

# From cable replacement to the IoT

## Bluetooth 5.1

### White Paper

The Bluetooth® wireless standard has been an unparalleled success. It has found its way into virtually all smartphones, PCs, cars, entertainment hardware and wearables. Bluetooth SIG reports that more than 8 billion devices are currently in use. Bluetooth supports Internet of Things (IoT) technologies and direction finding methods, making it a sure bet for the future as well.

This white paper summarizes the various Bluetooth technologies with a focus on the physical layer in line with core specification version 5.1.

The Bluetooth® word mark and logos are registered trademarks owned by Bluetooth SIG, Inc. and any use of such marks by Rohde & Schwarz is under license.

**Note:**

Please find the most up-to-date Application Note on our homepage [www.rohde-schwarz.com/appnote/1MA108](http://www.rohde-schwarz.com/appnote/1MA108).

# Contents

<b>1</b>	<b>Introduction.....</b>	<b>3</b>
<b>2</b>	<b>Overview of Bluetooth.....</b>	<b>4</b>
<b>3</b>	<b>Bluetooth Classic.....</b>	<b>8</b>
<b>4</b>	<b>Bluetooth Low Energy for the IoT.....</b>	<b>18</b>
<b>5</b>	<b>Summary.....</b>	<b>38</b>
<b>6</b>	<b>Appendix.....</b>	<b>39</b>
<b>7</b>	<b>Rohde &amp; Schwarz.....</b>	<b>41</b>

# 1 Introduction

Bluetooth, named after a 10th century Danish king, was originally developed in the 1990s as a replacement for cable connections (e.g. a keyboard or smartphone to a PC). Initially, the objective was to cover a limited area (about 10 m) with moderate data rates and low energy consumption. A new version in the early 2000s tripled the data rate, and in 2010 a new specification additionally provided support for small battery-operated (“button-cell”) devices such as sensors.

After WLAN (Wi-Fi, 802.11), Bluetooth is the second best known wireless standard in the consumer sector and has since found its way into every computer and smartphone. The industry has also devised additional opportunities such as beacons for positioning and automation. The advent of fitness trackers and smartwatches further drives the Bluetooth market.

According to Bluetooth Special Interest Group (SIG), over 8 billion Bluetooth devices are in use today. Market analyses predict up to 5 billion additional devices annually, to a total of ca.40 billion by the year 2021. The additional growth is primarily driven by IoT applications [1].

This white paper primarily focuses on the physical layer.

Chapter 2 provides a general overview and explains the most important concepts and the individual versions. The chapters 3 and 4 provide detailed descriptions of the two main variants, Bluetooth Classic and Bluetooth Low Energy (LE) and highlights version 5 features. The final chapter summarizes and compares the characteristics of both variants.

## 2 Overview of Bluetooth

### Versions

Bluetooth has been developed over multiple versions. [Table 2-1](#) shows an overview of the major versions. Officially, all versions from V2.1 (including Basic Rate) are valid. Although development of high-speed mode has since been stopped, the specification remains valid. The versions up to and including V3 are known as Bluetooth Classic and from V4 on as Bluetooth Low Energy. Bluetooth Low Energy (V4 and later) is optimized for high efficiency requirements as needed in devices running for long timespans on small current intake. Devices may support both modes (Dual Mode).

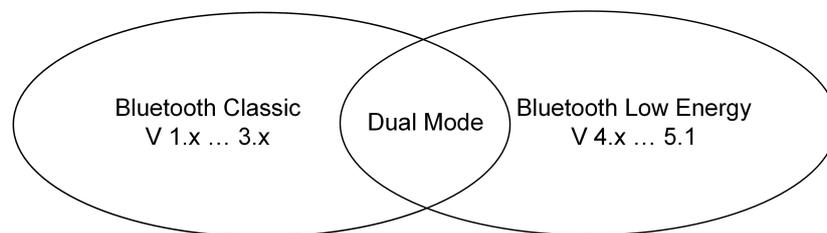
Bluetooth Classic and Low Energy are similar but not compatible with one another.

Version 5 further improves several low energy characteristics for IoT applications:

- Quadruple the range (**LE Long Range**)
- Double the speed (**2 Msym/s**)
- Increase data broadcasting capacity by 800% (**LE Advertising Extensions**)

Version 5.1 introduces **Direction Finding** in Low Energy with Angle of Arrival (AoA) and Angle of Departure (AoD)

For more information, see [Chapter 4, "Bluetooth Low Energy for the IoT"](#), on page 18.



**Figure 2-1: Bluetooth modes. The feature set of version 1...3 are called Bluetooth Classic, the feature set of version 4 and 5 are called Bluetooth Low Energy**

**Table 2-1: Development of the major Bluetooth versions**

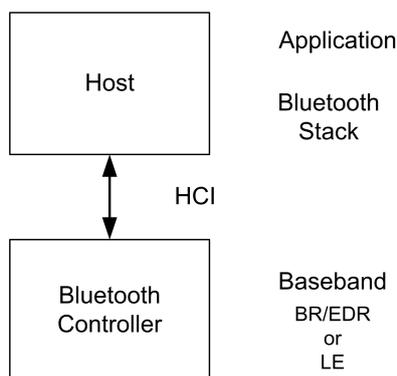
Bluetooth versions				
Version	Feature	Description	Year	Mode
1	Basic Rate (BR)	Conventional Bluetooth, low data rate	1999–2003	Classic
2	Enhanced Data Rate (EDR)	Improved transmission speed	2004–2007	
3	High Speed (HS)	High-speed mode	2009	
4	Low Energy (LE)	Low energy, IoT	2010–2014	Low Energy
5	Improvements for LE	LE: higher data rates, extended range, greater throughput	2016	
5.1	Direction Finding AoA / AoD	via Constant Tone Extension (CTE)	2019	

**ISM band**

Bluetooth operates in the unlicensed industrial, scientific and medical (ISM) band of 2.4 GHz, which it must share with other applications such as WLAN, microwave ovens, ANT+, DECT wireless telephones (in some countries) and baby monitors, as well as industrial and medical applications (e.g. X-ray in hospitals).

**Architecture**

A Bluetooth device primarily consists of a host and a Bluetooth controller. The Bluetooth stack and the actual application run on the host; the baseband can support either Bluetooth Classic (BR/EDR) or Low Energy. Both components communicate via the host controller interface (HCI).



**Figure 2-2: Basic Bluetooth architecture. The controller can support BR/EDR or LE.**

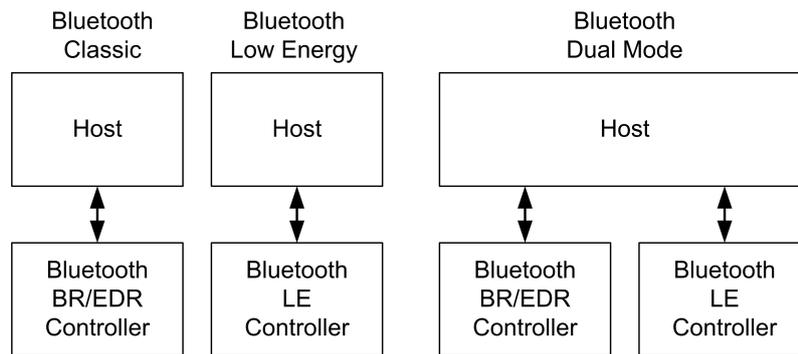


Figure 2-3: Different architecture variations.

Dual mode devices use two controllers, one for BR/EDR and one for LE. In principle, devices can also contain an additional controller for Bluetooth 3.0 (see introduction to [Chapter 3, "Bluetooth Classic"](#), on page 8); however, that option is not shown here.

The following communications take place via the HCI:

- Commands from host to baseband (BB)
- Events from BB to host
- Data in both directions

A Bluetooth device does not require the host; in this case everything runs on the baseband and HCI is not implemented. This makes sense only for devices with limited (Bluetooth) functionality, e.g. headsets.

### Addresses

Each Bluetooth device has a unique, fixed address with a length of 48 bits (6 bytes) that also includes a special identifier of the manufacturer (see also [2]).

### Security

Bluetooth supports security at multiple levels. However, this is not covered by this white paper. For more information, see [2].

The following overview is derived from [2]:

- Pairing: the process for creating one or more shared secret keys
- Bonding: the act of storing the keys created during pairing for use in subsequent connections in order to form a trusted device pair
- Device authentication: verification that the two devices have the same keys
- Encryption: message confidentiality
- Message integrity: protects against message forgeries

### Profiles

Bluetooth provides only the physical ability to transfer data without a cable. However, users have expectations that certain use cases are implemented (e.g. "I want to transfer a file from my PC to my cell phone"). Bluetooth therefore defines certain profiles,

that means how a specific scenario should be implemented (in keeping with the above example, a file transfer profile (FTP) is offered).

Some profiles are universally applicable and must be supported in every Bluetooth device. Others appear only in certain devices or versions, depending on their purpose (e.g. the handsfree profile makes sense in headsets but not in smartphones).

Two devices that want to exchange data must support the same profile.

The following are examples of general profiles:

- GAP – general access profile
  - Must be supported by all devices
  - Defines parameters such as Bluetooth addresses, PINs and user-friendly Bluetooth names
- SDP – service discovery application profile
  - Used to request device services

Other examples are found in the chapters describing Bluetooth Classic and Bluetooth Low Energy.

For a complete overview, go to [www.bluetooth.com/specifications/profiles-overview](http://www.bluetooth.com/specifications/profiles-overview).

### Qualification

Bluetooth SIG requires certification of all devices. This certification can be obtained only from a Bluetooth Qualification and Test Facility (BQTF). Bluetooth SIG provides a list of certified test houses and defines the test specifications for Bluetooth Classic and Bluetooth Low Energy. These test specifications, which are intended to ensure interoperability among Bluetooth devices, cover various aspects of Bluetooth devices. For example, profile interoperability must be tested. Testing of the physical layer is especially important.

