Bluetooth Low Energy (Bluetooth Smart)

References

[1] Specification **Core Version 4.0**:
http://www.bluetooth.org/Technical/Specifications/adopted.htm

[2] wikipedia, „Bluetooth“, March 2012, http://de.wikipedia.org/wiki/Bluetooth

[3] wikipedia, „Bluetooth“, March 2012, http://en.wikipedia.org/wiki/Bluetooth

[4] online training (registration required):
https://www.bluetooth.org/events/training/lowenergytraining.htm

Introduction

[3] „**Bluetooth Low Energy** (BLE), previously known as **WiBree**, is a subset to Bluetooth v4.0 with an entirely new protocol stack for rapid build-up of simple links. As an alternative to the Bluetooth standard protocols that were introduced in Bluetooth v1.0 to v3.0, it is aimed at very low power applications running off a coin cell. Chip designs allow for two types of implementation, dual-mode, single-mode …. The provisional names *Wibree* and *Bluetooth **ULP*** (Ultra Low Power) were abandoned and the BLE name was used for a while. In late 2011, new logos “Bluetooth Smart Ready” for hosts and “**Bluetooth Smart**” for sensors were introduced as the general-public face of BLE.

In a single mode implementation the low energy protocol stack is implemented solely. CSR, Nordic and TI (and EM) have released single mode Bluetooth low energy solutions.

In a dual-mode implementation, Bluetooth low energy functionality is integrated into an existing Classic Bluetooth controller. Currently (2011-03) the following semiconductor companies have announced the availability of chips meeting the standard: Atheros, CSR, Broadcom and TI. The compliant architecture shares all of Classic Bluetooth's existing radio and functionality resulting in a negligible cost increase compared to Classic Bluetooth.

Cost-reduced single-mode chips, which enable highly integrated and compact devices, feature a lightweight Link Layer providing ultra-low power idle mode operation, simple device discovery, and reliable point-to-multipoint data transfer with advanced power-save and secure encrypted connections at the lowest possible cost.“

Introduction: Overview

[1], Volume 1, Part A, Chapter 1.2, pp. 20-22

School of Engineering
NTM, BLE, 3

LE devices may fulfill the entire communication in the case of **unidirectional or broadcast communication** using advertising events.

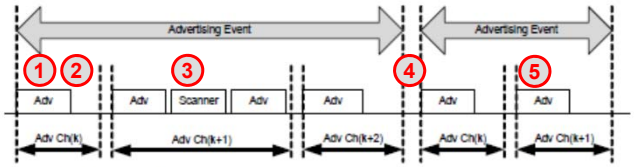


Figure 1.3: Advertising Events

1. **Advertiser transmits advertising packets on up to 3 advertising channels.**
2. **Scanners receive advertising without the intention to connect to the advertiser.**
3. **Scanner may make a scan request to the advertiser to get „more information“**
4. **Advertiser „periodically“ restarts an advertising event**
5. **Advertiser may end the advertising event at any time during the event.**

Introduction: Overview

[1], Volume 1, Part A, Chapter 1.2, pp. 20-22

School of Engineering
NTM, BLE, 4

LE devices may use advertising events to establish pair-wise **bi-directional communication** using data channels.

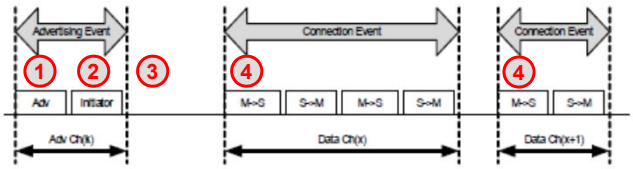


Figure 1.4: Connection Events

1. **Advertiser sends connectable advertising packets**
2. **Initiator sends a connection request (and advertiser accepts it)**
3. **connection is established (initiator => master M, advertiser => slave S)**
4. **connection events are used to send data packets between M and S (alternating)**
   M initiates the beginning of each connection event and can stop it at any time.
   (Adaptive) frequency hopping is used over 37 data channels.

