USB and Radio protocol of the Crazyradio dongle

The Crazyradio dongle is based on a Nordic semiconductor nRF24LU1 chip. The radio communication is done using the Nordic “Enhanced ShockBurst™” packet protocol in PTX mode with acknowledge. Variable sized packet, from 1 to 32 bytes, can be send and acknowledged by the copter. The acknowledgement packet can contain a payload from 0 to 32 Bytes.

This page documents the protocol used in version 0.52 of the Crazyradio dongle. Future version (up to 1.0) will be kept compatible.

Radio configuration

Crazyradio is configured in PTX mode. It can communicate with Nordic chips compatible with the nrf24L family (at least nrf24L01p, nRF51 and nRF52 tested). In order to communicate with the Crazyradio the target has to be configure correctly:

- PRX mode
- One active pipe with the address configured in the Crazyradio dongle, by default it is 0xE7E7E7E7E7
- 5 byte address
- Dynamic payload length enable
- Payload with ack enable

The Crazyflie is already configured that way. The relevant source code can be seen in radiolink.c.

USB protocol

The USB devices has the VID/PID couple 0x1915/0x7777.

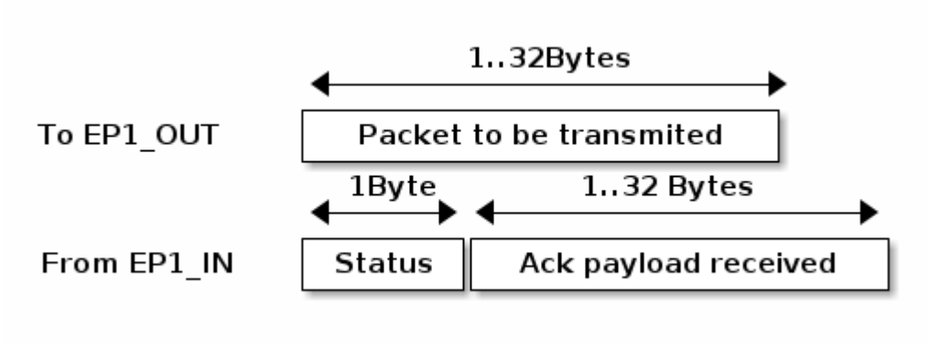
EP0	Control	Control endpoint. Used to configure the dongle
EP1IN/OUT	Bulk	Data endpoints. Used to send and receive radio packets

Data transfer

When the radio dongle is configured to use PTX (emitter) mode it sends a packet to the copter and waits for the acknowledge. The acknowledge can contain a payload which is the mean to receive data. If the auto acknowledge is disabled there is no IN transaction.

To send a packet, the following sequence must be followed:

- Send the packet to EP1_OUT. Its length should be between 1 to 32 Bytes
- Read the ACK from EP1_IN. The first byte is the transfer status and the following bytes are the content of the ACK payload, if any.



The status byte contains flags indicating the quality of the link:

Status Bit	Role
4..7	Number of retransmission
2..3	Reserved
1	Power detector
0	ACK received

Dongle configuration and functions summary

Crazyradio vendor requests summary:

bmRequestType	bRequest	wValue	wIndex	wLength	data
0x40	SET_RADIO_CHANNEL (0x01)	channel	Zero	Zero	None
0x40	SET_RADIO_ADDRESS (0x02)	Zero	Zero	5	Address
0x40	SET_DATA_RATE (0x03)	Data rate	Zero	Zero	None
0x40	SET_RADIO_POWER (0x04)	Power	Zero	Zero	None
0x40	SET_RADIO_ARD (0x05)	ARD	Zero	Zero	None
0x40	SET_RADIO_ARC (0x06)	ARC	Zero	Zero	None
0x40	ACK_ENABLE (0x10)	Active	Zero	Zero	None
0x40	SET_CONT_CARRIER (0x20)	Active	Zero	Zero	None

bmRequestType	bRequest	wValue	wIndex	wLength	data
0x40	START_SCAN_CHANNELS (0x21)	Start	Stop	Length	Packet
0xC0	GET_SCAN_CHANNELS (0x21)	Zero	Zero	63	Result
0x40	LAUNCH_BOOTLOADER (0xFF)	Zero	Zero	Zero	None

Set radio channel

bmRequestType	bRequest	wValue	wIndex	wLength	data
0x40	SET_RADIO_CHANNEL (0x01)	channel	Zero	Zero	None

The nRF24LU1 chip provides 126 Channels of 1MHz from 2400MHz to 2525MHz. The channel parameter shall be between 0 and 125 (if not, the command will be ignored).

The radio channel is set as soon as the USB setup transaction is completed, which takes about 1ms. The new frequency is going to be used for the following transferred packets. The default value for the radio channel is 2.

Set radio address

bmRequestType	bRequest	wValue	wIndex	wLength	data
0x40	SET_RADIO_ADDRESS (0x02)	Zero	Zero	5	Address

The packet sent by the radio contains a 5 bytes address. The same address must be configured in the receiver for the communication to work.

The address must follow the requirement of section 6.4.3.2 of the nRF24LU1 documentation:

```
Addresses where the level shifts only one time (that is, 000FFFFFFF) can often be detected in
noise and can give a false detection, which may give a raised Packet-Error-Rate. Addresses
as a continuation of the preamble (hi-low toggling) raises the Packet-Error-Rate.
```

The default address is 0xE7E7E7E7E7.

