

微光 RS485 通讯协议 V0.6

协议格式:

Master transmit data

SOH	Head			Data			Check	EOT
01H	Type	ID	FC	Length	Data	ETX 03H	Check Sum	04H
1byte	1byte	1byte	1byte	1byte/2bytes	nbytes	1byte	1byte	1byte

Reader respond data

SOH	Head			Data			Check	EOT
01H	Type	ID	FC	Length	Data	ETX 03H	Check Sum	04H
1byte	1byte	1byte	1byte	1byte/2bytes	nbytes	1byte	1byte	1byte

说明:

1. SOH,ETX,EOT 是一个字节的控制字。
2. Type 是设备类型，固定为 33H。
3. ID Reader 的地址范围：1-255。00 为广播地址（仅在 02H 指令中使用）。
4. FC 是功能代码，用一个字节。
5. Length 是数据的长度。Length=0 时，没有 ETX 项。
6. Check Sum 一个字节，所有数据的累加和，取低字节作校验码。
7. 默认通讯协议采用：19200，N，8，1。
8. 设备出厂带有下面默认参数，可以通过协议更改这些参数：
 固件默认 设备地址为： 0x01
 固件默认 SN 号为： abcdefgh
 默认串口配置为： 19200-8-N-1
9. 指令轮询速度 60ms

Command	Function
01H	设置/获取出厂序列号
02H	设置/获取读卡器 ID
06H	设置/获取读卡器 解码密钥（作废）
20H	获取解密后的数据/控制动作（作废）
21H	获取原始数据/控制动作
30H	设置系统参数
50H	读取 M1 卡的某个块
52H	写数据到 M1 卡的某个块
53H	设置 NFC 模块进入 命令读写模式
54H	发送 COS 指令
60H	蓝牙数据发送

Function Code: 01H			Function: Set/Get Factory Serial No	
说明: Data1-Data8 为 0-9 的 ASCII Code 当命令中数据长度为 08H 时, 表示设置序列号, 此时返回数据长度为 00H; 当命令中数据长度为 00H 时, 表示获取序列号, 此时返回数据长度为 08H。 注: Length=0 时, 无 ETX 项。				
序号	PC→Reader(Send)		Reader→PC(Receive)	
	Description	Content	Description	Content
01	起始字符(SOH)	01H	起始字(SOH)	01H
02	设备类型(Type)	33H	设备类型(Type)	33H
03	地址(ID)	01H-FFH	地址(ID)	01H-FFH
04	命令(FC)	01H	命令(FC)	01H
05	数据长(Length)	08H/00H	数据长(Length)	00H/08H
06	Data1	1Byte	Data1	1Byte
07	Data2	1Byte	Data2	1Byte
08	Data3	1Byte	Data3	1Byte
09	Data4	1Byte	Data4	1Byte
10	Data5	1Byte	Data5	1Byte
11	Data6	1Byte	Data6	1Byte
12	Data7	1Byte	Data7	1Byte
13	Data8	1Byte	Data8	1Byte
14	数据结束(ETX)	03H	数据结束(ETX)	03H
15	校验(Check Sum)	以上求和	校验(Check Sum)	以上求和
16	结束字符(EOT)	04H	结束字符(EOT)	04H

例如:

为 Device Id 为 0x01 的设备设置 SN 为 12345678:

PC-->Reader :01 33 01 01 08 31 32 33 34 35 36 37 38 03 E5 04

Reader-->PC :01 33 01 01 00 36 04

获取 Device Id 为 0x01 设备的 SN 号:

PC-->Reader :01 33 01 01 00 36 04

Reader-->PC :01 33 01 01 08 31 32 33 34 35 36 37 38 03 E5 04

Function Code: 02H			Function: Set/Get ReaderID	
说明: Data1-Data8 ->0-9 的 ASCII Code ,是 Reader 的 SN (Factory Serial No)。 Data9->ReaderID 要设定的 ID, 即设备地址（当获取 ID 时, 无需传输该字节）。				
Reader 收到此命令时, 首先检查 Serial No 是否正确, 如果正确则: 命令数据长度为 09H, ID 设置为 Data9, 返回长度为 00H 字节; 命令数据长度为 08H, 返回长度为 01H 字节, 内容为本机 ID。 注: Length=0 时, 无 ETX 项。				
序号	PC→Reader(Send)		Reader→PC(Receive)	
	Description	Content	Description	Content
01	起始字符(SOH)	01H	起始字符(SOH)	01H
02	设备类型(Type)	33H	设备类型(Type)	33H
03	地址(ID)	00H	地址(ID)	00H
04	命令(FC)	02H	命令(FC)	02H
05	数据长(Length)	09H/08H	数据长(Length)	00H/01H
06	Data1	1Byte	本机(ID)	xxH
07	Data2	1Byte	数据结束(ETX)	03H
08	Data3	1Byte	校验(Check Sum)	以上求和
09	Data4	1Byte	结束字符(EOT)	04H
10	Data5	1Byte		
11	Data6	1Byte		
12	Data7	1Byte		
13	Data8	1Byte		
14	Data9	1Byte		
15	数据结束(ETX)	03H		
16	校验(Check Sum)	以上求和		
	结束字符(EOT)	04H		

例:

为 SN 为 12345678 的设备设置 Device Id 为 0x05:

PC-->Reader :01 33 00 02 09 31 32 33 34 35 36 37 38 05 03 EB 04

Reader-->PC :01 33 00 02 00 36 04

获取 SN 为 12345678 的设备的 Device Id :