The R&S®CMW radio communication testers from Rohde & Schwarz are one-box instruments that support all the different stages – from development and precertification to production. Bluetooth® SIG has listed the R&S®CMW as a qualified product for RF testing. Test houses also use the R&S®CMW as a tester in validated Bluetooth qualification test systems. The R&S®CMW can thus be used in R&D prior to prequalification tests.

## 3 Bluetooth Classic

Bluetooth Classic includes versions 1, 2 and 3. Version 1 (Basic Rate) was extended to Version 2 (Enhanced Data Rate (EDR)) to permit higher data rates. The high-speed (HS) channel in Version 3 is a special mode (called alternative MAC/PHY (AMP)) that uses a WLAN 802.11 controller in the chip. This method is also known as offloading. This version remains valid but it is no longer developed and no longer plays an important role. As no special Bluetooth test specification is available, this version is not covered in detail here.

Bluetooth Classic and Low Energy are similar but not compatible with one another. If a Bluetooth device must provide both modes, it must support Dual Mode.

### 3.1 Piconet

It is possible to interconnect two or more devices. This is known as a piconet. A piconet consists of at least two and a maximum of eight Bluetooth Classic products, where one device assumes the master role and defines the clock. All remaining devices are slaves. A Bluetooth product can conduct an "inquiry", i.e. all remaining products (assuming they have been switched to visible) in the communications range respond by reporting their Bluetooth address and capabilities. In a piconet, all devices must share the available resources (data rate). Each link is initiated from the master. If a data connection (link) is established, it hops at certain times to different RF channels. Each piconet has its own hopping sequence in order to avoid collisions. Slaves cannot communicate directly with one another. A slave can be a member of multiple piconets.

### 3.2 Links

Two link types are defined in Bluetooth:

- Synchronous connection-oriented (SCO) link
- Asynchronous connectionless (ACL) link

A maximum of seven ACLs and three SCOs can be active at any given time in a piconet. A master can manage three SCOs to one or multiple slaves simultaneously. Only one ACL can be set up between a master and a slave. In total, one ACL and three SCOs are possible between the master and slave.

#### SCO

The SCO link provides a point-to-point connection between the master and slave. Reserved, fixed timeslots with symmetric data rates are used for this purpose. SCO links are used for time-critical applications such as voice transmissions. The typical data rate is 64 kbit/s. Extended SCO (eSCO) was introduced after version 1.2 to support more flexible connections.

### ACL

The ACL link establishes a point-to-multipoint connection between a master and multiple slaves and uses timeslots that are not already occupied or reserved by SCO links. Both symmetric and asymmetric links are supported. If basic rate is used, the maximum net data rate is 433.9 kbit/s in symmetric operation and 723.2 kbit/s in asymmetric operation. If EDR is used, the corresponding values are 1306.9 kbit/s and 2178.1 kbit/s. ACL packets may be repeated if necessary.

## 3.3 Profiles

A large number of classic profiles are implemented, and the number is constantly increasing.

Examples:

- A2DP advanced audio distribution profile: streaming of audio data
- AVRCP audio/video remote control profile: remote control for audio/video
- HFP handsfree profile: cordless telephone operation in an automobile

## 3.4 States

Bluetooth BR/EDR provides a state machine with the following principle states:

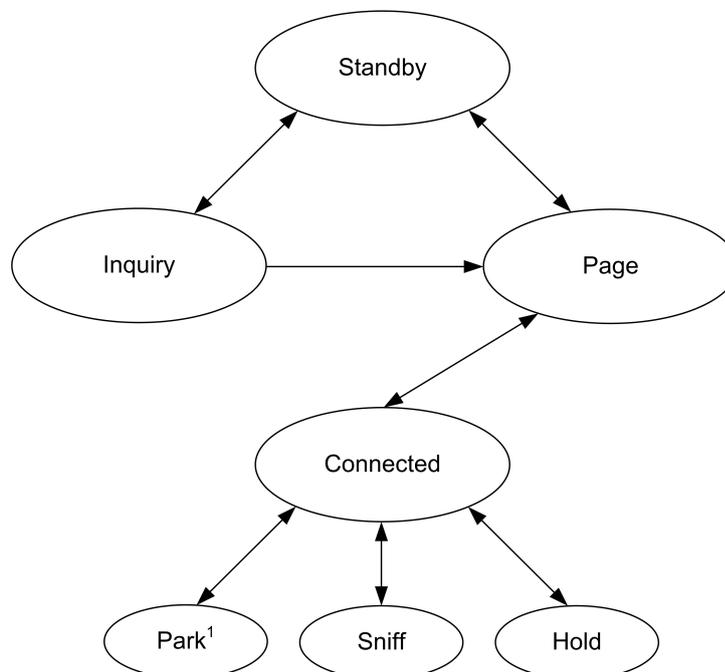


Figure 3-1: State machine for Bluetooth Classic. 1. Park is no longer available as of Version 5.

**Standby**

This is the default state in Bluetooth. A link is not set up.

**Inquiry**

Initially, Bluetooth devices are unaware of each other. An inquiry (lasting a defined time period, e.g. 3 s) requests other devices in the vicinity to report their address. Devices that are set to "visible" respond with their address. A connection can now be set up. -> see "Page".

**Page**

In the page state, a connection is set up to a known device.

**Active (connected)**

The device is part of an active link; packets are exchanged.

**Sniff**

A link is present in which the master transmits to the slave but only on specific time-slots. The slave needs to be ready solely for these timeslots, thus saving energy (battery operating time).

**Hold**

In this connection mode, no more ACL packets are allowed. SCO packets can still be sent. This frees up time for other activities such as taking part in other piconets.

**Park**

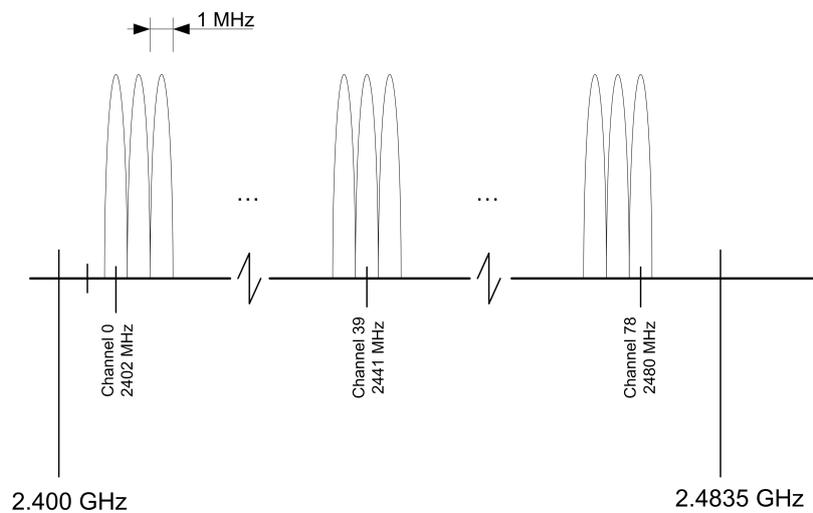
**Note:** Park state is no longer supported starting with Version 5.

In park mode, a device does not actively participate in a piconet but remains synchronized to the master. The device must wake up at regular intervals to resynchronize and "listen" for packets.

## 3.5 The Radio Interface

### 3.5.1 Channels, Frequencies and Hopping

Bluetooth Classic uses 79 channels with 1 MHz spacing in the unlicensed industrial, scientific and medical (ISM) band of 2.4 GHz. The range extends from channel 0 at 2402 MHz to channel 78 at 2480 MHz.



**Figure 3-2: Basic Bluetooth channel allocation in the ISM band.**

To take full advantage of the available spectrum and to prevent interference of or by other applications, pseudorandom frequency hopping at a nominal rate of 1600 hops per second is used. The hopping sequence is based on the Bluetooth address of the master, so every piconet uses its own hopping sequence.

To further enhance coexistence with WLAN, adaptive frequency hopping (AFH) was introduced in specification V1.2. AFH does not use all 79 channels. Instead, it uses only a limited range, where channels with known interferences are excluded.

### 3.5.2 Transmit Power

Bluetooth basic products are divided into three power classes:

- Class 1: max. 20 dBm (100 mW)
- Class 2: max. 4 dBm (2.5 mW)
- Class 3: max. 0 dBm (1 mW)

In addition, a rough power control may be defined as an option, i.e. a specific command causes the device to respond with a positive (or negative) step between 2 dB and 8 dB. Moreover, the device issues a message when the maximum or minimum power is reached. However, this message does not have to be generated within a specific amount of time.

### 3.5.3 Packets

In Bluetooth Classic, a timeslot is 625  $\mu$ s (see [Chapter 3.5.4, "Time Scheme"](#), on page 13).

### Single-slot and multi-slot packets

All Bluetooth products must support single-slot packets. These packets have a maximum length of 366  $\mu$ s (AUX1 packets) and fit in a timeslot of 625  $\mu$ s, i.e. the maximum frequency hopping rate is attained. The payload might include a payload header and/or CRC depending on the packet. In addition, products may also support three timeslots and/or five timeslots. The frequency is not changed during a packet.

### Basic rate packet format

Every (data) packet consists of an access code, a header and its payload:

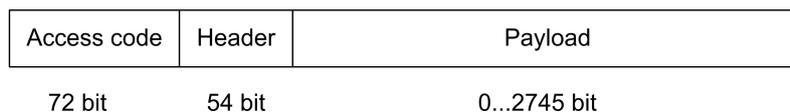


Figure 3-3: Packet format (basic rate).

The entire packet is GFSK-modulated.

