BLE sniffer guide

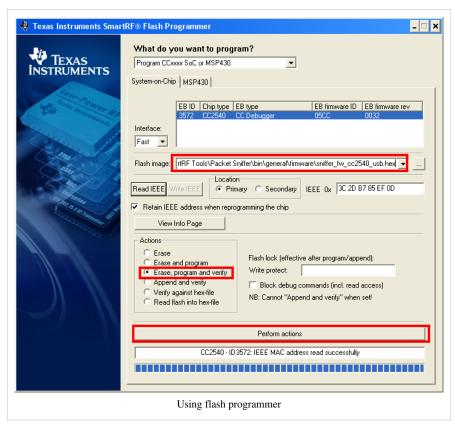
Bluetooth Low Energy Wiki Main Page [1]

Introduction

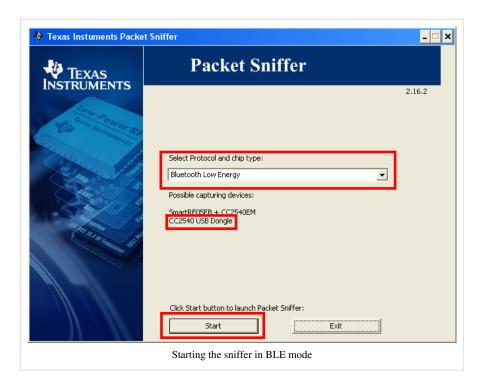
The TI Packet Sniffer can be used to look at everything that goes on between two BLE devices over the air, and is as such a good tool for debugging or just learning about Bluetooth Low Energy applications.

Installation and setup, using a CC2540 USB dongle as sniffer hardware

- 1. Download and install the SmartRF Packet Sniffer from [2]
- 2. Using SmartRF Flash Programmer, program the CC2540 USB dongle with the image found in \program files\Texas Instruments\SmartRF Tools\Packet Sniffer\bin\general\firmware\sniffer_fw_cc2540_usb.hex after installation.

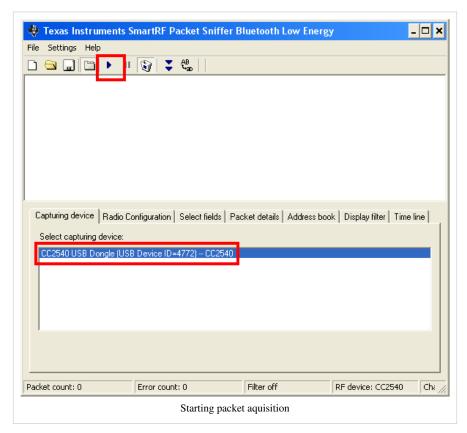


3. Start the sniffer, select Bluetooth Low Energy and press Start



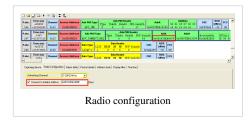
Using the sniffer

To start sniffing, select the now programmed USB dongle, and press the play button.



The received packets will be parsed according to the packet format laid out in the Bluetooth 4.0 Core Specification[3] Volume 6, Part B, chapters 2.1, 2.3 and 2.4.

Radio configuration pane



In the radio configuration pane you can

- Specify which initiator IEEE address' connection you want to follow in the case that there are multiple BLE devices active (red ring). Otherwise the first detected connection establishment will be followed. You will still see all advertisement data.
- Specify which advertisement channel you want to listen to (yellow).

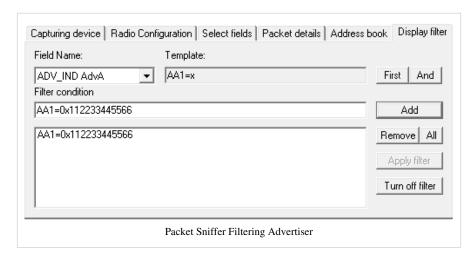
Address book

TODO

Display filter

Filter on Unique Advertiser

Choose "ADV_IND AdvA" and press button "First", then add the address where x is, so the line says ex. AA1=0x112233445566. Then press "Add" followed by "Apply filter".



You should now only see advertiser with address 0x112233445566.

Timeline

TODO

Packet types

According to the state the device is in, different communication channels are applicable.

