ILLUMRA™

SELF-POWERED WIRELESS CONTROLS

ZigBee
Single and Dual Rocker Switch
USER MANUAL

Part Numbers: ZBT-S1AWH & ZBT-S2AWH (white)

Observe precautions! Electrostatic sensitive devices!

Patent protected:
WO98/36395, DE 100 25 561, DE 101 50 128,
WO 2004/051591, DE 103 01 678 A1, DE
10309334, WO 04/109236, WO 05/096482,
WO 02/095707,
US 6,747,573, US 7,019,241

REVISION HISTORY

The following major modifications and improvements have been made to this document:

Version	Author	Reviewer	Date	Major Changes
1.0	JFF		02.24.2017	Initial Release
1.1	JFF		04.04.2017	Update spec tables

Published by www.ILLUMRA.com, info@ILLUMRA.com, phone 801-349-1200

Important!
This information describes the type of component and shall not be considered as assured characteristics. No responsibility is assumed for possible omissions or inaccuracies. Circuitry and specifications are subject to change without notice. For the latest product specifications, refer to the ILLUMRA website: http://www.ILLUMRA.com.
As far as patents or other rights of third parties are concerned, liability is only assumed for switches, not for the described applications, processes and circuits.
ILLUMRA does not assume responsibility for use of switches described and limits its liability to the replacement of switches determined to be defective due to workmanship. Devices or systems containing RF components must meet the essential requirements of the local legal authorities. The switches must not be used in any relation with equipment that supports, directly or indirectly, human health or life or with applications that can result in danger for people, animals or real value.
Components of the switches are considered and should be disposed of as hazardous waste. Local government regulations are to be observed.
Packing: Please use the recycling operators known to you.

TABLE OF CONTENTS

GENERAL DESCRIPTION 4

FUNCTIONAL INFORMATION 5
- ZBT-SxAyy Device Overview 5
- Basic Functionality 6
- User Interface 6
- ZBT-SxAyy radio channel parameters 7
- Security parameters 8
- ZBT-SxAyy button contact status encoding 9
- Operation modes 10
- Data mode 10
- Commissioning mode 10
- Commissioning mode entry 11
- IEEE 802.15.4 Frame Structure 14
- PHY Header 15
- MAC Header 15
- MAC Trailer 16
- MAC Payload 16

Device Integration 18
- Mechanical Interface Characteristics 18
- Device Label 19
- 3.3.1 Device DMC 20

APPLICATION INFORMATION 21
- Transmission range 21

REGULATORY INFORMATION 22
- FCC (United States) Certificate 22
- 5.1.1 FCC (United States) Regulatory Statement 22
- 5.2 IC (Industry Canada) Certificate 23
- 5.2.1 IC (Industry Canada) Regulatory Statement 23

Understanding ZBT-SxAyy telegram structure 23
- Installation instructions for TI CC2531 packet sniffer 24
- Configuration 25
- Data capture 27
- Interpretation of the telegram data 27

1 GENERAL DESCRIPTION

1.1 Basic functionality

ZBT-SxAyy enables the realization of energy harvesting wireless switches for ILLUMRA systems communicating based on the 2.4 GHz IEEE 802.15.4 radio standard.

ZBT-SxAyy pushbutton transmitters are self-powered (no batteries) and fully maintenance-free. They can therefore be used in all environments including locations that are difficult to reach or within hermetically sealed housings. The required energy is generated by an electro-dynamic energy transducer actuated by pressing the switch.

When the switch is pushed down or released, electrical energy is created and a 2.4GHz radio telegram according to the IEEE 802.15.4 standard is transmitted. This radio telegram transmits the operating status of all two or four buttons depending on the model.

ZBT-SxAyy telegram format has been defined to maximize compatibility with a wide range of devices including such supporting the ZigBee Green Power standard. ZBT-SxAyy radio telegrams are protected with AES-128 security based on a device-unique private key.

Figure 1 – ZBT-SxAyy Product Photo

1.2 Technical data

Antenna	Integrated antenna
Radio Transmission Power (typ. at 25°C)	+2 dBm
Radio Standard	IEEE 802.15.4 using 2.4 GHz radio channels 11 … 26
Default Radio Channel	IEEE 802.15.4 radio channel 11
Radio Channel Selection	User-selectable (Commissioning)
Device Identification	Individual 32 Bit Device ID (factory programmed)
Security	AES128 (CBC Mode) with Sequence Code
Power Supply	Integrated Kinetic Energy Harvester
Button Inputs	Up to four buttons or two rockers

1.3 Physical dimensions

Dimensions of Single Rocker	4.5" x 2.75" x 0.62" (114 x 70 x 16 mm)
Dimensions of Double Rocker	4.5" x 2.75" x 0.62" (114 x 70 x 16 mm)
Weight of Single Rocker	3.9 oz (111g)
Weight of Dual Rocker	3.9 oz (111g)
Mounting	Screw or double sided tape onto flat surface

1.4 Environmental conditions

Operating Temperature	-25°C … 65°C
Storage Temperature	-25°C … 65°C
Humidity	0% to 95% r.h. (non-condensing)

1.5 Packaging information

Packaging Unit	96 units
Packaging Method	Each unit packed in a box, 96 units packed in a case

1.6 Ordering information

Par Number	Description	Frequency
ZBT-S1AWH	Single Rocker ZigBee Switch - White	2.4 GHz (IEEE 802.15.4)
ZBT-S2AWH	Dual Rocker ZigBee Switch - White	2.4 GHz (IEEE 802.15.4)

2 FUNCTIONAL INFORMATION

2.1 ZBT-SxAyy Device Overview

The Single and Dual rocker ZigBee Switches from ILLUMRA send the implementation of wireless remote controls without batteries. Power is provided by a built-in electrodynamic power generator. ZBT-SxAyy device transmits data based on the 2.4GHz IEEE 802.15.4 standard.

2.2 Basic Functionality

ZBT-SxAyy devices contain an electro-dynamic energy transducer which is actuated by an energy bow. This bow is pushed by an appropriate switch rocker mounted onto the device. An internal spring will release the energy bow as soon as it is not pushed down anymore.

When the energy bow is pushed down, electrical energy is created and an IEEE 802.15.4 radio telegram is transmitted which identifies the status (pressed or not pressed) of the four button. Releasing the energy bow similarly generates energy which is used to transmit a different radio telegram.

It is therefore possible to distinguish between radio telegrams sent when the energy bar was pushed and radio telegrams sent when the energy bar was released.

By identifying these different telegrams types and measuring the time between pushing and releasing of the energy bar, it is possible to distinguish between "Long" and "Short" button contact presses. This enables simple implementation of applications such as dimming control or blinds control including slat action.