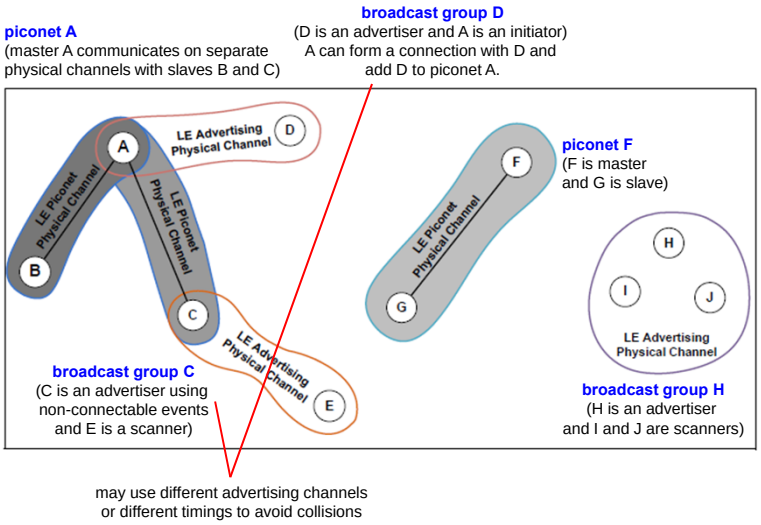
Introduction: Overview

[1], Volume 1, Part A, Chapter 4.1.2, pp. 75

School of Engineering

NTM, BLE, 5

LE Topology

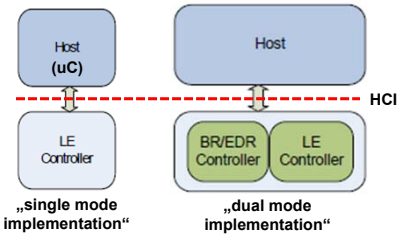


Introduction

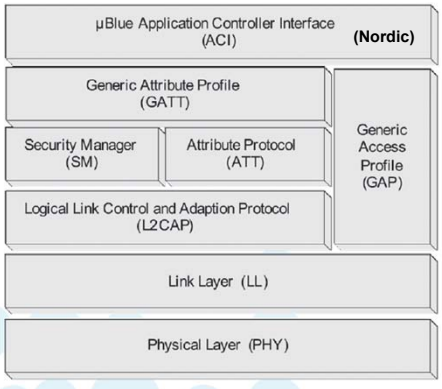
School of Engineering

NTM, BLE, 6

Host and Controller Combinations



Protocol Stack (nRF8001)*



*** Other single mode BLE-chip (Master or Slave)**
CC2540 (TI), EM9301 (EM)

Radio Specification

[1], Volume 6, Part A

School of Engineering
NTM, BLE, 7

Frequency Bands and Channel Arrangement

Regulatory Range	RF Channels
2.400-2.4835 GHz	f=2402+k*2 MHz, k=0, ,39

40 RF channels with 2 MHz spacing

Transmission Power

Minimum Output Power	Maximum Output Power
0.01 mW (-20 dBm)	10 mW (+10 dBm)

single mode Bluetooth Smart chip typ. has max. output power of 0 dBm

less output power to optimize power consumption or reduce interference

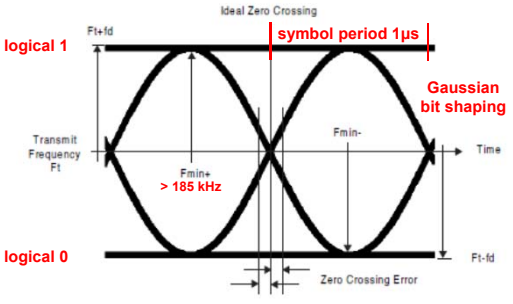
Radio Specification

[1], Volume 6, Part A

School of Engineering
NTM, BLE, 8

Modulation: GFSK (Gaussian Frequency Shift Keying)

BT = 0.5, symbol rate: 1 MSps, gross air bit rate: 1 Mbps



Receiver Sensitivity

<= -70 dBm to achieve a BER = 0.1%

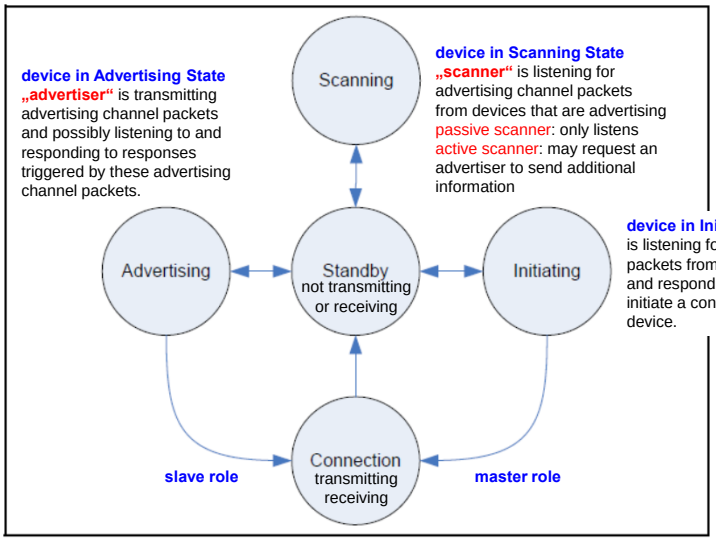
Example: Rx sensitivity of Nordic nRF8001 (slave) < - 85 dBm, which is slightly better than Rx sensitivity of Bluetooth BR/EDR products e.g. -84 dBm of ConnectBlue's Bluetooth Serial Port Adapter OBS411