### EDR packet format

An EDR packet contains the same access code and header (each GFSK) as a basic rate packet. In addition, a guard time area and a sync word area are inserted between the header and the payload. These two areas and the payload are DPSK-modulated.

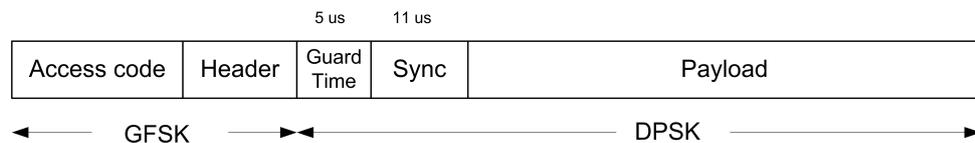


Figure 3-4: EDR packet format.

### ACL and SCO packets

The following tables show the defined packets for the ACL and SCO links. 'x' represents a numeral, e.g. DH5, that defines various payload and packet lengths. This length (1, 3 or 5) also influences the hopping. In the case of multi-slot packets, hopping occurs only after a complete packet (see Figure 3-6).

Table 3-1: ACL packets

ACL packets		
Packet	Type	Comment
DMx	Data middle	Max. 477 kbit/s
DHx	Data high	Max. 723.2 kbit/s
AUX	Auxiliary	Like DH1, but without CRC
2DHx	Extended DH (EDR, $\pi/4$ -DQPSK)	Max. 1448 kbit/s
3DHx	Extended DH (EDR, 8DPSK)	Max. 2178 kbit/s

Table 3-2: SCO packets

SCO packets		
Packet	Type	Comment
HVx	High quality voice	Max. 64 kbit/s
DV	Data/voice	64 kbit/s + 57 kbit/s data
EVx	Extended voice	Max. 288 kbit/s
2EVx	Extended voice (EDR, $\pi/4$ -DQPSK))	Max. 576 kbit/s
3EVx	Extended voice (EDR, 8DPSK))	Max. 864 kbit/s

### 3.5.4 Time Scheme

To provide master-and-slave communications in one channel, a time division duplex (TDD) scheme has been defined. The frequency hopping with a nominal rate of 1600 hops/s yields a time division scheme of 625  $\mu$ s (one timeslot).

Figure 3-5 shows the duplex scheme when using single-slot packets. Either the master or the slave transmits in each timeslot, and the frequency changes in every timeslot.

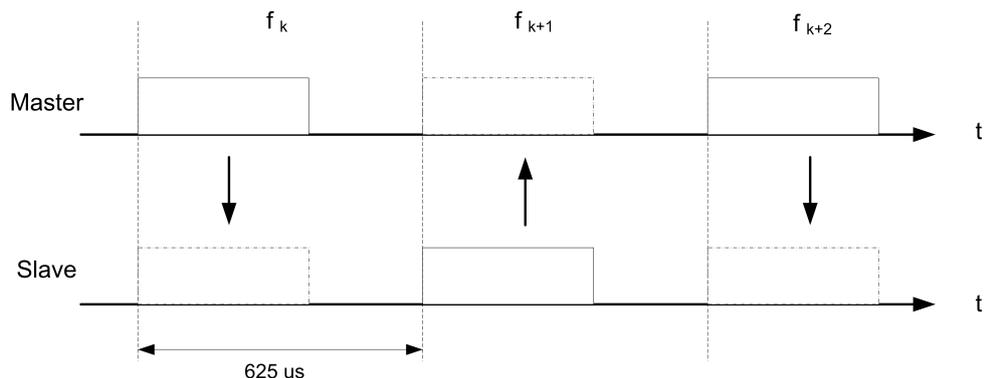


Figure 3-5: Timing scheme, single-slot.

If longer packets are used, the frequency is not changed until after the packet. The frequencies not used for transmitting the long packets are skipped (Figure 3-6).

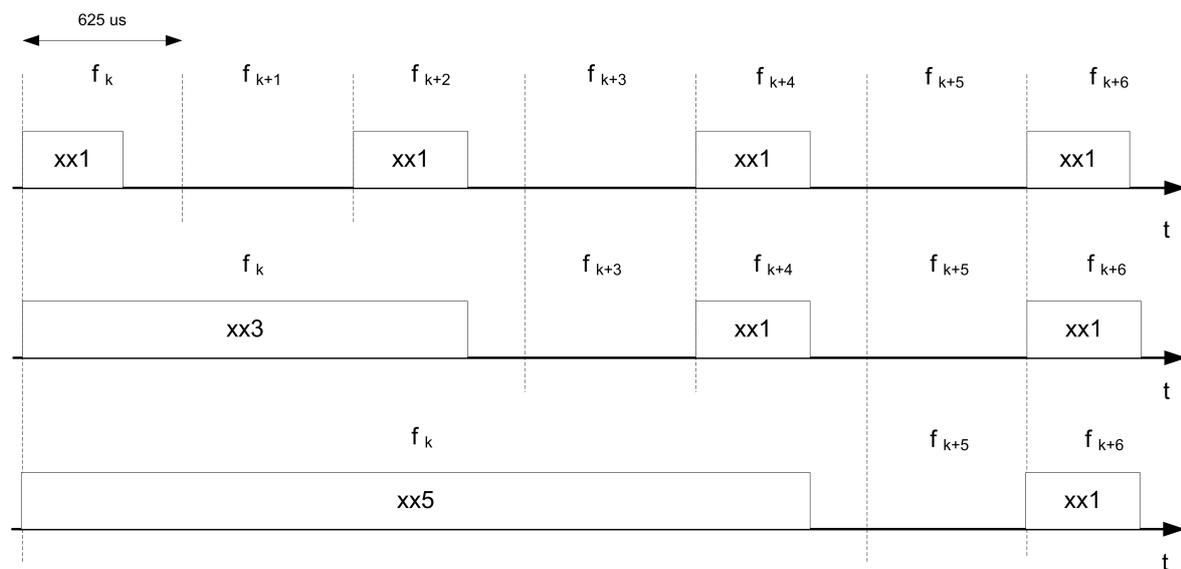


Figure 3-6: Timing scheme, multi-slot; xx1: single-slot packets, xx3/5: multi-slot packets.

## 3.5.5 Modulations

### 3.5.5.1 Basic Rate Modulation

For the basic rate, frequency shift keying modulation (Gaussian frequency shift keying, GFSK) with a symbol rate of 1 Msymbol/s is used. The nominal frequency deviation is  $\pm 160$  kHz. This yields a gross data rate of 1 Mbit/s. The Gaussian filter with a bandwidth bit period product  $BT$  is 0.5. The modulation index lies between 0.28 and 0.35.

### 3.5.5.2 EDR Modulation

The data rate is enhanced by using two new types of phase shift keying (PSK).

#### $\pi/4$ -DQPSK

This type of modulation (two bits per symbol) makes it possible to increase the gross data rate to 2 Mbit/s. If a device is V2.0+EDR-compatible, this type of modulation must be supported.

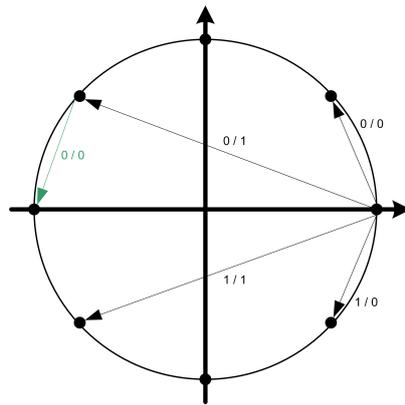


Figure 3-7:  $\pi/4$ -DQPSK.

### 8DPSK

This type of modulation (three bits per symbol) makes it possible to increase the gross data rate to 3 Mbit/s. It may also be supported in addition to  $\pi/4$ -DQPSK.

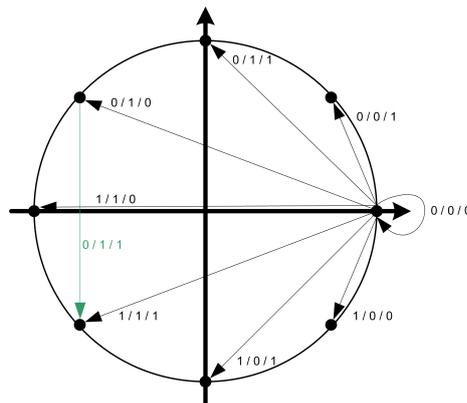


Figure 3-8: : 8DPSK.

## 3.5.6 RF Measurements

In addition to the Core Specification [2], the Radio Frequency [3] Bluetooth Test Specification defines the qualification tests for physical layer 1.

A test mode has been defined for these tests that can take place both directly on the test instrument (via HW or SW) as well as by signaling over the RF interface. In this test mode, the packets provided by the tester are returned from the DUT (loop back). For TX tests, a Tx only mode is also available.

Most of the tests listed below are nonhopping, they have to be performed on single RF channels.