2.3 User Interface

ZBT-SxAyy devices provide either 2 buttons (Single Rocker) or 4 buttons (Dual Rocker).

The state of the four button contacts (pressed or not pressed) is transmitted together with a unique device identification (32 Bit device ID) whenever the switch is pushed or released.

2.4 ZBT-SxAyy radio channel parameters

ZBT-SxAyy supports all sixteen IEEE 802.15.4 radio channels in the 2.4 GHz band (channels 11 … 26 according to IEEE 802.15.4 notation) which can be selected as described above.

Table 1 below shows the correspondence between channel number and channel frequency (in MHz).

Channel ID	Lower Frequency	Centre Frequency	Upper Frequency
11	2404	2405	2406
12	2409	2410	2411
13	2414	2415	2416
14	2419	2420	2421
15	2424	2425	2426
16	2429	2430	2431
17	2434	2435	2436
18	2439	2440	2441
19	2444	2445	2446
20	2449	2450	2451
21	2454	2455	2456
22	2459	2460	2461
23	2464	2465	2466
24	2469	2470	2471
25	2474	2475	2476
26	2479	2480	2481

Table 1 - IEEE 802.15.4 Radio Channels and Frequencies (in MHz)

2.5 Security parameters

ZBT-SxAyy secures its data transmissions using the following parameters:

- Algorithm
  AES128 encryption in CBC mode

- Input data
  Telegram payload including 32 bit sequence counter

- Security key
  Out of the box 128 bit device-unique random key (factory programmed)

- Output data
  32 bit device-unique and telegram-unique signature

The current status of the sequence counter together with the device-unique key are transmitted during commissioning to the receiver where ZBT-SxAyy is learned in. These parameters are subsequently used to authenticate received telegrams.

ZBT-SxAyy subsequently calculates the telegram signature based on telegram payload, sequence counter and device-unique secret key. The implementation uses AES128 in CCM (Counter with CBC-MAC) mode together with a sequence counter as described in IETF RFC3610:

http://www.ietf.org/rfc/rfc3610.txt

This implementation is used in a number of industry standard protocols including ZigBee Green Power. Implementation parameters used by ZBT-SxAyy have been chosen to maximize compatibility with such protocols.

For background information to the AES128 CCM algorithm, you can use below as a starting point:

https://asecuritysite.com/encryption/ccmaes

Please contact ILLUMRA if additional information is required.

2.6 ZBT-SxAyy button contact status encoding

Table 2 below shows the supported single and dual button contact actions of ZBT-SxAyy together with the encoding used for the transmission.

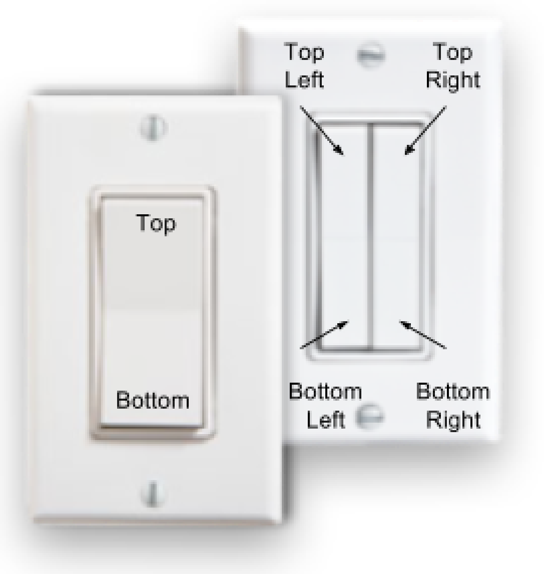
In this table, "0" indicates that a button contact is not pressed while "1" indicates that a button contact is pressed. The command encoding has been chosen to maximize interoperability with existing applications including such supporting the ZigBee Green Power standard.

Button	Motion	Command
Top	Press	0x12
Top	Release	0x13
Bottom	Press	0x14
Bottom	Release	0x15

Table 2: ZBT-S1Ayy Single Rocker button status encoding

Button	Motion	Command
Top Left	Press	0x12
Top Left	Release	0x13
Bottom Left	Press	0x14
Bottom Left	Release	0x15
Top Right	Press	0x18
Top Right	Release	0x19
Bottom Right	Press	0x22
Bottom Right	Release	0x23

Table 3: ZBT-S2Ayy Dual Rocker button status encoding



2.7 Operation modes

ZBT-SxAyy can operate in two modes:

- Data mode
  Data mode is used to transmit data telegrams reporting the status of ZBT-SxAyy button inputs

- Commissioning mode
  Commissioning mode is used to commission (teach-in) ZBT-SxAyy into a specific receiver or network. To do so, ZBT-SxAyy will identify its capabilities and its security parameters and – if required – change the radio channel it uses for telegram transmission.

2.8.1 Data mode

Data mode is the standard mode of operation. In this mode, ZBT-SxAyy will transmit data telegrams identifying the status of its four button contacts and the energy bar.

ZBT-SxAyy supports both single button actions (one button contact or only the energy bar being actuated) and dual button actions (two button contacts being actuated at the same time).

ZBT-SxAyy uses the following sequence to identify and transmit button contact status:

1. Determine direction of the energy bar movement (push or release)
2. Read status of all button contacts
3. Calculate telegram payload
4. Calculate security signature
5. Format IEEE 802.15.4 radio telegram
6. Transmit radio telegram

2.8.2 Commissioning mode

Commissioning mode is used to configure ZBT-SxAyy and learn it into an existing network. To do so, it provides two key functions:

- Transmission of a commissioning telegram in order to learn-in ZBT-SxAyy into a network

- Radio channel selection in order to set the radio channel of ZBT-SxAyy to that used by the network

These functions are described subsequently in more detail.

2.8.2.1 Commissioning mode entry

Commissioning mode is entered using a special button contact sequence. This is illustrated in Figure 5 below.