Set data rate

bmRequestType	bRequest	wValue	wIndex	wLength	data
0x40	SET_DATA_RATE (0x03)	Data rate	Zero	Zero	None

Possible values for the data rate:

Value	Radio data rate
0	250Kbps
1	1MBps
2	2Mbps (Default)

Set radio power

bmRequestType	bRequest	wValue	wIndex	wLength	data
0x40	SET_RADIO_POWER (0x04)	Power	Zero	Zero	None

Sets the radio amplifier output power. Possible values:

Value	Power
0	-18dBm
1	-12dBm
2	-6dBm
3	0dBm

Configure auto retry (ARD/ARC)

bmRequestType	bRequest	wValue	wIndex	wLength	data
0x40	SET_RADIO_ARD (0x05)	ARD	Zero	Zero	None
0x40	SET_RADIO_ARC (0x06)	ARC	Zero	Zero	None

After sending a packet the radio automatically waits for an acknowledge. ARD and ARC permit to configure the delay the radio waits for the acknowledge and the number of times the transfer will be retried in case the acknowledge is not received in that delay.

The delay ARD depends on the length, in seconds, of the ACK packet. This depends on the data rate and the payload length contained in the ACK packet. The ARD can be configured either by steps of 250us or by ACK payload length. If the ACK payload length is configured, the time will be recalculated automatically even if the data rate is changed. To set the ACK payload length the bit 7 of ARD must be set (length | 0x80).

Possible values for ARD:

Value	ARD wait time

Value	ARD wait time
0x00	250us
0x01	500us
…	…
0x0F	4000us
Value	**ACK payload length**
0x80	0Byte
0x81	1Byte
…	…
0xA0	32Bytes

ARC configures the number of times the radio will retry a transfer if the ACK has not been received, it can be set from 0 to 15.

By default ARD=32Bytes (0xA0) and ARC=3.

Auto ACK configuration

bmRequestType	bRequest	wValue	wIndex	wLength	data
0x40	ACK_ENABLE (0x10)	Active	Zero	Zero	None

By default, the Crazyradio is configured with auto ACK enabled. This means that after transmitting a packet, the radio waits for an acknowledge from the receiver. This setting permits to deactivate waiting for the ACK packet so that the packet will be sent only one time and there is no guarantee that it has been correctly received.

Active values	Meaning
0	Auto ACK deactivated
Not 0	Auto ACK enable (default)

Continuous carrier mode

bmRequestType	bRequest	wValue	wIndex	wLength	data
0x40	SET_CONT_CARRIER (0x20)	Active	Zero	Zero	None

The nRF24L radio chip provides a test mode in which a continuous non-modulated sine wave is emitted. This permits, among other things, to test the quality of the RF elements of the board. When this mode is activated the radio dongle does not transmit any packets.

While the continuous carrier mode is active, it is possible to set channel and power to change the frequency and power of the emitted wave.

Active values	Meaning
0	Dongle working normally (default)
Not 0	Dongle in continuous carrier mode

Channels scanning

This function is implemented in Crazyradio version 0.5 and over.

bmRequestType	bRequest	wValue	wIndex	wLength	data
0x40	START_SCAN_CHANNELS (0x21)	Start	Stop	Length	Packet
0xC0	GET_SCAN_CHANNELS (0x21)	Zero	Zero	64	Result

Scan a range of channels and compile a list of channel from which an ACK has been received. The command START_SCAN_CHANNELS should be executed first with start being the first scanned channel and stop the last one. Those should be within 0 to 125. The data is the packet payload sent on each channel, it should be at least one byte long.

All parameters, except the channel, are used unmodified during the scan. If the data rate is set to 2MBPs the scan is done every second channel. To get the list of channels that answered, GET_SCANN_CHANNELS should be called just after a scan. Up to 63 bytes are returned corresponding to up to 63 channels on which the packet was acknowledged.

Note After scanning, the channel will be set to the last scanned channel.

Warning On some platform, an empty scan will return a buffer of 64 bytes. This is though to be a USB host implementation bug, see ticket #9 in the Crazyradio firmware project. If a buffer of more than 63 bytes is returned, it means that no channel have been received.

Launch bootloader

bmRequestType	bRequest	wValue	wIndex	wLength	data
0x40	LAUNCH_BOOTLOADER (0xFF)	Zero	Zero	Zero	None

This command is used to launch the Nordic semiconductor USB bootloader. After sending this command, a USB reset shall be emitted which will trigger the dongle to start the bootloader. After sending this command, the Dongle is only waiting for a USB reset which means that any other commands or data will be ignored.

The bootloader is pre-loaded by Nordic Semi. in the nRF24LU1 chip at the address 0x7800. The Crazyradio firmware will jump to it when the sequence LAUCH_BOOTLOADER followed by a USB reset is executed. The bootloader will appear at VID/PID of 0x1915/0x0101. See nRF24LU1 datasheet for the bootloader documentation.

A PC client for the bootloader is part of the Crazyflie ground station program.

Radio protocol

The Crazyradio dongle is currently only operating in PTX mode. To get a downlink from the copter the ACK payload is used, which means that data are received only when data are sent. In the case of Crazyflie, to have bidirectional communication even when no data is send, a null packet (0xff) is sent periodically to pull the downlink data stream.

For Crazyflie the communication protocol is described in Communication protocol Overview.