**Table 3-3: RF transmitter tests for Bluetooth BR + EDR (Classic)**

RF transmitter measurements		
Number	Name	Comment
TP/TRM/CA/BV-01-C	Output power	
TP/TRM/CA/BV-02-C	Power density	
TP/TRM/CA/BV-03-C	Power control	
TP/TRM/CA/BV-04-C	TX output spectrum – frequency range	
TP/TRM/CA/BV-05-C	TX output spectrum – 20 dB bandwidth	
TP/TRM/CA/BV-06-C	TX output spectrum – adjacent channel power	
TP/TRM/CA/BV-07-C	Modulation characteristics	
TP/TRM/CA/BV-08-C	Initial carrier frequency tolerance	
TP/TRM/CA/BV-09-C	Carrier frequency drift	
TP/TRM/CA/BV-10-C	EDR relative transmit power	
TP/TRM/CA/BV-11-C	EDR carrier frequency stability and modulation accuracy	
TP/TRM/CA/BV-12-C	EDR differential phase encoding	
TP/TRM/CA/BV-13-C	EDR in-band spurious emissions	
TP/TRM/CA/BV-14-C	Enhanced power control	
TP/TRM/CA/BV-15-C	EDR Guard Time	
TP/TRM/CA/BV-16-C	EDR Synchronization Sequence and Trailer	

**Table 3-4: RF receiver tests for Bluetooth BR + EDR (Classic)**

RF receiver measurements		
Number	Name	Comment
TP/RVC/CA/BV-01-C	Sensitivity – single-slot packets	
TP/RVC/CA/BV-02-C	Sensitivity – multi-slot packets	
TP/RVC/CA/BV-03-C	C/I performance	
TP/RVC/CA/BV-04-C	Blocking performance	
TP/RVC/CA/BV-05-C	Intermodulation performance	
TP/RVC/CA/BV-06-C	Maximum input level	
TP/RVC/CA/BV-07-C	EDR sensitivity	
TP/RVC/CA/BV-08-C	EDR BER floor performance	
TP/RVC/CA/BV-09-C	EDR C/I performance	
TP/RVC/CA/BV-10-C	EDR maximum input level	

All of the tests listed above can be performed using the R&S®CMW radio communication tester platform. Some tests require additional test instruments.

Because Bluetooth must share the ISM band with other wireless standards, additional coexistence tests in addition to the required tests are useful. Those tests are available with the R&S®CMW platform.

## 4 Bluetooth Low Energy for the IoT

Bluetooth Low Energy is the designation for special extensions starting with Version 4. Versions 4.1 and 4.2 provide minor extensions/improvements. Version 5 brings fundamental improvements, such as a higher data rate. Version 5.1 enables special Direction Finding methods.

As indicated by the name, the most important feature is the low energy consumption. This is achieved by a device being mostly inactive (99.9 % of the time). Another objective was a fast connection setup. IoT applications require relatively low data rates.

Bluetooth Classic and Low Energy are similar but not compatible with one another. If a Bluetooth device must provide both modes, it must support dual mode.

### 4.1 Version 5 Features

- Two times the data rate to 2 Msymbols/s by using a new modulation mode. See section [Chapter 4.6.6, "Modulations"](#), on page 34
- Four times the range thanks to special coding (LE long range). See section [Chapter 4.6.4.2, "Packet Format for Coded PHYs \(LE Long Range\)"](#), on page 27
- Eight times the broadcast capacity through an extension of the advertising procedures (LE advertising extension). See section [Chapter 4.6.4.3, "PDU for Advertising"](#), on page 27, extended advertising table.
- Higher available transmit power (up to +20 dBm). See section [Chapter 4.6.3, "Transmit Power"](#), on page 25
- Direction Finding via Angle of Arrival (AoA)/ Departure (AoD) in version 5.1. See section [Chapter 4.3, "Direction Finding"](#), on page 19

### 4.2 Advertising and Data Transmission

Bluetooth LE allows multiple types of communications:

- Information transmission only (broadcast) (Tx)
- Data reception only (Rx)
- Mixed transmission and reception of data (Tx and Rx)

Bluetooth LE introduced "advertising" for this purpose. All communications at first take place via specialized channels (advertising channels, see [Chapter 4.6.4.3, "PDU for Advertising"](#), on page 27). A device transmits information on this channel, while one or more other devices listen (scanning). The name **Beacons** has come into use here. The primary meaning of beacons is to permit positioning within a defined area (e.g. inside a shop) along with related services (e.g. customer behavioral analysis or paid services) and customized advertisement. Beacons are typically Tx only devices.

To save energy, devices can opt out of these specific communications during scanning; this is implemented using a white list filter. Data can be exchanged directly between the devices via an advertising channel.

A device can require a connection (initiator) (e.g. to exchange additional data). This connection is equivalent to the piconet in Bluetooth Classic, with master and slave (see also [Chapter 3, "Bluetooth Classic"](#), on page 8). Hopping occurs within this piconet.

Version 5 brings an enhancement to advertising. Data channels can now also be used as auxiliary channels. In advertising mode, data is transmitted on the data channels using auxiliary packets (AUX), and no true connection is set up. This is called offloading. Offloading serves to reduce the load on the three advertising channels. Version 5.1 allows Direction Finding during Advertising.

### 4.3 Direction Finding

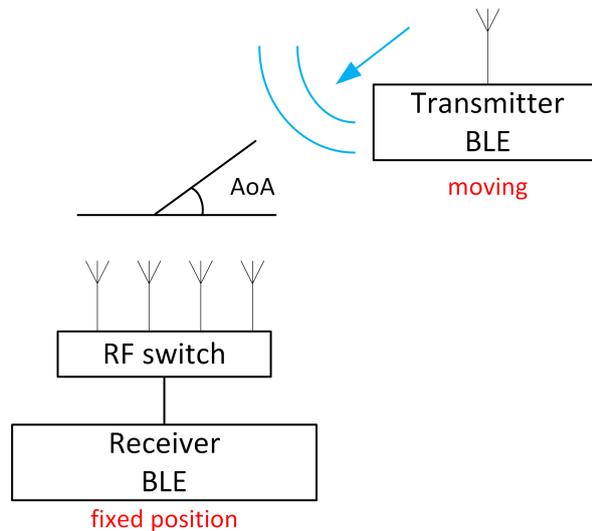
Until version 5.0, Bluetooth Low Energy already allows location services via proximity or trilateration with an external calculation. Version 5.1 now introduces Direction Finding to determine the angle between two devices directly. Bluetooth supports two methods via multiple antenna support:

- Angle of Arrival (AoA)
- Angle of Departure (AoD)

### Angle of Arrival

This method supports Real-Time Location Systems (RTLS) e.g. for asset tracking.

## Angle of Arrival (AoA)



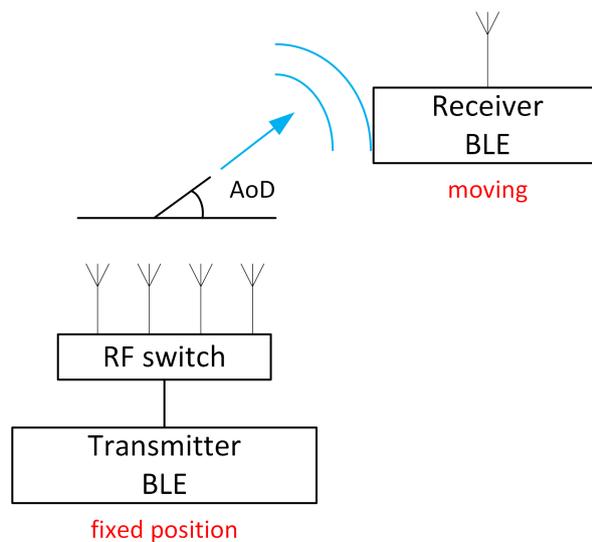
**Figure 4-1: AoA**

A (moving) device transmits with one antenna a special BLE-RF signal. The receiver determines the angle of arrival with switching between the antennas during the crossing of the signal. The receiver captures the BLE-RF signals and saves the different IQ samples of the different antennas and is now able to determine the angle (AoA) by calculation of the phase offsets.

### Angle of Departure

This method supports Indoor Position Systems (IPS) e.g. for indoor navigation (way-finding) via Smartphones.

## Angle of Departure (AoD)

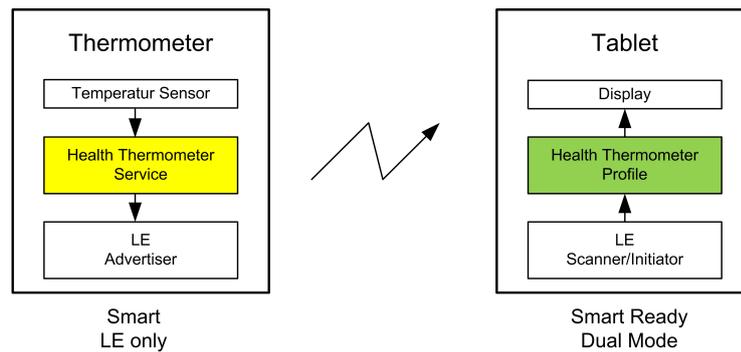


**Figure 4-2: AoD**

Here a (moving) device calculates its own position (relative phase) by receiving a BLE signal from a (fixed) transmitter. The Transmitter switches during a special Bluetooth signal the antennas. The receiver (with one antenna) samples the RF signal and is able to calculate the angle by the phase differences of the samples.

## 4.4 Profiles and Services

Bluetooth LE defines services and profiles. A service describes one or more features governing the behavior of a small peripheral device with only limited functionality (e.g. temperature measurement). A profile describes how a service can be used for a specific application. This is especially relevant for central devices such as smartphones and tablets.



