James Ball → http://blog.jamesball.co.uk/2013/02/sma-bluetooth-level-2-packet-format.html

SMA Bluetooth Level 2 Packet Format

Please see my other post for discussion of the use of the packets - this post is just to record the specific details of the packet layout.

SMA Bluetooth Level 2 Protocol Format

Byte #	Name	Description	Possible values
1	Head	Indicates the start of a packet. Always 0x7e.	0x7e
2-5	Header	Indicates the start of a packet. 0x6065 indicates that this is SMA Net2+.	0xff036065
6	Packet length	Length of the packet in 4-byte words - length * 4 = bytes. Doesn't include header, FCS or 0x73 footer.	0x07 up
7	Destination address header	Function unknown. 0xa0 is used when the address is a broadcast one. 0xe0 is used when destination is inverter. 0x80, 0xc0 used when destination is computer.	0x80, 0xa0, 0xc0, 0xe0
8-13	Destination address	6-byte address. It seems to be one byte value, one byte 0 then serial number (not MAC address) of device. In the example the serial number is 2001787857 which translates to 0xd1db5077.	Example: 0x6300d1db5077
14	Padding	Always 0x00.	0x00
15	Source address header	Function unknown. Not sure how these are split. Some only seem to be used when destination is a broadcast address.	0x00, 0x01, 0x03, 0x05, 0xa0, 0xe0
16-21	Source address	6-byte address. It seems to be one byte value, one byte 0 then serial number (not MAC address) of device. In the example the serial number is 2001787857 which translates to 0xd1db5077.	Example: 0x6300d1db5077
22-23	Mystery 1	Two bytes of unknown function. Almost always set to 0x0000. Other values only seen when command is 0xfdff.	0x00 (occasionally 0x01, 0x03 or 0x05)
24	Acknowledge	This is either 0x00 (majority) or 0x15. 0x15 only comes from inverter and seems to be some form of acknowledgement.	0x00 or 0x15
25	Mystery 2	Unknown, always 0x00	0x00
26	Telegram number	For very long responses the inverter may choose to send multiple packets. If so it will set a telegram number. If this is 0x00 then the response is one packet or this is the last packet. So 0x06 means there are seven packets in the response. (I think it is possible to send more than 256 packets - you count down to 0x01 then go back up to 0xff - only sending 0x00 for the last packet.)	0x00 to 0xff
27	Mystery 3	Unknown, always 0x00	0x00
28	Counter	Each packet sent includes a counter - the response will have the same counter value to allow you to know which incoming packets correspond to your request. After 0xff return to 0x00 and continue.	0x00 to 0xff then 0x00…
29	Command Group 1	I think this is an indicator that the current packet is the first in a command or response. This value is always 0x80 unless the response is over multiple packets in which case it will be 0x80 for the first packet and 0x00	0x80 or 0x00 (0x81 and 0x01 after counter goes round past 0xff)

Byte #	Name	Description	Possible values
		for all the remaining packets. (Update: I have also seen 0x81 and 0x01 and wasn't sure the purpose. I've now checked. It seems that once the counter goes past 0xff then Command Group 1 has one added. I haven't sniffed for long enough to see if it goes to 0x82, 0x83 etc each time the counter rolls over)	
30	Command Group 2	I think this is mainly used to indicate if the packet is a request or a response. It is sent from the computer as 0x00 and returned with data as 0x01. Other values are seen, rarely, and seem to be related to specific commands (0xfdff and 0x00f0).	0x00 and 0x01 (0xc0, 0xd0 and 0xe0 seen with command 0xfdff and 0xa0 with command 0x00f0)
31	Command Group 3	Not sure of purpose. For normal commands it is aways 0x02. For command 0xfdff it is another value.	0x02. (For 0xfdff is is 0x00, 0x01 or 0x04)
32-33	Command	Two byte command. The data set after the command can change the results significantly. Some require dates but others specific strings. See separate table for command details)	example 0x0070 or 0xfdff
34+	Data	Data content of the packet. Format of data varies by comand.	Series of bytes.
Last-but-3 bytes (2)	FCS	Two bytes of the calculated FCS value. Standard PPP FCS calculation. See SMA Data specification for details. Calculated on all bytes from Header to Data inclusive.	Two bytes
Last byte	Footer	Terminates the packet, always 0x7e.	0x7e

