

Mesh packet

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46
Protocol	Access address				Adv. Type	Length	Advertisement address				Ad length	Service UUID	Handle	DFU Data																																CRC	

All fields are little endian.

Serial command packet

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
Length	OPCODE				Handle	DFU Data																							

Length = dfu-packet length + 1

Serial event packet

	0	1	2	3	4	5	6	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29
Debug	Length	OPCODE				Handle	DFU Data																						

Debug = 0, Length = dfu-packet length + 1

GATT Mesh characteristic transfer

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27
OPCODE	Handle		DFU Data																									

Length is given as part of the GATT write metadata, OPCODE = 0x00

DFU BEACON	FWID	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15								
		0xFFEE	SD	VERSION				Company ID			App ID		App version												
STATE	DFU READY APP	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21		
		0xFFFD	Type	Authority				Transaction ID			Company ID		App ID		App version										
	DFU READY SD	0	1	2	3	4	5	6	7	8	9	10	11	12	13										
		0xFFFD	Type	Authority				Transaction ID			SD		VERSION												
		DFU READY BOOTLOADER	0	1	2	3	4	5	6	7	8	9	10	11	12	13									
			0xFFFD	Type	Authority				Transaction ID			BOOTLOADER		VERSION											
DATA	START DFU	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18					
		0xFFFC	0	Transaction ID				START ADDRESS			LENGTH / 4			Sign	length	FLAGS									
	DFU DATA	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
		0xFFC	SEGMENT	Transaction ID				DATA SEGMENT																	
RECOVERY	DFU DATA REQ	0	1	2	3	4	5	6	7																
		0xFFB	SEGMENT	Transaction ID																					
	DFU DATA RSP	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
		0xFFA	SEGMENT	Transaction ID				DATA SEGMENT																	
?	RELAY REQUEST	0	1	2	3	4	5	6	7	8	9	10	11												
		0xFF9	Transaction ID				Adv addr																		

Bitfields								
Type	0	1	2	3	4	5	6	7
	Software Bootloader		Application	BL info	RFU			
Authority	0	1	2	3	4	5	6	7
	Authority level		Flood		Relay node	RFU		
START FLAGS	0	1	2	3	4	5	6	7
	DIFF	SINGLE BANK	FIRST	LAST	RFU			

- Flags: all are currently ignored.
- Transaction ID is a completely random 32bit number
- Flood field: indicate whether the transmission should be relayed unconditionally
- Relay node field: true if the device only participates passively, but don't flash the content
- If start address is not 16byte-aligned, the first data packet contains (16 - (START_ADDR & 0x0F)) bytes, making the second packet 16byte-aligned, ie the first packet fills the rest of the first 16byte segment.

Segment address offset: SEG 1 = START_ADDR, SEG N > 1 = (START_ADDR + 16 * (i-1)) & 0xFFFFFFF0