**Figure 4-3: Services versus profiles: The thermometer is exclusively an advertiser, and as such uses a service. As a dual-mode device, a tablet uses a profile to read the data from the thermometer as a scanner and/or initiator.**

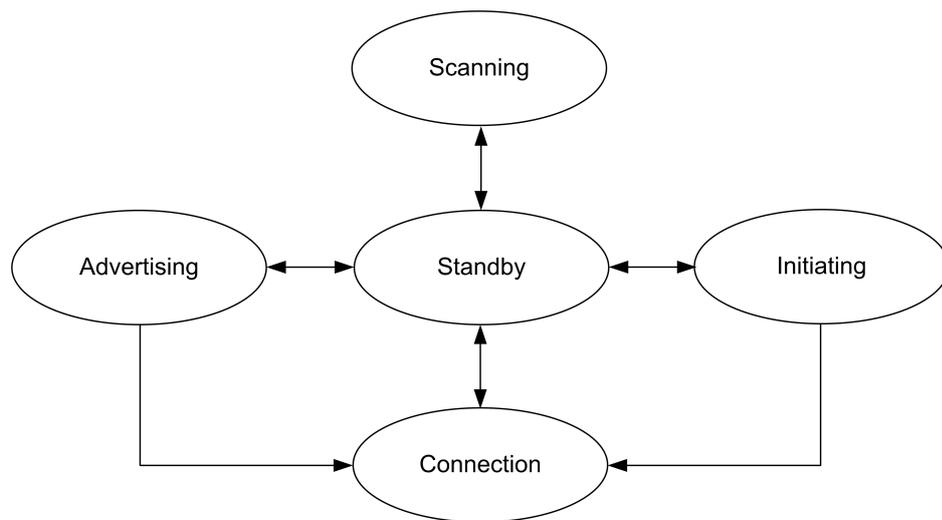
Bluetooth LE includes a predefined generic attribute profile (GATT). This profile defines a type of framework for profile development. Profiles can inherit a predefined architecture from the GATT.

A few examples of services and profiles are provided here:

- General service
  - BAS battery service
- Example for medical
  - GLP glucose profile and glucose service
- Example for health and fitness
  - Pulse oximeter profile and pulse oximeter service

## 4.5 States

The link layer (LL) in Bluetooth LE administers one or more state machines to implement multiple roles simultaneously. As a result, a device can perform advertising at the same time that it monitors other devices via scanning.



*Figure 4-4: State machine for Bluetooth Low Energy. A device can run multiple machines simultaneously, e.g. to support advertising and scanning in parallel.*

### Standby

Default state.

### Advertising

In advertising state, the device sends advertising events (see also [Chapter 4.6.4.3, "PDU for Advertising"](#), on page 27) on the advertising channels, acting only as transmitter, not as receiver. The advertiser can use all three channels or just one selected channel. The device transmits a message ("here I am") to other devices in the vicinity. Initially, no connection is set up. User data can also periodically be transmitted to the scanner via advertising channels.

### Scanning

This state is the opposite of advertising. The device listens to the advertising channels for advertising events. There are two different scanning modes:

- Passive scanning: data reception only; no transmission
- Active scanning: scan requests can be transmitted

### Initiating

A scanner can send a connection request to an advertiser if the advertiser signals a connection opportunity (see also [Table 4-6](#)). This connection request is sent to the advertiser on the advertising channels.

### Connection

If the connection setup (initiating) was successful, both devices are in connection state, and they can now exchange data within the piconet. The initiator (previously the scanner) is the master and the advertiser is the slave. This mode is similar to a connection

in Bluetooth Basic. The data channels are used in hopping mode. Adaptive frequency hopping (AFH) is also available.

## 4.6 The Radio Interface

### 4.6.1 Overview of Three PHYs

Version 5 introduces new technologies on the lower layers. As a result, three different PHYs are now defined, providing differing modulations, coding and net data rates. Coding permits the increased range and is described in more detail in 4.5.4. S=8 indicates that eight symbols code one bit; correspondingly S=2 means that two symbols are equal to one bit. LE 1M is mandatory and backward compatible to V4. The uncoded PHYs (LE 1M and LE 2M) allow Direction Finding (DF). [Table 4-1](#) summarizes the PHYs.

**Table 4-1: Three LE PHYs**

PHY	Blue-tooth LE	Modulation scheme (GFSK) gross data rate	Coding		Net data rate	Direction Finding via CTE
			Access header	Payload		
LE 1M	Mandatory	Nominal Frequency Deviation 250 kHz 1 Msymbols/s	Uncoded		1 Mbit/s	yes
LE 2M	Optional	Nominal Frequency Deviation 500 kHz 2 Msymbols/s	Uncoded		2 Mbit/s	yes
LE coded	Optional	Nominal Frequency Deviation 250 kHz 1 Msymbols/s	S = 8	S = 2 S = 8	500 kbit/s 125 kbit/s	no

### 4.6.2 Channels, Frequencies and Hopping

Bluetooth low energy uses 40 channels with 2 MHz spacing in the unlicensed industrial, scientific and medical (ISM) band of 2.4 GHz. The range extends from 2402 MHz (RF channel 0; logical channel 37) to 2480 MHz (RF channel 39; logical channel 39). Three channels (logical 37, 38 and 39) are so called primary advertising channels; logical channels 0 to 36 are data channels. The three primary advertising channels are positioned so that they are not disturbed by the nonoverlapping WLAN channels 1, 6 and 11 in the ISM band (see [Figure 4-5](#)). Hopping is used only if a connection exists between two devices. Advertising and data exchange during advertising does not use hopping; for this reason the ETSI does not consider Bluetooth LE to be a hopping system.

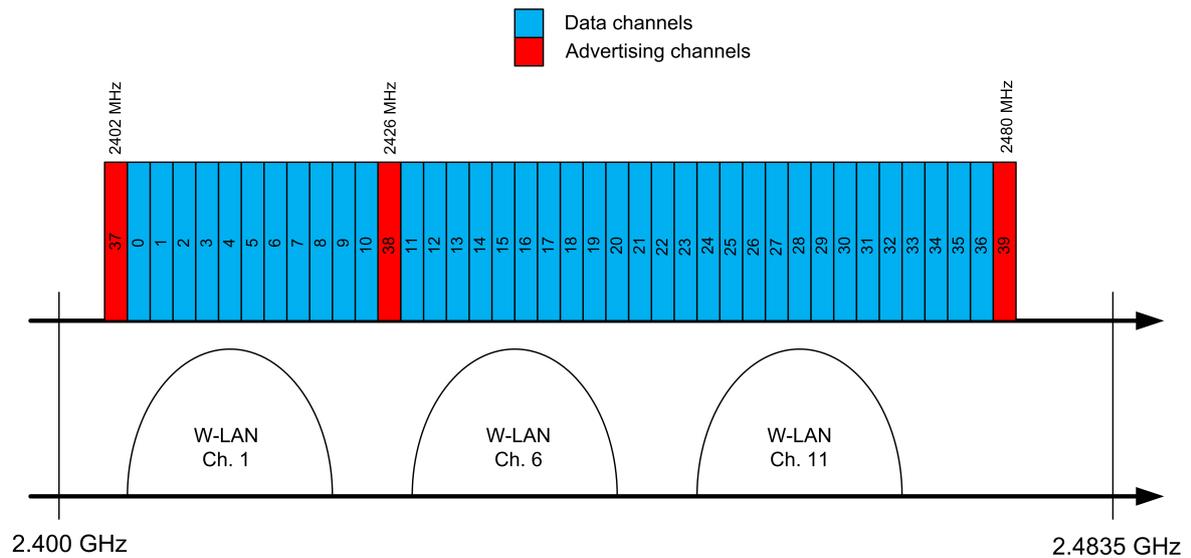


Figure 4-5: Bluetooth low energy channels. Red advertising channels; blue data channels. Along the bottom the three nonoverlapping WLAN channels 1, 6 and 11.

### 4.6.3 Transmit Power

The maximum output power in Bluetooth LE lies between  $-20$  dBm (0.01 mW) and  $+20$  dBm (100 mW) (up until V4.2 it was only  $+10$  dBm (without the addendum 5)). To keep the energy consumption down, a power control can be independently implemented in a device. The following informative classes are defined:

Table 4-2: Informative Tx power classes in LE

Class	Max output (dBm)
1	+20
1.5	+10
2	+4
3	0

### 4.6.4 Packets

The individual basic parts of a Bluetooth LE packet are fundamentally the same.



Figure 4-6: General parts of a Bluetooth LE packet.

- The **preamble** is a fixed sequence of zeros and ones to support the receiver, e.g. for time synchronization and AGC.

- The **access address** is a random value that identifies the access to a physical channel.
- The protocol data unit (**PDU**) carries the actual message. This includes both the transmitter and receiver addresses as well as user data, for example.
- Cyclic redundancy check (**CRC**)

The packets are primarily distinguished by their PDU.

The Bluetooth **addresses** are specified directly in the PDU payload and are 6 bytes (48 bits) in length. This normally includes the source address and destination address.

Version 5 introduced the coded PHY, providing additional fields for coding. Version 5.1 expands the format for Direction Finding support (Constant Tone Extension) for uncoded PHYs (see next chapter).

#### 4.6.4.1 Packet Format for Uncoded PHYs (LE 1M and LE 2M)

The general packet format applies to the uncoded PHY. Differences result in the length of the preamble and in the duration of the packet, as LE 2M PHY has double the bit rate.



*Figure 4-7: Packet of uncoded PHYs.*

The part **Constant Tone Extension (CTE)** is optional and used for direction finding from version 5.1 on. It is available both in Advertising and Data packets (PDUs). The length is signaled in the PDU header ([Chapter 4.6.4, "Packets"](#), on page 25 and [Chapter 4.6.4.4, "PDU for Data"](#), on page 30) and the duration is between 16  $\mu$ s to 160  $\mu$ s (see [Chapter 4.6.4, "Packets"](#), on page 25).

*Table 4-3: Duration of uncoded packets*

PHY		Preamble	Access address	PDU	CRC
LE 1M	Length in bits	8	32	16...2064	24
	Length in $\mu$ s	8	32	16...2064	24
LE 2M	Length in bits	16	32	16...2064	24
	Length in $\mu$ s	8	16	8...1032	12

In Bluetooth LE V4.1, the PDU was only 39 bytes (312 bits), while 257 bytes (2056 bits) are possible starting with V4.2. This V4.2 feature is called extended packet length. The LE 2M PHY preamble is 16 bits to ensure a consistent duration.