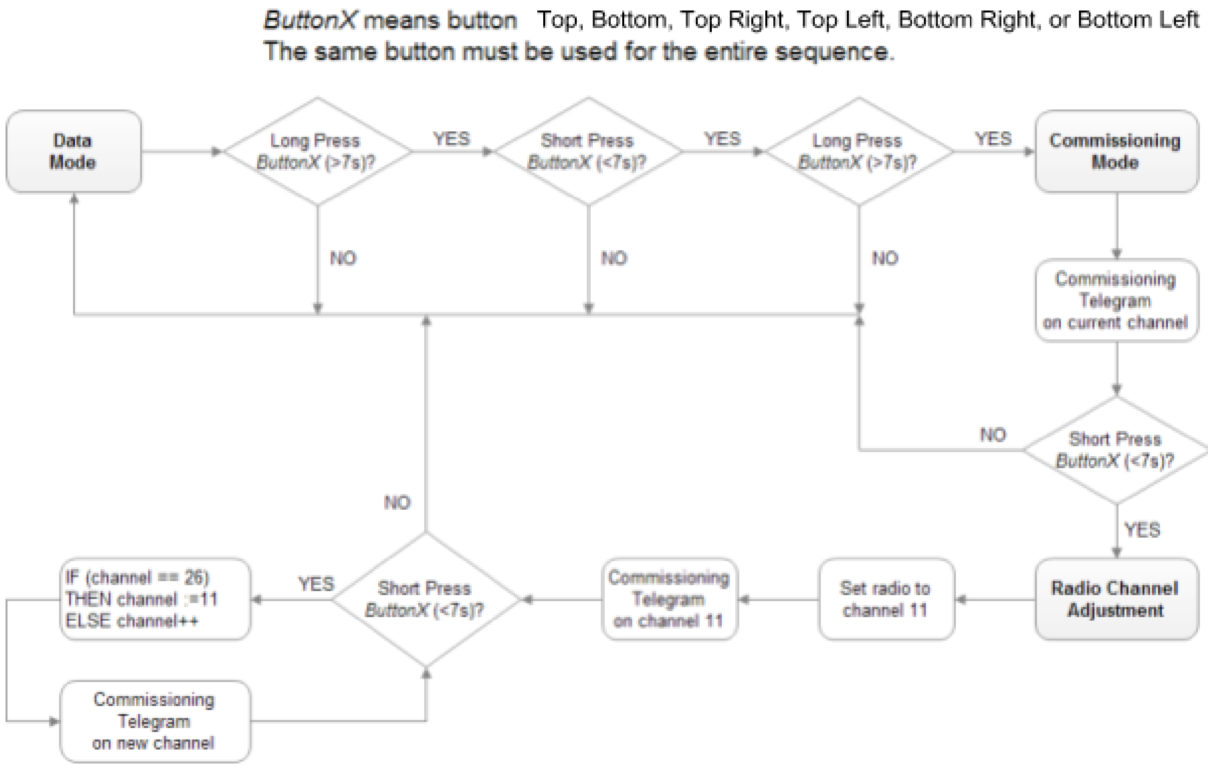


Figure 5 – Button sequence for commissioning mode

To enter commissioning mode, start by selecting one button contact of ZBT-SxAyy. Any contact of ZBT-SxAyy (Top Left, Bottom Left, Top Right, Bottom Right) can be used. This contact is referred to as *ButtonX* in Figure 5 above.

Next, execute the following long-short-long sequence:

1. Press and hold the selected button contact together with the energy bar for more than 7 seconds before releasing it

2. Press the selected button contact together with the energy bar quickly (hold for less than 2 seconds)

3. Press and hold the selected button contact together with the energy bar again for more than 7 seconds before releasing it

Upon detection of this sequence, ZBT-SxAyy will enter commissioning mode and transmit a commissioning telegram on the current radio channel.

2.9.1.1 Commissioning telegram transmission

ZBT-SxAyy will transmit a commissioning telegram on the current radio channel immediately upon entering commissioning mode. This allows teach-in into additional devices without changing the currently used radio channel.

The default radio channel used by ZBT-SxAyy is channel 11 (see chapter 2.5). It can be subsequently adjusted as described in the following chapter.

Whenever a new radio channel is selected, ZBT-SxAyy will transmit a commissioning telegram on the new radio channel. This enables the receiver to provide feedback to the user to indicate when ZBT-SxAyy has reached the correct radio channel (i.e. when the receiver receives a commissioning telegram from ZBT-SxAyy on the radio channel the receiver is using). See chapter 2.8.2.5 for a discussion of feedback mechanisms.

The format of ZBT-SxAyy radio telegrams including commissioning telegrams is described in chapter 2.9.

2.9.1.2 Radio channel adjustment

The radio channel used by ZBT-SxAyy can be changed whenever ZBT-SxAyy is in commissioning mode. Refer to chapter 2.5 for a summary of the supported radio channels.

In order to change the radio channel, press the selected button contact shortly (< 7s) once after entry into commissioning mode. This will reset the radio channel used by ZBT-SxAyy to channel 11 and enable subsequent channel adjustment.

If ZBT-SxAyy was already operating on channel 11 (default condition) then the radio channel will remain unchanged. This ensures that ZBT-SxAyy will always use channel 11 as starting point for the radio channel adjustment.

The radio channel can now be incremented by continuing to press the selected button contact shortly (< 7s). For each such button press, the radio channel is incremented. If channel 26 has been reached then channel 11 will be used next.

2.9.1.3 Radio channel adjustment examples

Example 1: ZBT-SxAyy operating on channel 11 (out of the box condition)
In this case, ZBT-SxAyy would send a commissioning telegram on channel 11 immediately after detecting the long-short-long sequence.

After that, it would for each additional short button press send commissioning telegrams on incrementing radio channels starting with channel 11.

This means that the channel sequence would be:
11 (current channel) - 11 – 12 – 13 … 25 – 26 – 11 – 12 and so on

Example 2: ZBT-SxAyy operating on channel 15
In this case, ZBT-SxAyy would send a commissioning telegram on channel 15 immediately after detecting the long-short-long sequence.

After that, it would for each additional button press send commissioning telegrams on incrementing radio channels starting with channel 11.

This means that the channel sequence would be:
15 (current channel) - 11 – 12 – 13 … 25 – 26 – 11 – 12 and so on

2.9.1.4 Determining the correct radio channel

The user requires system feedback to determine if the correct radio channel has been reached.

Several methods are possible for that, including:

- Feedback from the device into which ZBT-SxAyy is learned in
  E.g. blinking a status light, toggling a connected load, moving a motor etc.
- Feedback from a dedicated user interface
  This could for instance instruct the user on the required key sequence and confirm correct execution

It is the responsibility of the system designer to define a suitable feedback mechanism.

2.9.1.5 Storing the new radio channel and return to data mode

If ZBT-SxAyy has been successfully set to the desired radio channel then this radio channel has to be stored and operation should return to data mode.

This is achieved by pressing any button contact other than the one used for entry into commissioning mode (and channel change). So if the bottom button was used to enter commissioning mode then pressing top button will cause storing of the current radio channel and return to data mode.

Failure to store the selected radio channel and to return to data mode could cause accidental reconfiguration of ZBT-SxAyy.

2.9.1.6 Setting ZBT-SxAyy to a defined state (data mode)

Sometimes the user might be unsure if ZBT-SxAyy is operating in data mode, in commissioning mode or if part of the entry sequence into commissioning mode has already been executed.