- Advertising channel: 37 (2402MHz), 38 (2426 MHz) and 39 (2480 MHz)
- Data channel: 0-36 (2404-2478 MHz) excluding (2426 MHz)

The advertising channel and data channel allow different Protocol Data Unit (PDU) types

PDU Types

Channel	State	PDU Type	Explanation	Core spec chapter
Advertising	Advertising	ADV_IND	Connectable undirected advertising event. Contains AdvA and AdvData.	6.B.2.3.1.1 // 6.B.4.4.2.3 // 3.C.11 // 3.C.18.1 (payload)
		ADV_DIRECT_IND	Connectable directed advertising event. Contains AdvA and InitA	6.B.2.3.1.2 // 6.B.4.4.2.4
		ADV_NOCONN_IND	Broadcast. Contains AdvA and AdvData	6.B.2.3.1.3 // 6.B.4.4.2.6
		ADV_SCAN_IND	Connectable directed advertising event. Scannable.	6.B.2.3.1.4 // 6.B.4.4.2.5
	Scanning	ADV_SCAN_REQ	Request for more information from LL in scanning state. ScanA, AdvA.	6.B.2.3.2.1 // 6.B.4.4.2.5
	Advertising	ADV_SCAN_RSP	Response.	6.B.2.3.2.2 // 6.B.4.4.3.2
	Initiating	CONNECT_REQ	Sent by initiator to establish a connection	6.B.2.3.3.1 // 6.B.4.4.4
Data	Data	LLID field is 1 or 2. Empty PDUs allow the slave to respond with any PDU.	General data	6.B.2.4 // 6.B.4.5
	Control	LLID field is 3. PDU can not be emtpy	Control data, see core spec	6.B.2.4.2 // 6.B.4.5

Advertisement packets

You will immediately start receiving captured advertisement packets, given that a peripheral is advertising. Fields 1,2,3,4 and 9,10,11 are common to all captured packets.



Explanation for advertisement packet fields.

Field #	Source	Explanation	Core spec chapter
1	Sniffer	Packet number as logged by the sniffer	
2	Capture device	Time in microseconds since last packet was received and absolute time	
3	Capture device	Radio channel data was captured on	6.B.1.4.1
4	Air	Bluetooth spec specified address for advertising and scan response	6.B.2.1.2
5	Air	Type of advertisement packet	6.B.2.3
6	Air	Header	6.B.2.3
7	Air	Advertiser IEEE address	6.B.2.3
8	Air	Advertisement data. In this example it's capabilities and three UUIDs the device provides.	6.B.2.3 / 3.C.11 / 3.C.18.1
9	Air	Precalculated CRC checksum	6.B.2.1.4
10	Capture device	Received signal strength indicator.	
11	Capture device	Field Control Sequence. If OK, the checksum is correct	

The advertisement fields are further explained in 6.B.2.3 on page 2202 of the BT core spec.

Scan request / response

Scan request and response are two other types specified in 6.B.2.3, and look like the image below in the sniffer. The example below is of Active scan, and a sequence diagram is found in 6.D.4.2.



Here we can see that immediately following an advertisement indication (366µs), in the same advertisement event when the peripheral goes into RX mode, another device sends a scan request, which is then immediately answered by the peripheral device. The scan response in this instance is "Keyfobdemo"

Connection establishment

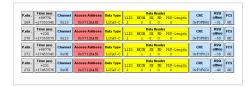
Connection establishment is initiated by the initiator (sic) on the peripheral RX slot of an advertisement event. The message format of the connection request is described in 6.B.2.3.3 in the Bluetooth core spec[3], and a message sequence diagram can be found in 6.D.5.1.



Here we see that Bluetooth LE connection establishment is pretty fast. Packet #185 shows an advertisement event peripheral TX slot, #186 shows connection request in the peripheral RX slot in the same event. Now the link is established. This is followed 20ms later by the first Central device initiated connection event's TX slot in #187, followed by a peripheral answer in #188 in the same connection event.

Empty connection events

After connection establishment we are in the connected state as defined by 6.B.4.5 in the BT Core spec. The data header is defined in 6.B.2.4 and is summarized below.



Data header

Field	Long name	Explanation	Core spec chapter
LLID	Link Layer ID	0x1 = Data PDU; continued fragment or emtpy, 0x2 Data PDU Start of fragmented data or complete message, 0x3 Control PDU.	6.B.2.4 / 6.B.4.5
NESN	Next expected sequence number	1-bit, used with SN for ack/nack	6.B.2.4 / 6.B.4.5.9
SN	Sequence number	1-bit, used with NESN for ack/nack	6.B.2.4 / 6.B.4.5.9
MD	More Data	Used to indicate whether more data is coming. See table in spec.	6.B.4.5.6
PDU Length	Length of payload + MIC in octets.	PDU Length is maximum 27 octets. MIC 4 octets if present.	6.B.2.4

In this example we can see that the central device has SN = NESN indicating new data, and the peripheral device responds with ACK (SN!=NESN because it expects next packet).