Command Possible Request Values

Command	Name	Request Data	Response
0x0000	I am here	8-bytes of 0	None
0x0051		0x00002000ffff5f00	power now, max power phases 1-3, ac voltage, ac current, grid frequency, 0x1f4a
0x0054	Totals	0x00002000ffff5f00	Total generated, total today, operating time, feed in time
0x0058	Unknown	-	Data set in 4-byte chunks. 1) start frame number 2) end frame number 3) Data in 40 byte cycles
0x0061	Power now	0x00002600ffff2600	Data set in 4-byte chunks. 1) Start frame number 2) End frame number 3) Data 40 byte cycles, 4-byte type code, 4-byte time stamp, 4-byte value, 4-byte value, 4-byte value, 4-byte value, 4-byte padding. Values in Watts. Four values usually the same. Not sure why repeated.
0x0061	Max Phase power	0x00004100ffff4100	Data set in 4-byte chunks. 1) Start frame number 2) End frame number 3) Data 28 byte cycles, 4-byte type code, 4-byte time stamp, 4-byte value, 4-byte value, 4-byte value, 4-byte value, 4-byte padding. Values in Watts. Four values usually

Command	Name	Request Data	Response
			the same. Not sure why repeated - I think the 3rd value is how much is active. I have a single phase system and only Phase 1 has a value for the third position.
0x0064	Totals	0x00002600ffff2600 or 0x00004600ffff4600	Total generated, total generated today. OR Feed in time, operating time.
0x0068	????	-	-
0x0070	Request historical yield (by 5 mins)	4-byte unix timestamp for start and 4-byte unix timestamp for end. Data returned between dates. Standard if requesting a day is from 22:00 the day before to 21:59:59 on the day.	Data set in 4-byte chunks. 1) Start frame number 2) End frame number 3) Data 12 byte cycles, 4-byte time stamp, 4-byte value, 4-byte padding. Values in Watt hours.
0x00f0	Time set	0x006d2300006d2300006d2300	-
0x1070	See 0x0070	This seems to be 0x0070 once the counter has gone round.	-
0x2063	????	No data returned	-
0x2070	Request yield (by day)	time stamp start, time stamp end	As 0x0070
0x4063	????	No data returned	-
0x8051	????	-	-
0x8053	DC values	0x00002000ffff5f00	Returns DC voltage and DC current. 4-byte chunks. 1) Start frame number 2) End frame number 3) Data 28 byte cycles
0x8061	????	-	-
0x8063	DC values	0x00004500ffff4500	Returns DC voltage and DC current. 4-byte chunks. 1) Start frame number 2) End frame number 3) Data 28 byte cycles
0xf5ff	????	0x00000000ffffffff	0x00000000ffffffff
0xfdff	????	Part of log in but other uses too. I think it can be used as a keep alive.	

Date Type Codes

Code	Description	Unit
0x1e41	Max power phase 1	Watts
0x1f41	Max power phase 2	Watts
0x2041	Max power phase 3	Watts
0x3f26	Power now	Watts
0x0126	Total generated	Watt hours
0x2226	Total generated today	Watt hours
0x4846	AC line voltage phase 1	Volts/100
0x5046	AC current phase 1	milli Amps
0x5746	Grid frequency	Hertz/100
0x2e46	Inverter operating time	Seconds

Code	Description	Unit
0x2f46	Inverter feed-in time	Seconds
0x1f45	DC voltage	Volts/100
0x2145	DC current	milli Amps
0x1f4a	????	?
-	-	-