ZBT-SxAyy can always be set into a defined state (data mode) by shortly (< 7s) pressing two different buttons one after another. After that, ZBT-SxAyy will operate in data mode and the full sequence for commissioning mode entry (long-sort-long) would have to be executed to enter commissioning mode.

2.9 IEEE 802.15.4 Frame Structure

ZBT-SxAyy transmits radio telegrams in the 2.4 GHz band according to IEEE 802.15.4 frame structure. For detailed information about the IEEE 802.15.4 standard, please refer to the applicable specifications.

Note that the data format used by IEEE 802.15.4 is little endian. This means that for multibyte structures (such as 2 byte, 4 byte or 8 byte fields) the least significant byte (LSB) is transmitted first.

The IEEE 802.15.4 frame structure used by ZBT-SxAyy consists of the following four main parts:

- PHY Header
  The PHY header indicates to the receiver the start of a transmission and provides information about the length of the transmission.
  It contains the following fields:
    - Preamble
      Pre-defined sequence (4 byte, value 0x00000000) used to adjust the receiver to the transmission of the sender
    - Start of frame
      Pre-defined symbol (1 byte, value 0xA7) identifying the start of the actual data frame
    - Length of frame
      1 byte indicating the combined length of all following fields

- MAC Header
  The MAC header provides detailed information about the frame. It contains the following fields:
    - Frame control field - 2 bytes to identify frame type, protocol version, addressing and security mode
    - Sequence number - 1 byte sequential number to identify the order of transmitted frames
    - Address - PAN ID and address of source (if present) and destination of the telegram ZBT-SxAyy does not use source address and source PAN ID

- MAC Payload
  The MAC Payload field contains telegram control, device ID, telegram data and telegram security (if present) fields.
  The MAC Payload field structure depends on telegram type (data or commissioning) and security mode (secure or standard transmission).

- MAC Trailer
  The MAC Trailer contains the Frame Check Sum (FCS) field used to verify the integrity of the telegram data.

Figure 6 below summarizes the IEEE 802.15.4 frame structure.

PHY Header			MAC Header			MAC Payload	MAC Trailer
Preamble	Start of Frame	Length of Frame	Frame Control	Sequence Number	DstAddress PAN | Addr	Depending on Telegram Type	Frame Check Sum
4 Byte	1 Byte	1 Byte	2 Byte	1 Byte	4 Byte	Depending on Telegram Type	2 Byte

Figure 6 – IEEE 802.15.4 Frame Structure

The content of these fields is described in more detail below.

2.9.2 PHY Header

The IEEE 802.15.4 PHY header consists of the following fields:

D Preamble

D Start of Frame

D Length of Frame fields

The content of the *Preamble* and *Start of Frame* fields is fixed for all telegram types supported by ZBT-SxAyy as follows:

D Preamble = 0x00000000

D Start of Frame = 0xA7

The content of the *Length of Frame* field differs depending on the telegram type as follows:

D Commissioning
telegram Length=
42 bytes (0x2A)

D Data telegram
Length = 24 bytes (0x18)

2.9.3 MAC Header

The IEEE 802.15.4 MAC Header contains the following fields:

D Frame Control Field (2 byte)
The *Frame Control Field* is set to 0x0801 in all ZBT-SxAyy telegrams in order to identify them as data telegrams with short addresses based on version IEEE 802.15.4-2003

D Sequence Number (1 byte)
The *Sequence Number* is an incremental number used to identify the order of telegrams

D Address Field (4 byte in ZBT-SxAyy implementation)

The *Address Field* is set to 0xFFFFFFFF to identify ZBT-SxAyy telegrams as broadcast telegrams using short Destination Address (16 Bit) together with the Destination PAN ID (16 Bit). Source address and Source PAN ID are not present in ZBT-SxAyy MAC Header.

2.9.4 MAC Trailer

The MAC Trailer only contains the Frame Check Sum (FCS) field.

Its length is 2 byte and it is calculated as Cyclic Redundancy Check (CRC16) over the entire MAC payload including the *Length of Frame* field of the PHY Header using the following polynomial: $x^{16} + x^{12} + x^{5} + 1$

2.9.5 MAC Payload

The MAC Payload depends on the telegram type (data telegram or commissioning telegram). The MAC Payload structure for these telegram types are described in the following chapters.

2.9.5.1 MAC Payload structure for data telegrams

Figure 7 below shows the MAC Payload structure for data telegrams.

Telegram Control	Source ID	Sequence Counter	Command	Telegram Signature
2 Byte	4 Byte	4 Byte	1 Byte	4 Byte

Figure 7 – MAC Payload structure for data telegrams

The payload format has been chosen to ensure interoperability with a wide range of devices including such supporting the ZigBee Green Power standard.

The following fields are used for the MAC Payload of data telegrams:

- Telegram Control (2 bytes, 0x308C)
  The *Telegram Control* field is set to 0x308C to identify a secure telegram with device- unique key

- Source ID (4 bytes)
  The *Source ID* field contains a 4 byte ID uniquely identifying each ZBT-SxAyy device

- Sequence Counter (4 bytes)
  The *Sequence Counter* field contains an always incrementing counter.
  Security processing is based on the combination of the Command and Sequence Counter in order to prevent replay attacks (sending the same telegram again)

- Command (1 byte)
  The *Command* field is a one byte field which identifies the state of the ZBT-SxAyy contacts. For the encoding please refer to Table 2

- Telegram Signature (4 byte)
  The *Telegram Signature* field is used to validate the telegram authenticity. The telegram signature is calculated based on the telegram payload using AES128 (CBC mode).
  ILLUMRA can provide upon request additional information on how to implement telegram validation.

2.9.5.2 MAC Payload structure for commissioning telegrams

Figure 8 below shows the MAC payload structure for commissioning telegrams.

Telegram Control	Source ID	Commissioning Command	Device Type	Device Options	Device-unique Security Key	Security Key Validation	Sequence Counter
1 Byte	4 Byte	1 Byte	1 Byte	2 Byte	16 Byte	4 Byte	4 Byte

Figure 8 – MAC Payload structure for commissioning telegrams

The following fields are used for commissioning telegrams:

- Telegram Control (1 byte)
  The *Telegram Control* field is set to 0x0C to identify a standard telegram (secure communication will be established based on the commissioning telegram)

- Source ID (4 bytes)
  The *Source ID* field contains a 4 byte ID uniquely identifying each ZBT-SxAyy device

- Command (1 byte)
  The *Command* field is set to 0xE0 to identify this command as commissioning command

- Device Type (1 byte)
  The *Device Type* field is set to 0x02 to identify ZBT-SxAyy as switch

- Device Options (2 bytes)
  The *Device Options* field is set to 0xF281 to identify the device as ZBT-SxAyy communicating securely using the AES128 (CBC mode) algorithm and a 4 byte sequence counter to generate a 4 byte signature

- Device-unique Security Key (16 bytes)
  Each ZBT-SxAyy contains a random, device-specific security key which is generated as part of the production flow. During commissioning, this key is transmitted in encrypted format. Contact ILLUMRA for details.