Read request, read response

TODO

Write request, write response

TODO

References

- [1] http://processors.wiki.ti.com/index.php/Category:BluetoothLE
- [2] http://www.ti.com/tool/packet-sniffer
- [3] http://www.bluetooth.org/docman/handlers/downloaddoc.ashx?doc_id=229737

Article Sources and Contributors

BLE sniffer guide Source: http://processors.wiki.ti.com/index.php?oldid=135419 Contributors: A.normann, JLindh, Sandeepkamath

Image Sources, Licenses and Contributors

File:flashprogrammer.png Source: http://processors.wiki.ti.com/index.php?title=File:Flashprogrammer.png License: unknown Contributors: A.normann

File:startsniffer.png Source: http://processors.wiki.ti.com/index.php?title=File:Startsniffer.png License: unknown Contributors: A.normann

File:using select start.png Source: http://processors.wiki.ti.com/index.php?title=File:Using select start.png License: unknown Contributors: A.normann

File:using_radio_conf.png Source: http://processors.wiki.ti.com/index.php?title=File:Using_radio_conf.png License: unknown Contributors: A.normann

File:packetsniffer_filter.png Source: http://processors.wiki.ti.com/index.php?title=File:Packetsniffer_filter.png License: unknown Contributors: JLindh

Image: Using capt adv.png Source: http://processors.wiki.ti.com/index.php?title=File:Using_capt_adv.png License: unknown Contributors: A.normann

Image: Using scan req.png Source: http://processors.wiki.ti.com/index.php?title=File:Using_scan_req.png License: unknown Contributors: A.normann

Image: Using conn est.png Source: http://processors.wiki.ti.com/index.php?title=File:Using_conn_est.png License: unknown Contributors: A.normann

Image: Using empty conn ev.png Source: http://processors.wiki.ti.com/index.php?title=File: Using_empty_conn_ev.png License: unknown Contributors: A.normann

License

THE WORK (AS DEFINED BELOW) IS PROVIDED UNDER THE TERMS OF THIS CREATIVE COMMONS PUBLIC LICENSE ("CCPL" OR "LICENSE"). THE WORK IS PROTECTED BY COPYRIGHT AND/OR OTHER APPLICABLE LAW. ANY USE OF THE WORK OTHER THAN AS AUTHORIZED UNDER THIS LICENSE OR COPYRIGHT LAW IS PROHIBITED.

BY EXERCISING ANY RIGHTS TO THE WORK PROVIDED HERE, YOU ACCEPT AND AGREE TO BE BOUND BY THE TERMS OF THIS LICENSE. TO THE EXTENT THIS LICENSE MAY BE CONSIDERED TO BE A CONTRACT, THE LICENSOR GRANTS YOU THE RIGHTS CONTAINED HERE IN CONSIDERATION OF YOUR ACCEPTANCE OF SUCH TERMS AND CONDITIONS.

License

1. Definitions

- "Adaptation" means a work based upon the Work, or upon the Work and other pre-existing works, such as a translation, adaptation, derivative work, arrangement of music or other alterations of a literary or artistic work, or phonogram or performance and includes cinematographic adaptations or any other form in which the Work may be recast, transformed, or adapted including in any form recognizably derived from the original, except that a work has not performance and includes cinematographic adaptations or any other form in which the Work in which the Work is a musical work, performance or phonogram, the synchronization of the Work in time-develation with a moving image ("synchrigh") will be considered an Adaptation for the purpose of this License." To the considered in the works in the wor

2. Fair Dealing Rights

Nothing in this License is intended to reduce, limit, or restrict any uses free from copyright or rights arising from limitations or exceptions that are provided for in connection with the copyright protection under copyright law or other applicable laws.

to the terms and conditions of this License, Licensor hereby grants You a worldwide, royalty-free, non-exclusive, perpetual (for the duration of the applicable copyright) license to exercise the rights in the Work as stated

- to Reproduce the Work, to incorporate the Work into one or more Collections, and to Reproduce the Work as incorporated in the Collections; to create and Reproduce Adaptations provided that any such Adaptation, including any translation in any medium, takes reasonable steps to clearly label, demarcate or otherwise identify that changes were made to the original Work. For example, a translation could be marked "The original work was translated from English to Spanish," or a modification could indicate "The original work has been modified."; to Distribute and Publicly Perform the Work including as incorporated in Collections; and, to Distribute and Publicly Perform Adaptations.

 For the avoidance of doubt:

- i. Non-waivable Compulsory License Schemes. In those jurisdictions in which the right to collect royalties through any statutory or compulsory licensing scheme cannot be waived, the Licensor reserves the exclusive right to collect such royalties for any exercise by You of the rights granted under this License;
 ii. Waivable Compulsory License Schemes. In those jurisdictions in which the right to collect royalties through any statutory or compulsory licensing scheme can be waived, the Licensor waives the exclusive right to collect such royalties for any exercise by You of the rights granted under this License; and,
 iii. Voluntary License Schemes. The Licensor waives the right to collect royalties, whether individually or, in the event that the Licensor is a member of a collecting society that administers voluntary licensing schemes, via that society, from any exercise by You of the rights granted under this License.