Link Layer States

[1], Volume 6, Part B

School of Engineering

NTM, BLE, 9



device in Advertising State
„advertiser“ is transmitting advertising channel packets and possibly listening to and responding to responses triggered by these advertising channel packets.

device in Scanning State
„scanner“ is listening for advertising channel packets from devices that are advertising
passive scanner: only listens
active scanner: may request an advertiser to send additional information

device in Initiating State „initiator“ is listening for advertising channel packets from a specific device(s) and responding to these packets to initiate a connection with another device.

Figure 1.1: State diagram of the Link Layer state machine
The Link Layer may have multiple instances of the Link Layer state machine (certain combination are prohibited).

Link Layer

[1], Volume 6, Part B

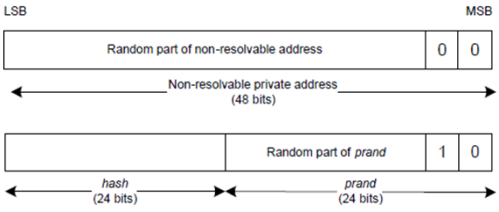
School of Engineering

NTM, BLE, 10

48 bit Device Address

public device address (in accordance with IEEE 802-2001 standard)

random device address (resolvable and non-resolvable private address)



Privacy feature to reduce the ability to track a LE device
by changing the Bluetooth device address on a frequent basis.

Link Layer
[1], Volume 6, Part B

School of Engineering
NTM, BLE, 11

Advertising physical channel uses 3 RF channels

for discovering devices, initiating a connection and broadcasting data

Data physical channel uses up to 37 RF channels

for communication between connected devices

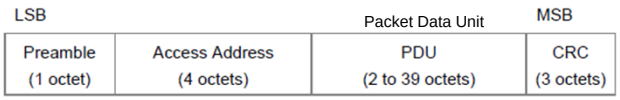
RF Channel	RF Center Frequency	Channel Type	Data Channel Index	Advertising Channel Index
0	2402 MHz	Advertising channel		37
1	2404 MHz	Data channel	0	
2	2406 MHz	Data channel	1	
...		Data channels		
11	2424 MHz	Data channel	10	
12	2426 MHz	Advertising channel		38
13	2428 MHz	Data channel	11	
14	2430 MHz	Data channel	12	
...		Data channels		
38	2478 MHz	Data channel	36	
39	2480 MHz	Advertising channel		39

Table 1.2: Mapping of RF Channel to Data Channel Index and Advertising Channel Index

Link Layer
[1], Volume 6, Part B

School of Engineering
NTM, BLE, 12

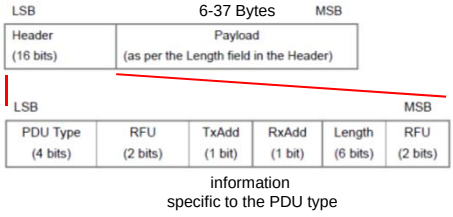
One packet format for both advertising channel and data channel



Preamble for frequency synchronization, symbol timing estimation, and Automatic Gain Control (AGC) training

Access Address fixed for advertising channel packets and random for data channel packets (and different for link layer connections)

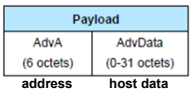
Advertising Channel PDU



Link Layer
[1], Volume 6, Part B

School of Engineering
NTM, BLE, 13

Advertising Channel PDU types



PDU Type $b_3b_2b_1b_0$	Packet Name	
0000	ADV_IND	connectable undirected advertising event
0001	ADV_DIRECT_IND	connectable directed advertising event
0010	ADV_NONCONN_IND	non-connectable undirected advertising event
0011	SCAN_REQ	scan request
0100	SCAN_RSP	scan response
0101	CONNECT_REQ	connection request
0110	ADV_SCAN_IND	scannable undirected advertising event
0111-1111	Reserved	

Link Layer
[1], Volume 6, Part B

School of Engineering
NTM, BLE, 14

Advertising Channel PDU types (continued)