- Security Key Validation (4 bytes)
  In order to ensure correct reception, an additional 4 byte validation value is provided. Contact ILLUMRA for details.

- Sequence Counter (4 bytes)
  The *Sequence Counter* is an always incrementing counter which is used as part of the security processing to avoid replay attacks (sending the same telegram again).
  Receiving devices shall only accept data telegrams with sequence counter values higher than that of the last received telegram; therefore the current value needs to be communicated during commissioning.

2 Device Integration

ZBT-SxAyy is designed for integration into button or rocker based switches. It implements the established PTM 2xx mechanical form factor and can therefore be used with a wide variety of existing designs.

2.1 Mechanical Interface Characteristics

Energy bow travel / operating force	1.8 mm / typ. 10 N At room temperature Only one of the two energy bows may be actuated at the same time!
Restoring force at energy bow	typ. 0.7 N Minimum restoring force of 0.5 N is required for correct operation
Number of operations at 25°C	typ. 100.000 actuations tested according to VDE 0632 / EN 60669
Cover material	Poly-carbonate

2.2 Device Label

Each ZBT-SxAyy module contains a device label as shown in Figure 15 below.

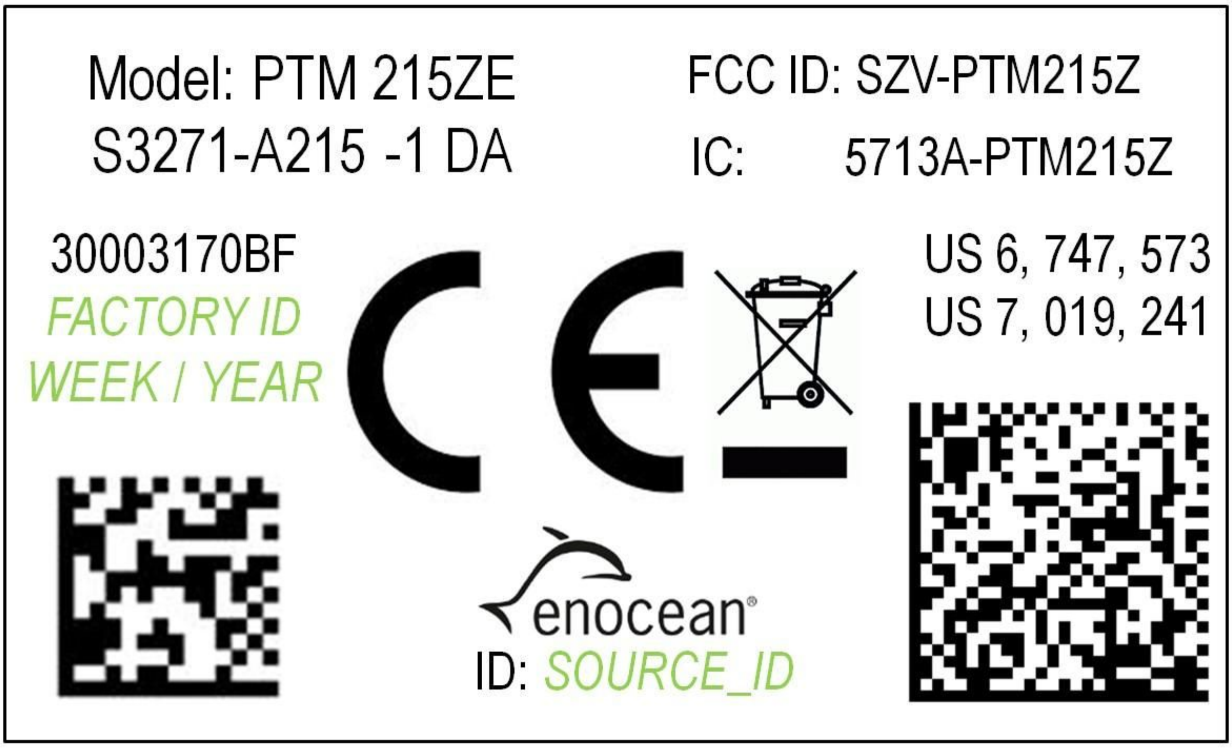


Figure 15 – ZBT-SxAyy device label

This device label identifies the following parameters in writing:

- Manufacturing date (WEEK / YEAR)
- IEEE 802.15.4 MAC Layer Source ID (SOURCE_ID)

Note that the device label also contains a DMC code in the lower right corner as described below.

3.3.1 Device DMC

Each ZBT-SxAyy module contains a data matrix code (DMC) on the lower right hand side of the device label which can be used to automatically scan device parameters.

The DMC uses the ECC200 standard to encode up to 52 characters. The content of the DMC uses the following format:

<PRODUCT_NAME>ID<SOURCE_ID>OOB<DEVICE_KEY>

This identifies the following parameters:

- Product Name (ZBT-SxAyy)
- IEEE 802.15.4 MAC Layer Source ID (different for each device)
- Device-unique random security key (different for each device)

One possible DMC reading could for instance be:

PTM215ZEID01500100OOB0123456789ABCDEF0123456789ABCDEF

This would identify the following parameters:

- Product Name = ZBT-SxAyy
- IEEE 802.15.4 MAC Layer Source ID = 01500100
- Device-unique random security key = 0123456789ABCDEF0123456789ABCDEF

3 APPLICATION INFORMATION

3.1 Transmission range

The main factors that influence the system transmission range are:
- Type and location of the antennas of receiver and transmitter
- Type of terrain and degree of obstruction of the link path
- Sources of interference affecting the receiver
- "Dead spots" caused by signal reflections from nearby conductive objects.

Since the expected transmission range strongly depends on this system conditions, range tests should always be performed to determine the reliably achievable range under the given conditions.

The following figures should be treated as a rough guide only:

- Line-of-sight connections
  Typically 15 m range in corridors, up to 50 m in halls

- Plasterboard walls / dry wood
  Typically 15 m range, through max. 2 walls

- Ferro concrete walls / ceilings
  Maximum 1 wall or ceiling, depending on thickness and material

- Fire-safety walls, elevator shafts, staircases and similar areas should be considered as shielded

The angle at which the transmitted signal hits the wall is very important. The effective wall thickness – and with it the signal attenuation – varies according to this angle. Signals should be transmitted as directly as possible through the wall. Wall niches should be avoided.

