initialization is carried out with $CLK_1$ written to position 0, $CLK_2$ written to position 1, etc. An exception forms the FHS packet sent during frequency hop acquisition, where initialization of the whitening register is carried out differently. Instead of the master clock, the X-input used in the **inquiry** or **page response** (depending on current state) routine is used, see Table 11.3 and Table 11.4 for the 79-hop and 23-hop systems, respectively. In case of a 79-hop system, the 5-bit values is extended with two MSBs of value one. In case of a 23-hop system, the 4-bit value is extended with three bits; the two MSBs are set to one and the third most significant bit is set to zero. During register initialization, the LSB of X (i.e., $X_0$) is written to position 0, $X_1$ is written to position 1, etc.
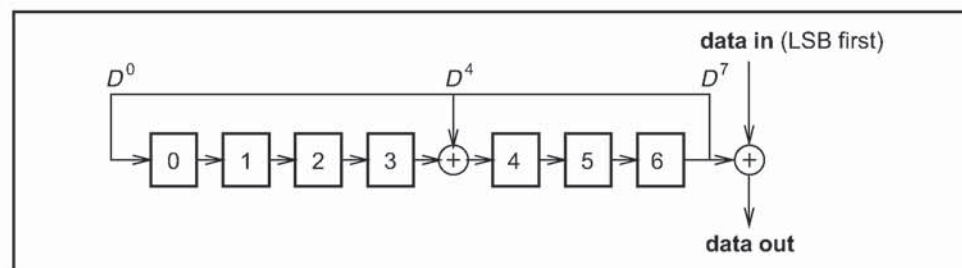


Figure 7.1: Data whitening LFSR.

After initialization, the packet header and the payload (including the CRC) are scrambled. The payload whitening continues from the state the whitening LFSR had at the end of HEC. There is no re-initialization of the shift register between packet header and payload. The first bit of the "Data In" sequence is the LSB of the packet header.

# 8 TRANSMIT/RECEIVE ROUTINES

This section describes the way to use the packets as defined in Section 4 in order to support the traffic on the ACL and SCO links. 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 8.1 and 8.2 are of an informative character only. The final implementation may be carried out differently.*

## 8.1 TX ROUTINE

The TX routine is carried out separately for each ACL link and each SCO link. Figure 8.1 on page 81 shows the ACL and SCO buffers as used in the TX routine. In this figure, only a single TX ACL buffer and a single TX SCO buffer are shown. In the master, there is a separate TX ACL buffer for each slave. In addition there may be one or more TX SCO buffers for each SCO slave (different SCO links may either reuse the same TX SCO buffer, or each have their own TX SCO buffer). Each TX buffer consists of two FIFO registers: one **current** register which can be accessed and read by the Bluetooth controller in order to compose the packets, and one **next** register that can be accessed by the Bluetooth Link 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 Bluetooth Link Controller. The switches at the input and the output of the FIFO registers can never be connected to the same register simultaneously.
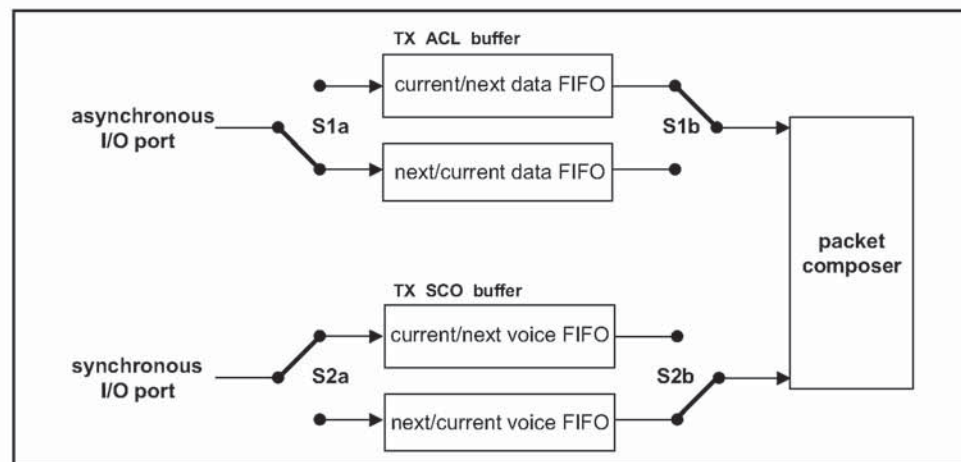


*Figure 8.1: Functional diagram of TX buffering.*

Of the packets common on the ACL and SCO links (**ID**, **NULL**, **POLL**, **FHS**, **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

ACL buffer. All ACL packets make use of the ACL buffer. All SCO packets make use of the SCO buffer except for the **DV** packet where the voice part is handled by the SCO buffer and the data part is handled by the ACL buffer. In the next sections, the operation for ACL traffic, SCO traffic, and combined data-voice traffic on the SCO link will be considered.