Advertising Event Type	PDU used in this advertising event type	Allowable response PDUs for advertising event	
		SCAN_REQ	CONNECT_REQ
Connectable Undirected Event	ADV_IND	YES	YES
Connectable Directed Event	ADV_DIRECT_IND	NO	YES*
Non-connectable Undirected Event	ADV_NONCONN_IND	NO	NO
Scannable Undirected Event	ADV_SCAN_IND	YES	NO

Table 4.1: Advertising event types, PDUs used and allowable response PDUs

*** only the correctly addressed initiator may respond.**

Link Layer
[1], Volume 6, Part B

School of Engineering
NTM, BLE, 15

Data Channel PDU

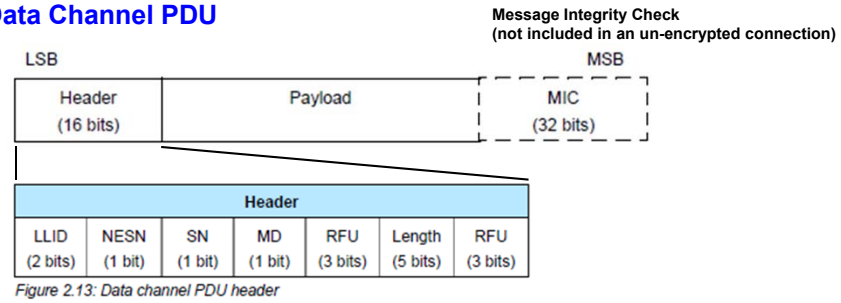


Figure 2.13: Data channel PDU header

Logical Link ID indicates whether the packet is an LL Data PDU (to send L2CAP data) or an LL Control PDU (to control the Link Layer connection).

NSEN Next Expected Sequence Number

SN Sequence Number

MD More Data

Length indicates the size, in octets, of the Payload and MIC, if included.

Link Layer
[1], Volume 6, Part B

School of Engineering
NTM, BLE, 16

Device Filtering

The set of devices that the Link Layer uses for device filtering is called the **White List**.

The White List is configured by the Host and is used by the Link Layer to filter *advertisers*, *scanners* or *initiators*.

This allows the Host to configure the Link Layer to act on a request without awakening the Host.

Link Layer
[1], Volume 6, Part B

School of Engineering
NTM, BLE, 17

Advertising Event Timing

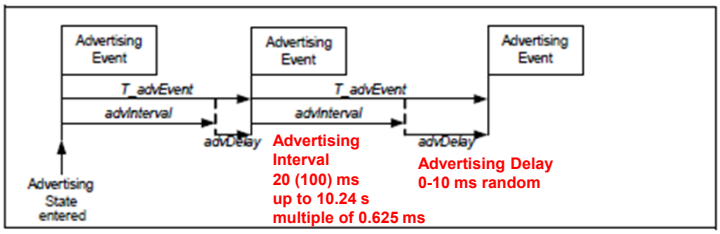


Figure 4.1: Advertising events perturbed in time using advDelay

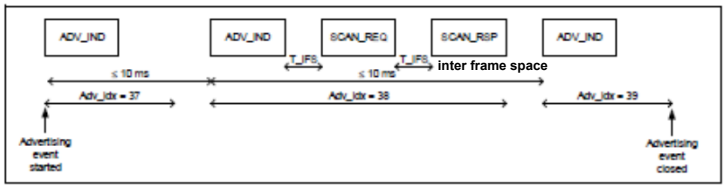
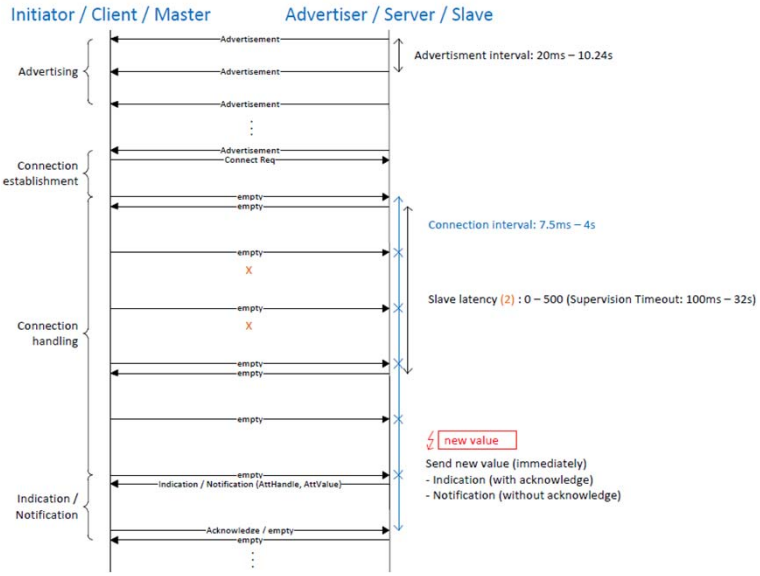