Other factors restricting transmission range include:
- Switch mounting on metal surfaces (up to 30% loss of transmission range)
- Hollow lightweight walls filled with insulating wool on metal foil
- False ceilings with panels of metal or carbon fibre
- Lead glass or glass with metal coating, steel furniture

The distance between the receiver and other transmitting devices such as computers, audio and video equipment that also emit high-frequency signals should be at least 0.5 m.

4 REGULATORY INFORMATION

ZBT-SxAyy has been certified according to FCC, IC and CE regulations.
Changes or modifications not expressly approved by ILLUMRA could void the user's authority to operate the equipment.

4.1 FCC (United States) Certificate

TCB — GRANT OF EQUIPMENT AUTHORIZATION — TCB

Certification
Issued Under the Authority of the
Federal Communications Commission
By:

EMCCert Dr, Rasek GmbH
Stoernhofer Berg 15
91364 Unterleinleiter,
Germany

Date of Grant: 05/12/2016

Application Dated: 05/12/2016

EnOcean GmbH
Kolpingring 18a
Oberhaching, 82041
Germany

Attention: Armin Anders , Director Product Marketing

NOT TRANSFERABLE

EQUIPMENT AUTHORIZATION is hereby issued to the named GRANTEE, and is VALID ONLY for the equipment identified hereon for use under the Commission's Rules and Regulations listed below,

FCC IDENTIFIER: SZV-PTM215Z
Name of Grantee: EnOcean GmbH
Equipment Class: Part 15 Low Power Communication Device Transmitter
Notes: 2405 MHz - 2480 MHz transmitter

Grant Notes	FCC Rule Parts	Frequency Range (MHZ)	Output Watts	Frequency Tolerance	Emission Designator
	15C	2405.0 - 2480.0			

5.1.1 FCC (United States) Regulatory Statement

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions:

(1) this device may not cause harmful interference, and

(2) this device must accept any interference received, including interference that may cause undesired operation.

5.2 IC (Industry Canada) Certificate

EMCC™ DR. RAŠEK

FCB under the Canada-EC MRA
TCB under the USA-EC MRA
RFCAB under the Japan-EC MRA
Notified Body RTTE Directive 99/5/EC
Notified Body EMC Directive 2014/30/EU

No. CA001666G

TECHNICAL ACCEPTANCE CERTIFICATE CANADA

CERTIFICAT D'ACCEPTABLITÉ TECHNIQUE CANADA

CERTIFICATION No. / No. DE CERTIFICATION ► 5713A-PTM215Z

ISSUED TO / DELIVRE A ► EnOcean GmbH

Street Address / Numéro et rue: Kolpingring 18 a   City / Ville: Oberhaching

Province or State / Province ou Etat: Germany   Postal Code / Code postal: 82041

TYPE OF EQUIPMENT / GENRE DE MATERIEL ► Low Power Device (2400-2483.5 MHz)   PMN ► PTM 215ZE   HVIN ► PTM 215ZE

ANTENNA / ANTENNE ► Integrated / Incorporé   ANTENNA GAIN / GAIN D'ANTENNE ►

FREQUENCY RANGE BANDE DE FRÉQUENCES	EMISSION TYPE GENRE D'ÉMISSION	RF POWER PUISSANCE H.F.	SPECIFICATION / ISSUE / DATE SPÉCIFICATION / ÉDITION / DATE
2405 - 2480 MHz	2M45G1DDN	71.3 dBµV/m	RSS-210 / 8 / December 2010

TEST LABORATORY / LABORATOIRE D'ESSAY ► EMCCons DR. RAŠEK GmbH & Co. KG   CN 3464C   OATS 3464C-1

Street Address / Numéro et rue: Stoernhofer Berg 15   City / Ville: Unterleinleiter

Province or State / Province ou Etat: Germany   Postal Code / Code Postal: 91364

Name / Nom: Reinhard Sauerschell   Tel: 0049 9194 7263-301

E-mail: r.sauerschell@emcc.de   Fax: 0049 9194 7263-309

Certification of equipment means only that the equipment has met the requirements of the above-noted specification. Licence applications, where applicable to use certified equipment, are acted on accordingly by the Industry Canada issuing office and will depend on the existing radio environment, service and location of operation. This certificate is issued on condition that the holder complies and will continue to comply with the requirements and procedures issued by Industry Canada. The equipment for which this certificate is issued shall not be manufactured, imported, distributed, leased, offered for sale or sold unless the equipment complies with the applicable technical specifications and procedures issued by Industry Canada.

I hereby attest that the subject equipment was tested and found in compliance with the above-noted specification.

La certification du matériel signifie seulement que le matériel a satisfait aux exigencies de la norme indiquée ci-dessus. Les demandes de licences nécessaires pour l'utilisation du matériel certifié sont traitées en conséquence par le bureau de deliverance d'Industrie Canada et dépendent des conditions radio ambiantes, du service et de l'emplacement d'exploitation. Le présent certificat est délivré à la condition que le titulaire satisfasse et continue de satisfaire aux exigences et aux procedures d'Industrie Canada. Le matériel à l'égard duquel le présent certificat est délivré ne doit pas être fabriqué, importé, distribué, loué, mis en vente ou vendu à moins d'être conforme aux procédures et aux spécifications techniques applicables publiées par Industrie Canada.

J'atteste par la présente que le matériel a fait l'objet d'essai et jugé conforme à laspécification ci-dessus.

DATE 12 May 2016

Certification Officer

EMCCert DR. RAŠEK GmbH • Stoernhofer Berg 15, 91364 Unterleinleiter, Germany
Tel.: +49 9194 72279-01 • Fax: +49 9194 72279-06 • E-mail: emc.cert@emcc.de • Web: www.emcc.de

5.2.1 IC (Industry Canada) Regulatory Statement

This device complies with Industry Canada licence-exempt RSS standard(s). Operation is subject to the following two conditions:

(1) this device may not cause interference, and

(2) this device must accept any interference, including interference that may cause undesired operation of the device.

Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio exempts de licence.
L'exploitation est autorisée aux deux conditions suivantes :

(1) l'appareil ne doit pas produire de brouillage, et

(2) l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement."

A Understanding ZBT-SxAyy telegram structure

This appendix describes – purely for reference purposes – how to analyse the ZBT-SxAyy radio telegram structure using the TI CC2531EMK packet sniffer (USB dongle) on a Windows 7 based system.