### 8.1.1 ACL traffic

In the case of pure (asynchronous) data, only the TX ACL buffer in Figure 8.1 on page 81 has to be considered. In this case, only packet types **DM** or **DH** are used, and these can have different lengths. The length is indicated in the pay-load header. The selection of high-rate data or medium-rate data shall depend on the quality of the link. When the quality is good, the FEC in the data payload can be omitted, resulting in a **DH** packet. Otherwise, **DM** packets must be used.

The default TYPE in pure data traffic is **NULL**. This means that, if there is no data to be sent (the data traffic is asynchronous, and therefore pauses occur in which no data is available) or no slaves need to be polled, **NULL** packets are sent instead – in order to send link control information to the other Bluetooth unit (e.g. ACK/STOP information for received data). When no link control information is available either (no need to acknowledge and/or no need to stop the RX flow) no packet is sent at all.

The TX routine works as follows. The Bluetooth Link Manager loads new data information in the register to which the switch S1a points. Next, it gives a **flush** command to the Bluetooth Link Controller, which forces the switch S1 to change (both S1a and S1b switch in synchrony). When the payload needs to be sent, the packet composer reads the current register and, depending on the packet TYPE, builds a payload which is appended to the channel access code and the header and is subsequently transmitted. In the response packet (which arrives in the following RX slot if it concerned a master transmission, or may be postponed until some later RX slot if it concerned a slave transmission), the result of the transmission is reported back. In case of an ACK, the switch S1 changes position; if a NAK (explicit or implicit) is received instead, the switch S1 will not change position. In that case, the same payload is retransmitted at the next TX occasion.

As long as the Link Manager keeps loading the registers with new information, the Bluetooth Link Controller will automatically transmit the payload; in addition, retransmissions are performed automatically in case of errors. The Link Controller will send **NULL** or nothing when no new data is loaded. If no new data has been loaded in the **next** register, during the last transmission, the packet composer will be pointing to an empty register after the last transmission has been acknowledged and the **next** register becomes the **current** register. If new data is loaded in the **next** register, a **flush** command is required to switch the S1 switch to the proper register. As long as the Link Manager keeps loading the data and type registers before each TX slot, the data is automatically processed by the Link Controller since the S1 switch is controlled by the

**Bluetooth.**

ACK information received in response. However, if the traffic from the Link Manager is interrupted once and a default packet is sent instead, a **flush** command is required to continue the flow in the Link Controller.

The **flush** command can also be used in case of time-bounded (isochronous) data. In case of a bad link, many retransmission are necessary. In certain applications, the data is time-bounded: if a payload is retransmitted all the time because of link errors, it may become outdated, and the system might decide to continue with more recent data instead and skip the payload that does not come through. This is accomplished by the **flush** command as well. With the **flush**, the switch S1 is forced to change and the Link Controller is forced to consider the next data payload and overrules the ACK control.

### 8.1.2  SCO traffic

In case of an SCO link, we only use **HV** packet types. The synchronous port continuously loads the **next** register in the SCO buffer. The S2 switches are changed according to the $T_{sco}$ interval. This $T_{sco}$ interval is negotiated between the master and the slave at the time the SCO link is established.

For each new SCO slot, the packet composer reads the **current** register after which the S2 switch is changed. If the SCO slot has to be used to send control information with high priority concerning a control packet between the master and the considered SCO slave, or a control packet between the master and any other slave, the packet composer will discard the SCO information and use the control information instead. This control information must be sent in a DM1 packet. Data or link control information can also be exchanged between the master and the SCO slave by using the **DV** or **DM1** packets. Any ACL type of packet can be used to sent data or link control information to any other ACL slave. This is discussed next.

### 8.1.3  Mixed data/voice traffic

In Section 4.4.2 on page 58, a **DV** packet has been defined that can support both data and voice simultaneously on a single SCO link. When the TYPE is **DV**, the Link Controller reads the data register to fill the data field and the voice register to fill the voice field. Thereafter, the switch S2 is changed. However, the position of S1 depends on the result of the transmission like on the ACL link: only if an ACK has been received will the S1 switch change its position. In each **DV** packet, the voice information is new, but the data information might be retransmitted if the previous transmission failed. If there is no data to be sent, the SCO link will automatically change from **DV** packet type to the current **HV** packet type used before the mixed data/voice transmission. Note that a **flush** command is required when the data stream has been interrupted and new data has arrived.

Combined data-voice transmission can also be accomplished by using separate ACL links in addition to the SCO link(s) if channel capacity permits this.