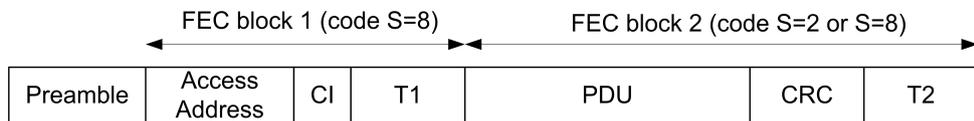
With the variable length of the PDU and the optional CTE field, the minimum and maximum packet length are in:

**Table 4-4: Min and max duration of uncoded PHY packets**

	LE 1M	LE 2M
	packet duration in $\mu$ s	
without CTE	80...2120	44...1064
with CTE	104...2288	64...1228

#### 4.6.4.2 Packet Format for Coded PHYs (LE Long Range)

In the coded packet, the preamble remains uncoded and the access address, coding indicator (CI) and termination field 1 (T1) form FEC block 1, which is always transmitted with S=8. PDU, CRC and termination field 2 (T2) form FEC block 2, which can be coded with either S=8 or S=2. CI signals the coding of block 2. T1 and T2 are generated using a forward error correction encoder.



**Figure 4-8: Packet of coded PHYs.**

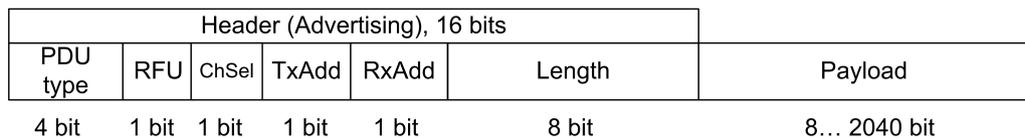
**Table 4-5: Duration of coded packets.**

	Code	Preamble	Access address	CI	T1	PDU	CRC	T2
Length in bits		80	32	2	3	16...2056	24	3
Length in $\mu$ s	S=8	80 (uncoded)	256 (S=8)	16 (S=8)	24 (S=8)	128...16448	192	24
	S=2					32...4112	48	6

With the variable length of the PDU, a coded packet is between 160 bits and 2200 bits. A coded packet with S=8 is between 720  $\mu$ s and 17040  $\mu$ s. Accordingly, with S=2 it is between 462  $\mu$ s and 4542  $\mu$ s.

#### 4.6.4.3 PDU for Advertising

The PDU for advertising consists of a header with a length of 16 bits and the actual payload (Figure 4-9).



**Figure 4-9: PDU Advertising**

Important fields:

- PDU type: defines the type of advertising/scanning: e.g. ADV\_IND for general advertising or CONN\_REQ for connection initiation
- Length: defines the length of the subsequent payload

The advertiser can broadcast four different events and thereby influence the possible actions of a scanner. As they are legacy version 4, all are available in PHY **LE 1M** only. All actions take place on the primary advertising channels:

**Table 4-6: Legacy (V4) advertising and scanner responses (primary advertising channels) (LE 1M)**

Purpose	PDU content	Scanner		Comment
		SCAN_REQ	CONNECT_IND	
General advertising	ADV_IND	yes	yes	
Direct advertising	ADV_DIRECT_IND	no	yes	Rapid connection setup for directly addressed devices
Discoverable advertising	ADV_SCAN_IND	yes	no	Dynamic user data in broadcast
Nonconnectable	ADV_NONCONN_IND	no	no	Broadcast only, e.g. beacons for positioning

Depending on the advertising event, the scanner can respond with two possible ways:

- Scan Request: request for user data via advertising channels
- Connect Request: connection setup

Version 5 additionally allows extended advertising. They are controlled directly in the Advertising Payload with an additional Extended Header.

**Table 4-7: Additional extended advertising messages in line with V5**

Purpose	PDU content	PHY			Advertising	Comment
		LE 1M	LE 2M	LE coded		
General advertising extended	ADV_EXT_IND	yes	no	yes	primary	Indicates secondary advertising. Points to an AUX packet
AUX packet	AUX_ADV_IND	yes	yes	yes	secondary	Contains secondary advertising data
Periodic advertising	AUX_SYNC_IND	yes	yes	yes		Fixed interval
Chain of data	AUX_CHAIN_IND	yes	yes	yes		Large data volumes

For this extended advertising, the version 5 introduces an extended payload format which is embedded in the standard payload and consists of an extended header.

Payload (Advertising), 1...255 octets (8...2040 bit)			
Extended Header Length	Adv Mode	Extended Header	AdvData
6 bit	2 bit	0...504 bit 0...63 octets	0...2032 bit 0...254 octets

Figure 4-10: Common extended advertising payload format

Fields:

- **Extended Header Length:** indicates the length of the Extended Header in octets (value 0...63)
- **AdvMode:** indicates the mode: connectable and / or scannable or not
- **AdvData:** the advertising data (payload)
- **Extended Header:** the extended header with variable length

Extended Header (Advertising)								
Ext Header Flags	AdvA	Target A	CTE Info	ADI	Aux Ptr	SyncInfo	TxPower	ACAD
8 bit	48 bit	48 bit	8 bit	16 bit	24 bit	144 bit	8 bit	varies

Important Fields:

- **Extended Header Flags:** Register to indicate bitwise, if associated field is present or not
- **AdvA:** Advertiser Address
- **Target A:** the target of the message
- **CTEInfo:** Constant Tone Info field for Direction Finding

The information whether and how a scanner can respond is transmitted as a data message in the ADV\_EXT\_IND or the AUX\_ADV\_IND payload. The following possibilities are available:

- Nonconnectable and nonscannable (unidirect and direct)
- Connectable (unidirect and direct)
- Scannable (unidirect and direct)

The scanner can respond only to AUX\_ADV\_IND:

- Connectable: with an AUX\_CONNECT\_REQ
- Scannable: with an AUX\_SCAN\_REQ

#### 4.6.4.4 PDU for Data

The PDU for data consists of a header with a length of 16 or 24 bits and the actual payload. A message integrity check (MIC) field can be appended (Figure 4-11). The length of the header depends on whether Direction Finding is used or not. This is encoded in the CP field.

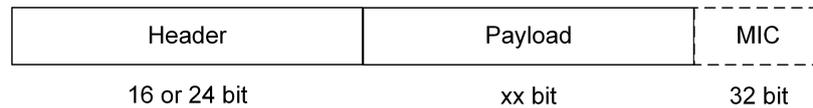


Figure 4-11: PDU format for data.

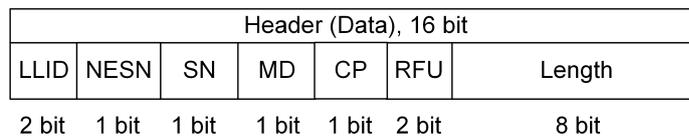


Figure 4-12: Standard Data PDU header

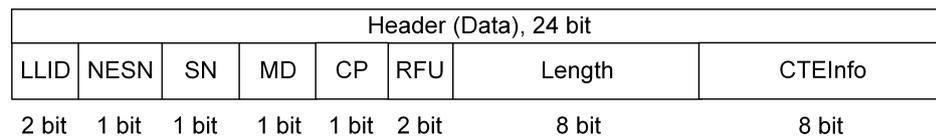


Figure 4-13: Data PDU header for direction Finding with additional CTEInfo field

Important fields:

- **LLID**: indicates whether a data or control PDU is transmitted
- Sequence number (**SN**) and next expected sequence number (**NESN**) act as flow control and acknowledgement mechanisms
- **CP**: The CTEInfo Present field indicates whether the header has a CTEInfo field and therefore uses Direction Finding with Constant Tone Extension. '0' means no CTEInfo, the header is 16 bit long. '1' means with CTEInfo, the header is 24 bit long.
- **Length**: defines the length of the payload
- **CTEInfo**: see Figure 4-14

#### 4.6.4.5 Constant Tone Extension (for Direction Finding)

The handling of the Constant Tone Extension (CTE) is controlled in the PDU in the field CTEInfo.

CTEInfo		
CTETime	RFU	CTEType
5 bit	1 bit	2 bit

Figure 4-14: CTEInfo field in PDU

Fields:

- **CTETime**: controls the duration of the CTE in 8- $\mu$ s-units via a value between 2 and 20. Thus the length can be between 16  $\mu$ s and 160  $\mu$ s.
- **CTEType**: defines the type and the switching slots.

CTEType	Description
0	AoA
1	AoD, 1 $\mu$ s slots
2	AoD, 2 $\mu$ s slots
3	Reserved

The figures below show the general timing structure of the CTE. It consists in principle always of a guard period and a reference period plus one or several switching and sample slots, which can be either 1- $\mu$ s-slots or 2- $\mu$ s-slots. The support of 2- $\mu$ s-slots is mandatory, the support of 1- $\mu$ s-slots is optional.

### Angle of Arrival

In this case, the (moving) transmitter uses continuous transmission of '1', no switching.



Figure 4-15: AoA transmit, no switching [2]

The (fixed) receiver switches between the antennas on following slots.



Figure 4-16: AoA receive, 2- $\mu$ s slots [2]

### Angle of Departure

In this case, the (fixed) transmitter uses continuous transmission of '1', but switches through the antennas.



Figure 4-17: AoD transmit, 2- $\mu$ s slots [2]

The (moving) receiver samples on the right slots, no switching necessary.



Figure 4-18: AoD receive, 2- $\mu$ s slots [2]

### 1- $\mu$ s slots

The support of 1- $\mu$ s slots is optional. the figures above are in principle the same. There are 74 sample slots.

### Transmitting CTE

- **AoA:** The transmitter has only one antenna. Thus there is no need for switching.
- **AoD:** The transmitter has two or more antennas. Thus the transmitter performs switching with the used rate.

### Receiving CTE (IQ Sampling)

- **AoA:** The receiver has two or more antennas. Thus the receiver performs switching with the used rate.
- **AoD:** The receiver has only one antenna. Thus there is no need for switching. The sampling takes place in the dedicated slots.