A.1 Installation instructions for TI CC2531 packet sniffer

The following description assumes the use of the TI CC2531EMK described here: http://www.ti.com/tool/cc2531emk

CC2531EMK can be used in conjunction with the "TI SmartRF Protocol Packet Sniffer" to capture and visualize IEEE 802.15.4 data telegrams.

To use TI SmartRF Protocol Packet Sniffer, please download the SW package from the TI website. At the time of writing, the SW could be obtained using this link:

http://www.ti.com/tool/packet-sniffer

Please download and install this SW before proceeding with the instructions given in the next chapter.

A.1.1 CC2531EMK setup

After setting up the TI SmartRF Protocol Packet Sniffer please insert the CC2531EMK USB dongle into a USB port of the PC and make sure that the green LED of the dongle is active.

Please make sure that the required device driver for the CC2531EMK has been correctly installed. To do so, please check the Device Manager where you should see an entry named "CC2531 USB Dongle" under the group label "CEBAL Controlled Devices".

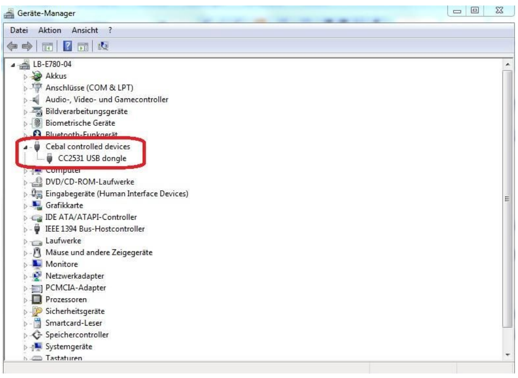


Figure 16 – Correctly installed CC2531EMK

A.2 Configuration

After the installation of the CC2531EMK driver, please start the TI SmartRF Packet Sniffer program. The protocol selection dialog program window which appears after the start of is shown in Figure 17 below.

Figure 17 – Protocol selection dialog of TI SmartRF Packet Sniffer

In this dialog, please select "IEEE 802.15.4/ZigBee" as shown above and press the "Start" button. Once the main window comes up, please make sure that "CC2531" is shown in the "Capturing device" tab and in the "RF device:" footer line as shown in Figure 18 below.

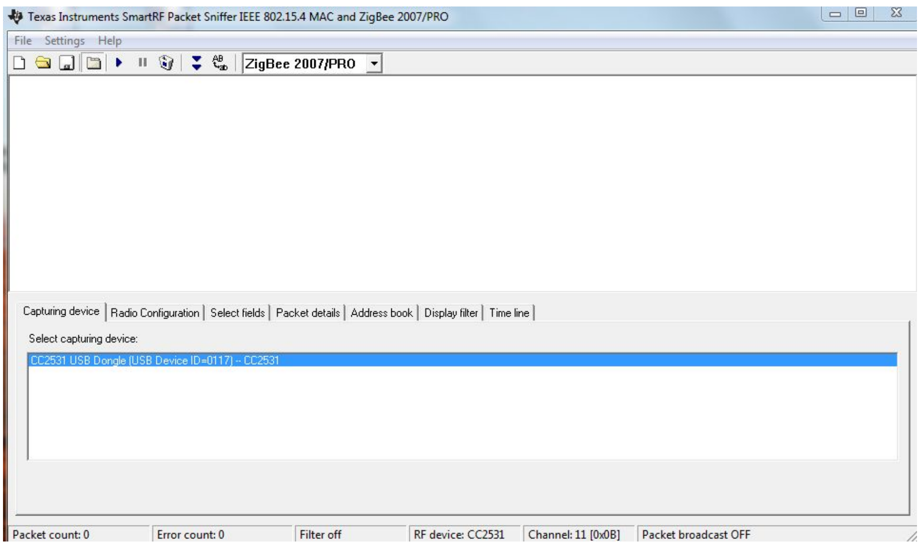


Figure 18 – Main window TI SmartRF Packet Sniffer

Out of the box, ZBT-SxAyy is configured for using IEEE 802.15.4 radio channel 11. Make sure that this radio channel (0x0B) is selected in the "Radio Configuration" tab and shown in the "Channel:" footer line.

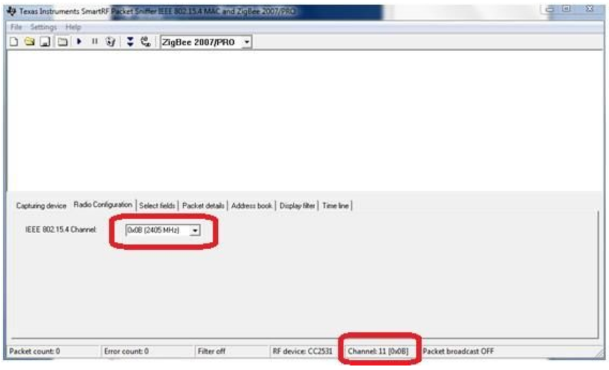


Figure 19 – Radio channel selection

The data fields that will be displayed can be selected in the "Select fields" tab. Make sure that all "MAC Header", "Data" and "Footer" fields are selected and that the "LQI/RSSI" drop-down list is set to "RSSI".