 The above rights may be exercised in all media and formats whether now known or hereafter devised. The above rights include the right to make such modifications as are technically necessary to exercise the rights in other media and formats. Subject to Section 8(f), all rights not expressly granted by Licensor are hereby reserved.

4. Restrictions

ise granted in Section 3 above is expressly made subject to and limited by the following restrictions:

- Restrictions
 license granted in Section 3 above is expressly made subject to and limited by the following restrictions:

 You may Distribute or Publicly Perform the Work only under the terms of this License. You must include a copy of, or the Uniform Ressurce Identifier (URI) for, this License with every copy of the Work You Distribute or Publicly Perform. You may not offer or impose any terms on the Work that restrict the terms of this License or the ability of the recipient of the Work to exercise the rights granted to that recipient under the terms of the License. Perform the Work. You may not impose any effective technological measures on the Work that restrict the ability of a recipient of the Work from You to exercise the rights granted to that recipient under the terms of the License. This Section 4(a) applies to the Work as incorporated in a Collection, but this does not require the Collection apart from the Work itself to be made subject to the terms of this License. If You create a Collection, upon notice from any Licensor You must, to the extent practicable, remove from the Adaptation any credit as required by Section 4(c), as requested. If You create an Adaptation, upon notice from any Licensor You must, to the extent practicable, remove from the Adaptation any credit as required by Section 4(c), as requested. If You create an Adaptation, upon notice from any Licensor You must, to the extent practicable, remove from the Adaptation and practicable and

5. Representations, Warranties and Disclaimer

License 8

UNLESS OTHERWISE MUTUALLY AGREED TO BY THE PARTIES IN WRITING, LICENSOR OFFERS THE WORK AS-IS AND MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND CONCERNING THE WORK, EXPRESS, IMPLIED, STATUTORY OR OTHERWISE, INCLUDING, WITHOUT LIMITATION, WARRANTIES OF TITLE, MERCHANTIBILITY, FITNESS FOR A PARTICULAR PURPOSE, NONINFRINGEMENT, OR THE ABSENCE OF LATENT OR OTHER DEFECTS, ACCURACY, OR THE PRESENCE OF ABSENCE OF ERRORS, WHETHER OR NOT DISCOVERABLE. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OF IMPLIED WARRANTIES, SO SUCH EXCLUSION MAY NOT APPLY TO YOU.

6. Limitation on Liability
EXCEPT TO THE EXTENT REQUIRED BY APPLICABLE LAW, IN NO EVENT WILL LICENSOR BE LIABLE TO YOU ON ANY LEGAL THEORY FOR ANY SPECIAL, INCIDENTAL, CONSEQUENTIAL, PUNITIVE
OR EXEMPLARY DAMAGES ARISING OUT OF THIS LICENSE OR THE USE OF THE WORK, EVEN IF LICENSOR HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

7. Termination

- a.
- This License and the rights granted hereunder will terminate automatically upon any breach by You of the terms of this License. Individuals or entities who have received Adaptations or Collections from You under this License, however, will not have their licenses terminated provided such individuals or entities remain in full compliance with those licenses, Sections 1, 2, 5, 6, 7, and 8 will survive any termination of this License. Subject to the above terms and conditions, the license granted here is perpetual (for the duration of the applicable copyright in the Work). Notwithstanding the above, Licenseor reserves the right to release the Work under different license terms or to stop distributing the Work at any time; provided, however that any such election will not serve to withdraw this License (or any other license that has been, or is required to be, granted under the terms of this License), and lift license (in this License) and lift license (in the license) and the license term of the license term of this License (in this License).

8. Miscellaneous

- Each time You Distribute or Publicly Perform the Work or a Collection, the Licensor offers to the recipient a license to the Work on the same terms and conditions as the license granted to You under this License.
 Each time You Distribute or Publicly Perform an Adaptation, Licensor offers to the recipient a license to the original Work on the same terms and conditions as the license granted to You under this License.
 If any provision of this License is invalid or unenforceable law, it shall not affect the varieties of the remainder of the terms of this License, and without further action by the parties to this agreement, such provision shall be reformed to the minimum extent necessary to make such provision valid and enforceable.
 No term or provision of this License shall be deemed waived and no breach consented to unless such waiver or consent shall be in writing and signed by the party to be charged with such waiver or consent.
 This License constitutes the entire agreement between the parties with respect to the Work licensed here. There are no understandings, agreements or representations with respect to the Work not specified here. Licensor shall not be bound by any additional provisions that may appear in any communication from You. This License was not be modified without the mutual written agreement of the Licensor and You.
 The rights granted under, and the subject matter referenced, in this License were darfied utilizing the terminology of the Berne Convention of 1961, the WIPO Copyright Treaty of 1996, the WIPO Copyright T