Figure 4.3: Connectable undirected advertising event with SCAN_REQ and SCAN_RSP PDUs in the middle of an advertising event

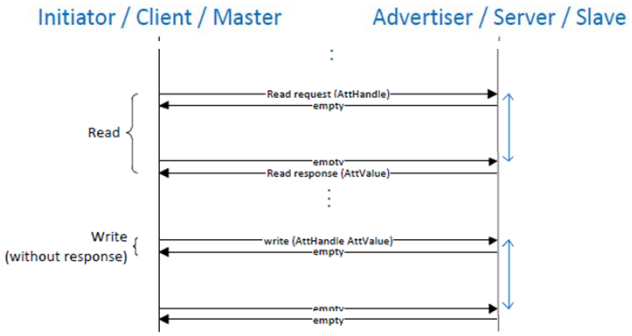
Link Layer (L2CAP, ATT)

School of Engineering
NTM, BLE, 18



Link Layer, (L2CAP, ATT)

School of Engineering
NTM, BLE, 19



slave latency
Slave latency allows a slave to use a reduced number of connection events.
The connSlaveLatency parameter (set to 2 in the example) defines the number of consecutive connection events that the slave device is not required to listen for the master.

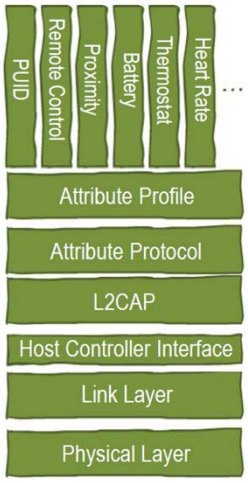
LE System Architecture

Source Bluetooth SIG

School of Engineering
NTM, BLE, 20

Layered Architecture:

- Device Profiles – what can we do…
- Attribute Profile – how things are organized
- Attribute Protocol – protocol for accessing data
- L2CAP – multiplexor
- HCI – interface between Host and Controller
- Link Layer – packets and control
- Physical Layer – transmits/receives bits



Current Consumption (Example)

Nordic nRF8001, Rev. C (newest rev is D)

Input

Connection inteval	200.00 ms
Advertising interval	5000.000 ms
Master clock accuracy (ppm)	10

Configuration settings

Slave clock accuracy (ppm)	250
DC/DC enabled	No
Slave Latency	0
Advertising payload	0
Device security	No security

90% of the time advertising
10% of the time in a connection

Average current consumption:	11.61 µA
From RF	5.39 µA
From link layer	2.77 µA
From host processing	0.95 µA
From idle	2.50 µA
From sleeping:	0.00 µA
Batter Lifetime	
Battery capacity (mAh):	220
Battery lifetime (hours):	18951.24
Battery lifetime (years):	**2.16**

LE versus Classic Bluetooth Technology

Source Bluetooth SIG

Technical Specification	Classic *Bluetooth* technology	*Bluetooth* low energy technology
Radio frequency	2.4 GHz	2.4 GHz
Distance/Range	10 meters	50 meters
Over the air data rate	1 - 3 Mbps	1 Mbps
Application throughput	0.7 - 2.1 Mbps	0.2 Mbps
Nodes/Active slaves	7	Unlimited
Security	64b/128b and application layer user defined	128b AES and application layer user defined **key generation in the host**
Robustness	Adaptive fast frequency hopping, FEC, fast ACK	Adaptive fast frequency hopping
Latency (from a non connected state)		
Total time to send data (det. battery life)	100 ms	<3 ms
Government regulation	Worldwide	Worldwide
Certification body	Bluetooth SIG	Bluetooth SIG
Voice capable	Yes	No
Network topology	Scatternet	Star-bus
Power consumption	1 as the reference	0.01 to 0.5 (depending on use case)
Peak current consumption	<30 mA	<15 mA (max 15 mA to run on coin cell battery)
Service discovery	Yes	Yes
Profile concept	Yes	Yes
Primary use cases	Mobile phones, gaming, headsets, stereo audio streaming, automotive, PCs, etc.	Mobile phones, gaming, PCs, watches, sports & fitness, healthcare, automotive, Home electronics, automation, industrial, etc.