The receiver samples always in 1  $\mu$ s during the reference period (8 times) and during the sample slots (see slot timing (Figure 4-18)):

- **2- $\mu$ s slots:** latter 1- $\mu$ s-part only, 1...37 samples
- **1- $\mu$ s slots:** 2...74 samples

The sampling window is in the middle of the slot, thus 0.75  $\mu$ s long, for 2- $\mu$ s slots always in the latter part.

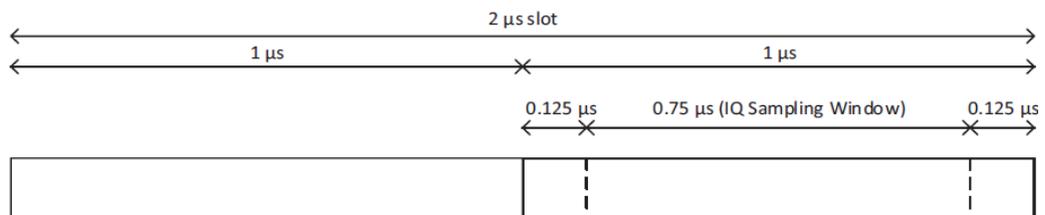


Figure 4-19: IQ sampling window. Here for a 2- $\mu$ s slot in the latter part

## 4.6.5 Time Schemes

All communications between two devices (initially) take place via advertising channels in the form of advertising events. The duration of an event lies between 20 ms and 10.24 s. Two sequential advertising PDUs should lie no more than 10 ms apart. The used advertising channel is determined by LL and can include all three channels (see Figure 4-20). Starting with Version 4.2, a high duty cycle mode is also specified for direct advertising (ADV\_DIRECT\_IND); in this case the maximum offset between two PDUs is only 3.75 ms, making a faster connection setup possible.

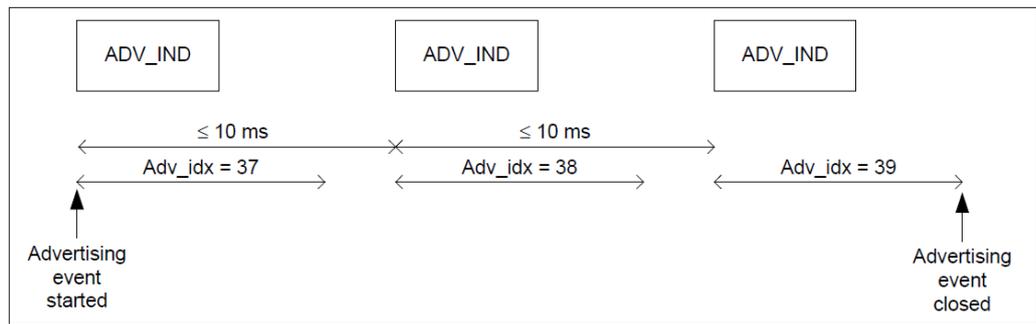


Figure 4-20: Advertising timing without scanner response [2].

Figure 4-21 shows an advertising event in which a scanner response (SCAN\_REQ) is received. The advertiser responds with a SCAN\_RSP and then transmits additional advertising PDUs.

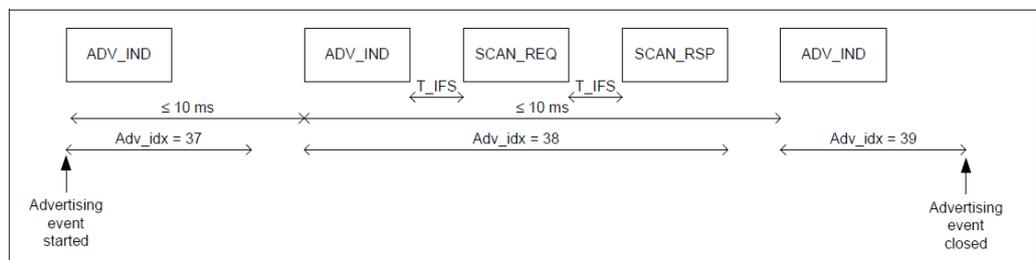


Figure 4-21: Advertising timing with scanner response: SCAN\_REQ [2].

Figure 4-22 illustrates the connection setup. In this case, the initiator transmits a CONNECT\_REQ that includes additional information about the planned connection, such as the TransmitWindowSize. Up to this point, all communications have taken place on the advertising channel. After a successful connection setup, the data exchange takes place in a packet from master to slave. After this packet, a hop is made to the next data channel (based on the hopping algorithm). Then the slave transmits, and so on.

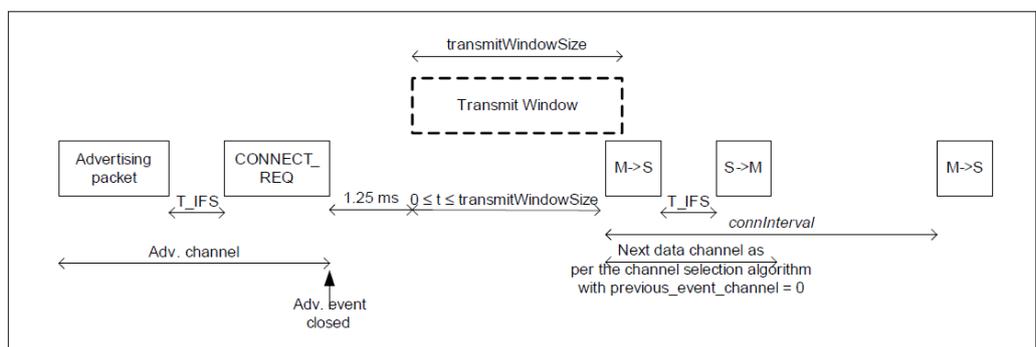


Figure 4-22: Connection setup [2].

Figure 4-23 illustrates extended advertising. The advertiser initially transmits events on the primary channels with a notification that an extended advertising (ADV\_EXT\_IN) is present. The event terminates on the primary channels and transmits an auxiliary

packet on a secondary channel (AUX\_ADV\_IND). This can then be used to transmit extended user data, for example.

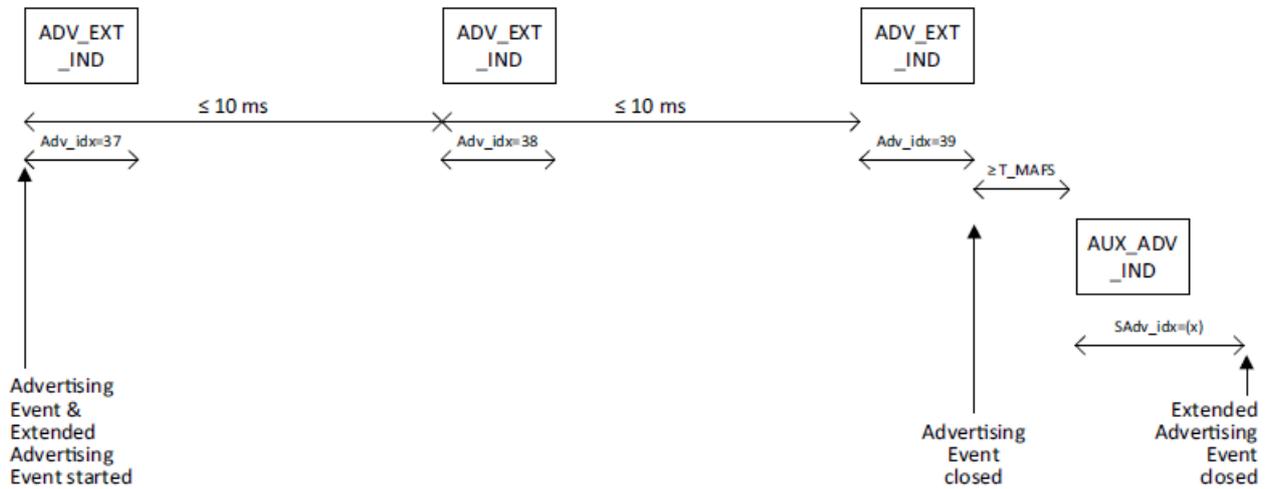


Figure 4-23: Example extended advertising event [2].

#### 4.6.6 Modulations

To keep Bluetooth LE simple, there is only a single, robust modulation mode. Just as with basic rate in Bluetooth Classic, Gaussian frequency shift keying (GFSK) is also used here. The nominal frequency deviation is ±250 kHz. This yields a gross data rate of 1 Mbit/s (LE 1M and coded PHY).

The Gaussian filter BT is 0.5 (which is the same as Basic Rate). The modulation index lies between 0.45 and 0.55.

Version 5 introduces a new optional PHY with a nominal frequency deviation of ±500 kHz, resulting in a gross data rate of 2 Mbit/s (LE 2M).

##### Stable modulation index (SMI)

The stable modulation index is also optional. Devices guarantee a modulation index of between 0.495 and 0.505, providing a more accurate frequency deviation and thus increasing the possible range. This is possible for all PHYs.

#### 4.6.7 RF Measurements

In addition to Core specification [2], the R PHY [4] Bluetooth Test Specification defines the qualification tests for physical layer 1 of Bluetooth LE.

Bluetooth LE defines a direct test mode for these tests; this mode directly controls the DUT via HCI or UART. A direct test mode control via signalling over the RF interface is not possible. Reports from the DUT such as a status or the PER are transferred directly from the DUT to the tester.

The Bluetooth LE RF PHY specification in version 4 describes a couple of fundamental tests. Version 5 extends these tests to all PHYs. Version 5.1 adds tests for direction finding with constant tone extension (CTE and AoA / AoD).