AFFLT0293311

**Samsung Ex. 1019 p. 83**

### 8.1.4 Default packet types

On the ACL links, the default type is always **NULL** both for the master and the slave. This means that if no user information needs to be send, either a **NULL** packet is sent if there is **ACK** or **STOP** information, or no packet is sent at all. The **NULL** packet can be used by the master to allocate the next slave-to-master slot to a certain slave (namely the one addressed). However, the slave is not forced to respond to the **NULL** packet from the master. If the master requires a response, it has to send a **POLL** packet.

The SCO packet type is negotiated at the LM level when the SCO link is established. The agreed packet type is also the default packet type for the SCO slots.

## 8.2 RX ROUTINE

The RX routine is carried out separately for the ACL link and the SCO link. However, in contrast to the master TX ACL buffer, a single RX buffer is shared among all slaves. For the SCO buffer, it depends how the different SCO links are distinguished whether extra SCO buffers are required or not. Figure 8.2 on page 84 shows the ACL and SCO buffers as used in the RX routine. The RX ACL buffer consists of two FIFO registers: one register that can be accessed and loaded by the Bluetooth Link Controller with the payload of the latest RX packet, and one register that can be accessed by the Bluetooth Link Manager to read the previous payload. The RX SCO buffer also consists of two FIFO registers: one register which is filled with newly arrived voice information, and one register which can be read by the voice processing unit.
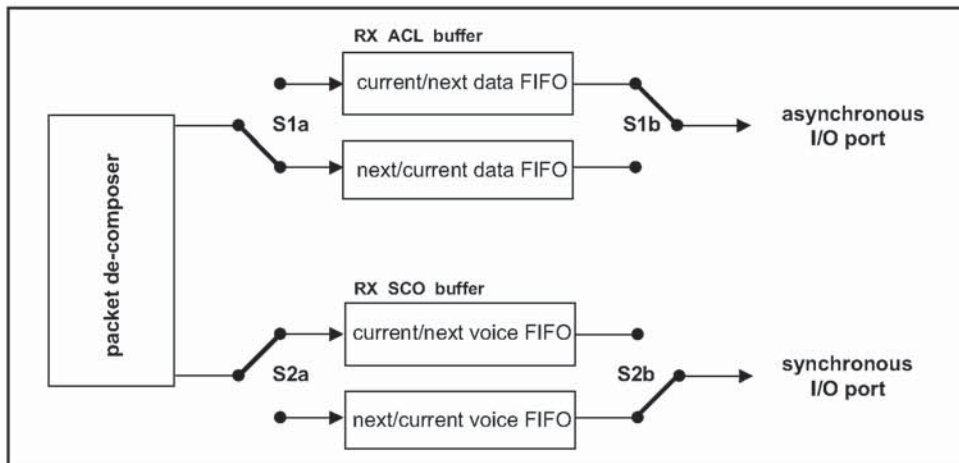


*Figure 8.2: Functional diagram of RX buffering*

Since the TYPE indication in the header of the received packet indicates whether the payload contains data and/or voice, the packet de-composer can automatically direct the traffic to the proper buffers. The switch S1 changes

**Bluetooth.**

every time the Link Manager has read the old register. If the next payload arrives before the RX register is emptied, a STOP indication must be included in the packet header of the next TX packet that is returned. The STOP indication is removed again as soon as the RX register is emptied. The SEQN field is checked before a new ACL payload is stored into the ACL register (flush indication in L_CH and broadcast messages influence the interpretation of the SEQN field see Section 5.3 on page 68).

The S2 switch is changed every $T_{SCO}$. If – due to errors in the header – no new voice payload arrives, the switch still changes. The voice processing unit then has to process the voice signal to account for the missing speech parts.

## 8.3 FLOW CONTROL

Since the RX ACL buffer can be full while a new payload arrives, flow control is required. As was mentioned earlier, the header field FLOW in the return TX packet can use STOP or GO in order to control the transmission of new data.

### 8.3.1 Destination control

As long as data cannot be received, a STOP indication is transmitted which is automatically inserted by the Link Controller into the header of the return packet. STOP is returned as long as the RX ACL buffer is not emptied by the Link Manager. When new data can be accepted again, the GO indication is returned. GO is the default value. Note that all packet types not including data can still be received. Voice communication for example is not affected by the flow control. Also note that although a Bluetooth unit cannot receive new information, it can still continue to transmit information: the flow control is separate for each direction.

### 8.3.2 Source control

On the reception of a STOP signal, the Link Controller will automatically switch to the default packet type. The current TX ACL buffer status is frozen. Default packets are sent as long as the STOP indication is received. When no packet is received, GO is assumed implicitly. Note that the default packets contain link control information (in the header) for the receive direction (which may still be open) and may contain voice (**HV** packets). When a GO indication is received, the Link Controller resumes to transmit the data as is present in the TX ACL buffers.

In a multi-slave configuration, only the transmission to the slave that issued the STOP signal is stalled. This means that the previously described routine implemented in the master only concerns the TX ACL buffer that corresponds to the slave that cannot accept data momentarily.