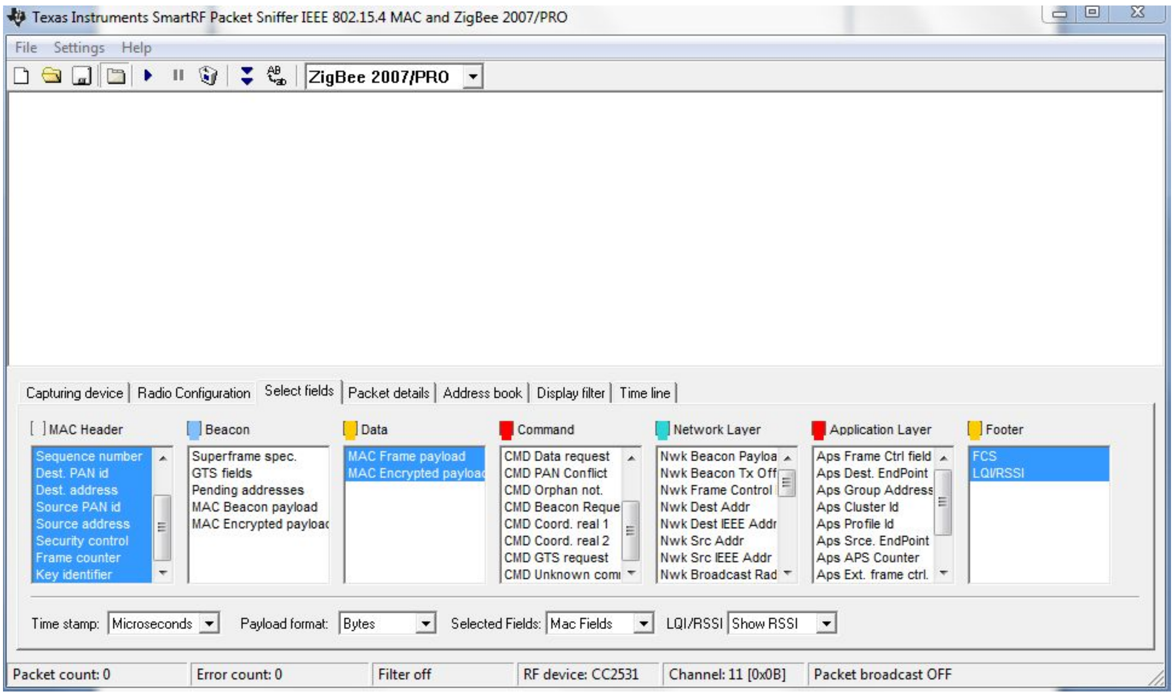


Figure 20 – Payload selection

The TI SmartRF Packet Sniffer is now ready.

A.3 Data capture

Press the triangular button ( ) to start the radio capture and press the auto-scoll button ( ) to automatically select the most recent data telegram. Then press a button of ZBT-SxAyy. You should now see the captured radio telegrams (ZBT-SxAyy sends several redundant radio telegrams per user action).

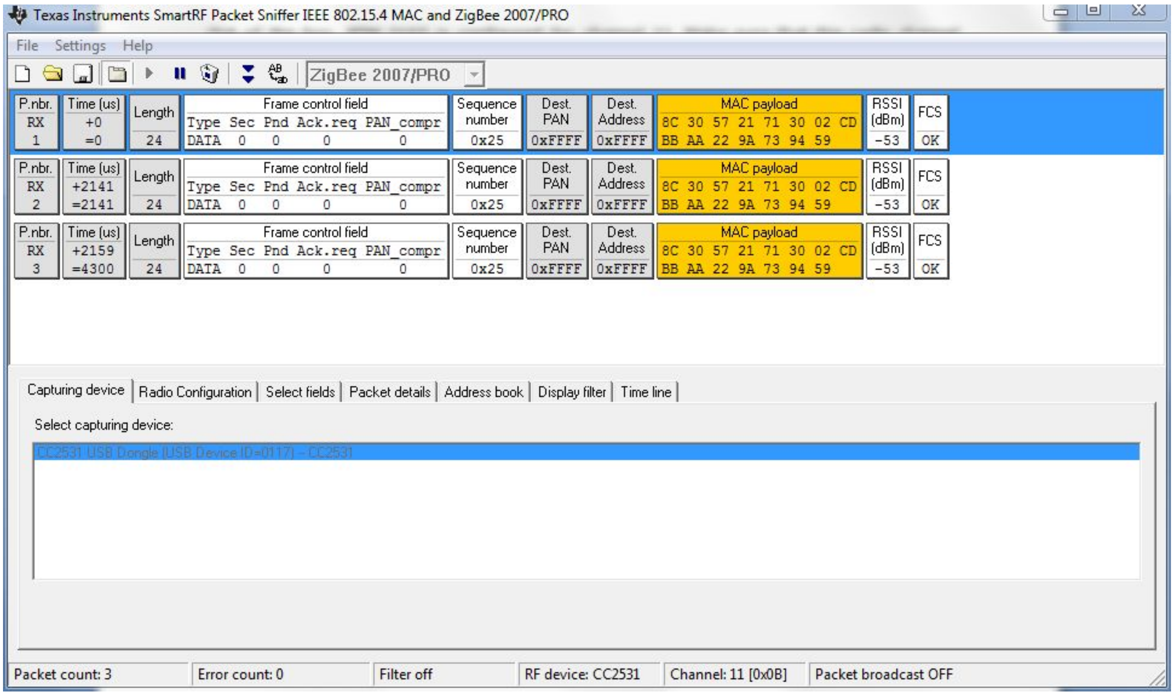


Figure 21 – Captured telegram data

A.4 Interpretation of the telegram data

The following parameters within captured radio telegrams are typically of interest:

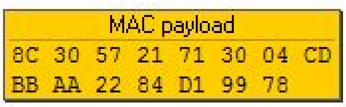
1. MAC Payload
   This will contain the ID of the sender, various control and security data fields as well as the actual command data (1 byte)
   The structure of this field is outlined subsequently in more detail.

2. RSSI
   This will show the received signal strength

3. FCS
   This will show the frame integrity (OK / not OK) and should normally show "OK".

A.4.1 MAC Payload

Below is an example of a captured MAC payload:



The hexadecimal representation of this specific payload is:

8C 30 57 21 71 30 04 CD BB AA 22 84 D1 99 78

The location and interpretation of key parameters is described in the following chapters.

A.4.2 Device ID

The device ID is used to uniquely identify each device in the network. It is 4 byte long and is allocated to byte 2…5 of the MAC payload as highlighted below:

8C 30 **57 21 71 30** 04 CD BB AA 22 84 D1 99 78

Note that the byte order is little endian, therefore the ID of this specific device is 0x30712157.

A.4.3 Sequence Counter

The sequence counter is used to uniquely identify each telegram in order to avoid telegram replay. It is 4 byte long and is allocated to byte 6…9 of the MAC payload as highlighted below:

8C 30 57 21 71 30 **04 CD BB AA** 22 84 D1 99 78

Note that the byte order is little endian, therefore the current sequence counter value of this specific device is 0xAABBCD04.

A.4.4 Command payload

The command payload identifies the action performed on the switch (i.e. which buttons have been pressed). The command is allocated to byte 10 of the MAC payload as highlighted below:

8C 30 57 21 71 30 04 CD BB AA **22** 84 D1 99 78

In this case it is 0x22 meaning that Bottom Right button has been pressed. Refer to chapter 2.7 for the description of commands supported by ZBT-SxAyy.

A.4.5 Telegram Signature

The ZBT-SxAyy radio telegram is authenticated via a 32 Bit signature. This signature is calculated based on the private key (unique for each device), the data payload and a 32 Bit sequence counter (which is incremented for each data telegram).

This approach prevents unauthorized senders from sending commands. Note that the content of the telegram itself is not encrypted, i.e. the switch command is sent as plain text.

The telegram signature is transmitted using the last 4 byte of the telegram:

8C 30 57 21 71 30 04 CD BB AA 22 **84 D1 99 78**

Note that the signature changes with each transmission even if the remainder of the MAC payload remains the same.

This is due to the inclusion of the rolling code into the MIC calculation which prevents message replay attacks (capture and reuse of a previous message).