**Tx tests**

- Output Power
- In-band emissions
- Modulation characteristics
- Carrier frequency offset and drift
- Output power with CTE
- Carrier frequency offset and drift with CTE
- Tx Power Stability, AoD Transmitter
- Antenna switching integrity, AoD Transmitter

**Rx tests**

- Receiver sensitivity
- C/I and Receiver Selectivity Performance
- Blocking Performance
- Maximum input signal level
- PER Report Integrity
- IQ Samples Coherency, AoD Receiver
- IQ Samples Coherency, AoA Receiver
- IQ Samples Dynamic Range, AoD Receiver
- IQ Samples Dynamic Range, AoA Receiver

These fundamental tests are repeated for the various PHYs. [Table 4-8](#) to [Table 4-12](#) provide an overview. The transmitter tests are named **RF-PHY/TRM/.../BV-xx-C** and the receiver tests are named **RF-PHY/RCV/.../BV-xx-C**. The corresponding numerals in the respective tables have to be inserted. All tests listed below are nonhopping, they have to be performed on single RF channels. SMI is the abbreviation for stable modulation index.

**Table 4-8: Mapping Transmitter test to the individual PHYs (RF-PHY/TRM/BV-xx-C)**

Test	LE 1M 1 Ms/s	LE 2M 2 Ms/s	LE 1M 1 Ms/s SMI	LE 2M 2 Ms/s SMI	Coded 1 Ms/s S =2	Coded 1 Ms/s S=8	Coded 1 Ms/s SMI S=2	Coded 1 Ms/s SMI S=8
Output power	01							
In-band emission	03	08						
Modulation characteristics	05	10	09	11		13		
Carrier frequency offset and drift	06	12				14		

**Table 4-9: Mapping Transmitter tests with Constant Tone Extension (CTE) (RF-PHY/TRM/BV-xx-C)**

Test	LE 1M 1 Ms/s	LE 2M 2 Ms/s
Output power with CTE	15	
Carrier frequency offset and drift with CTE	16	17

**Table 4-10: Mapping AoD Transmitter tests**

Test		LE 1M 1 Ms/s		LE 2M 2 Ms/s	
		2- $\mu$ s slots	1- $\mu$ s slots	2- $\mu$ s slots	1- $\mu$ s slots
Tx Power Stability AoD Transmitter	RF-PHY/TRM/PS/BV-xx-C	01	02	03	04
Antenna switching integrity AoD Transmitter	RF-PHY/TRM/ASI/BV-xx-C	05	06	07	08

**Table 4-11: Mapping Receiver test to the individual PHYs (RF-PHY/RCV/BV-xx-C)**

Test	LE 1M 1 Ms/s	LE 2M 2 Ms/s	LE 1M 1 Ms/s SMI	LE 2M 2 Ms/s SMI	Coded 1 Ms/s S =2	Coded 1 Ms/s S=8	Coded 1 Ms/s SMI S=2	Coded 1 Ms/s SMI S=8
Receiver sensitivity	01	08	14	20	26	27	32	33
C/I and receiver sensitivity	03	09	15	21	28	29	34	35
Blocking performance	04	10	16	22				
Intermodulation performance	05	11	17	23				
Maximum input signal level	06	12	18	24				
PER report integrity	07	13	19	25	30	31	36	37

**Table 4-12: Mapping AoX Receiver tests**

Test		LE 1M 1 Ms/s		LE 2M 2 Ms/s	
		2- $\mu$ s slots	1- $\mu$ s slots	2- $\mu$ s slots	1- $\mu$ s slots
IQ Samples Coherency AoD Receiver	RF-PHY/RCV/IQC/BV-xx-C	01	02	03	04
IQ Samples Coherency AoA Receiver		05		06	
IQ Samples Dynamic Range AoD Receiver	RF-PHY/RCV/IQDR/BV-xx-C	07	08	09	10
IQ Samples Dynamic Range AoA Receiver		11		12	

All of the tests listed above can be performed using the R&S<sup>®</sup>CMW radio communication tester platform. Some tests require additional test instruments.

For preformance tests, Rohde & Schwarz also offers an automated test solution with the R&S<sup>®</sup>CMWrun sequencer tool.

Because Bluetooth must share the ISM band with other wireless standards, additional coexistence tests in addition to the required tests are useful. Those tests are available with the R&S<sup>®</sup>CMW platform.

## 5 Summary

The chapters above have provided a detailed description of the two different Bluetooth standards. [Table 5-1](#) summarizes and compares the most important of these parameters.

**Table 5-1: Comparison of Classic and Low Energy**

Comparison of Classic and Low Energy		
	Classic (BR/EDR)	Low Energy (LE)
Application	Cell phones, headsets, stereo/audio streaming, automotive (handsfree), PCs, etc.	Smartwatches, sport & fitness, home electronics, automation, industry, healthcare, smartphones, etc.
Voice	Yes	No
RF band ISM	2.4 GHz	2.4 GHz
Energy consumption	Reference	0.5...0.01 times Classic as reference
Coverage	10 m	≥ 10 m
Power	3 classes (max.): <ul style="list-style-type: none"> <li>• +20 dBm</li> <li>• +4 dBm</li> <li>• 0 dBm</li> </ul>	max. + 20 dBm four informative classes
Connection	Inquiry Yes, always hopping	Advertising Connection only if necessary, then hopping
Connection setup	100 ms	6 ms
RF channels	79 with 1 MHz spacing	40 with 2 MHz spacing <ul style="list-style-type: none"> <li>• 3 advertising</li> <li>• 37 data (+ secondary advertising)</li> </ul>
Modulation	GFSK <ul style="list-style-type: none"> <li>• BT = 0.5</li> <li>• Deviation = 160 kHz</li> <li>• Mod index = 0.28...0.35</li> </ul> $\pi/4$ -DQPSK 8DPSK	GFSK <ul style="list-style-type: none"> <li>• BT = 0.5</li> <li>• Deviation = 250 kHz or 500 kHz</li> <li>• Mod index = 0.45...0.55</li> <li>• Stab Mod index = 0.495...0.505</li> </ul>
Gross data rate	1...3 Mbit/s	1...2 Mbit/s
Application data rate	0.7...2.1 Mbit/s	0.2...0.6 Mbit/s
Direction Finding	no	yes

## 6 Appendix

### 6.1 Abbreviations

ACL - asynchronous connectionless link
AFH - adaptive frequency hopping
AoA - Angle of Arrival
AoD - Angle of Departure
BB - baseband
BR - basic rate
BQTF - Bluetooth qualification and test facility
BT - bandwidth time product
CRC - cyclic redundancy check
CTE - Contant Tone Extension
EDR - enhanced data rate
GAP - generic access profile
GATT - generic attribute profile
HCI - host controller interface
HS - high speed
IPS - Indoor Positioning Service
ISM - industrial scientific medical band
LE - low energy
LL - link layer
PDU - protocol data unit
PER - packet error rate
PHY - physical layer
RF - radio frequency
RTLS- Real Time Location Service
SDP - service discovery application profile
SCO - synchronous connection-oriented link
TDD - time division duplex

## 6.2 Literature

- [1] ABI research Bluetooth Market Watch. - 2016.
- [2] Bluetooth Sig Bluetooth Core Package version: 5.1. - January 2019.
- [3] Bluetooth Sig. Bluetooth Test Specification: Radio Frequency (RF) // RF.TS.4.2.3. - July 2016.
- [4] Bluetooth Sig. Bluetooth Test Specification: Radio Frequency (RF) // RF-PHY.TS. 5.1.0. - November 2018.
- [5] Rohde & Schwarz Advanced Bluetooth RF Tests with RS CMWrun [Application Note, 1MA261]. - 2015.

## 6.3 Additional Information

Please send your comments and suggestions regarding this white paper to  
[TM-Applications@rohde-schwarz.com](mailto:TM-Applications@rohde-schwarz.com)

## 7 Rohde & Schwarz

The Rohde & Schwarz electronics group offers innovative solutions in the following business fields: test and measurement, broadcast and media, secure communications, cybersecurity, monitoring and network testing. Founded more than 80 years ago, the independent company has an extensive sales and service network with locations in more than 70 countries.

The electronics group ranks among the world market leaders in its established business fields. The company is headquartered in Munich, Germany. It also has regional headquarters in Singapore and Columbia, Maryland, USA, to manage its operations in these regions.

### Sustainable product design

- Environmental compatibility and eco-footprint
- Energy efficiency and low emissions
- Longevity and optimized total cost of ownership



### Contact us

- Europe, Africa, Middle East | [customersupport@rohde-schwarz.com](mailto:customersupport@rohde-schwarz.com)  
+49 89 4129 12345
- North America | [customer.support@rsa.rohde-schwarz.com](mailto:customer.support@rsa.rohde-schwarz.com)  
1-888-TEST-RSA (1-888-837-8772)
- Latin America | [customersupport.la@rohde-schwarz.com](mailto:customersupport.la@rohde-schwarz.com)  
+1-410-910-7988
- Asia Pacific | [customersupport.asia@rohde-schwarz.com](mailto:customersupport.asia@rohde-schwarz.com)  
+65 65 13 04 88
- China | [customersupport.china@rohde-schwarz.com](mailto:customersupport.china@rohde-schwarz.com)  
+86-800-810-8228 / +86-400-650-5896

### Rohde & Schwarz GmbH & Co. KG

Mühldorfstraße 15 | D - 81671 München

+ 49 89 4129 - 0 | Fax + 49 89 4129 – 13777

[www.rohde-schwarz.com](http://www.rohde-schwarz.com)

This application note and the supplied programs may only be used subject to observance of the conditions of use set forth in the download area of the Rohde & Schwarz website.

R&S® is a registered trademark of Rohde & Schwarz GmbH & Co. KG. Trade names are trademarks of their owners.