PC-->Reader :01 33 00 02 08 31 32 33 34 35 36 37 38 03 E5 04

Reader-->PC :01 33 00 02 01 05 03 3F 04

Function Code: 06H			Function: Set/Get Decoder Key	
说明: Data1-Data16 为可见字符的 ASCII Code 当命令中数据长度为 10H 时, 表示设置 Key, 此时返回数据长度为 00H; 当命令中数据长度为 00H 时, 表示获取 Key, 此时返回数据长度为 10H。 注: Length=0 时, 无 ETX 项。				
序号	PC→Reader(Send)		Reader→PC(Receive)	
	Description	Content	Description	Content
01	起始字符(SOH)	01H	起始字符(SOH)	01H
02	设备类型(Type)	33H	设备类型(Type)	33H
03	地址(ID)	01H-FFH	地址(ID)	01H-FFH
04	命令(FC)	06H	命令(FC)	06H
05	数据长(Length)	10H/00H	数据长(Length)	00H/10H
06	Data1	1Byte	Data1	1Byte
07	Data2	1Byte	Data2	1Byte
08	Data3	1Byte	Data3	1Byte
09	Data4	1Byte	Data4	1Byte
10	Data5	1Byte	Data5	1Byte
11	Data6	1Byte	Data6	1Byte
12	Data7	1Byte	Data7	1Byte
13	Data8	1Byte	Data8	1Byte
14	Data9	1Byte	Data9	1Byte
15	Data10	1Byte	Data10	1Byte
16	Data11	1Byte	Data11	1Byte
17	Data12	1Byte	Data12	1Byte
18	Data13	1Byte	Data13	1Byte
19	Data14	1Byte	Data14	1Byte
20	Data15	1Byte	Data15	1Byte
21	Data16	1Byte	Data16	1Byte
14	数据结束(ETX)	03H	数据结束(ETX)	03H
15	校验(Check Sum)	以上求和	校验(Check Sum)	以上求和
16	结束字符(EOT)	04H	结束字符(EOT)	04H

例:

获取 Device Id 为 0x01 的解密 KEY

PC-->Reader : 01 33 01 06 00 3B 04

Reader-->PC : 01 33 01 06 10 55 6E 51 6B 76 4E 70 58 4D 71 35 79 56 79 37 44 03 0F 04

设置 Device Id 为 0x01 的解密 KEY 为 mwJqxGLSxShB4Gju

PC-->Reader : 01 33 01 06 10 6D 77 4A 71 78 47 4C 53 78 53 68 42 34 47 6A 75 03 1A 04

Reader-->PC : 01 33 01 06 00 3B 04



Reader-->PC: 01 33 01 21 00 07 01 31 32 33 34 35 36 03 96 04 (有码数据)

Function Code: 30H			Function: Set/Get Parameter	
说明： 发送数据为 TLV 协议格式*； 回复数据为 2 字节，9000H 为成功，6001H 为失败。				
序号	PC→Reader(Send)		Reader→PC(Receive)	
	Description	Content	Description	Content
01	起始字符(SOH)	01H	起始字符(SOH)	01H
02	设备类型(Type)	33H	设备类(Type)	33H
03	地址(ID)	01H-FFH	地址(ID)	01H-FFH
04	命令(FC)	30H	命令(FC)	30H
05	数据长度	1byte	数据长度	02H
06	Data	N bytes	Data	2 bytes
07	数据结束(ETX)	03H	数据结束(ETX)	03H
08	校验(Check Sum)	以上求和	校验(Check Sum)	以上求和
09	结束字符(EOT)	04H	结束字符(EOT)	04H

TLV 说明

TLV 是 Tag、Length、Value 的简称。

每一个不同的 Tag 代表不同的数据，如“波特率”、“二维码超时时间”、“时间”等。

Tag 由二部分组成：

第一部分：用第一个字节的 Bit8-Bit6 表示数据类型(Data Type)，

Bit8-Bit6=0，表示整型数据

Bit8-Bit6=1，表示 Ascii 码数据

Bit8-Bit6=2，表示 BCD 码

Bit8-Bit6=3，表示连续的二进制字节数据（如：由控制器传来的照片数据，指纹数据等）

Bit8-Bit6=4，表示“^”分隔的字节数据（如：由 CC 传给 CS 的指纹数据等）。

Bit5=0，发送标签数据，Bit5=1：获取标签数据。

第二部分：剩下的 Bit4-Bit1 加上第二个字节共 12 个 Bits 表示数据标签(Data Tag)。

举例：比如数据是 Ascii，Tag 为 12，则 Tag 为 10H，0CH。

Length 固定两个字节，表示数据的长度。获取标签数据的时候，Length 为 0。

Value 是该 Tag 的数据，数据长度由 Length 决定。

数据包结构中的 Data 部分就采用 TLV 格式：

数据标签 Data tag	标签名称 Data name	数据类型 Data type	数据长度 Length	备注 Memo
001H	波特率	0H	0004H	115200 38400 19200 9600
002H(注 1)	二维码超时时间	0H	0004H	单位为秒
003H(注 2)	日期时间	0H	0007H	格式如下： 第一个字节为(year-2000) 第二个字节为 month 第三个字节为 date 第四个字节为 hour 第五个字节为 minute 第六个字节为 second 第七个字节为 weekday (0 代表周日，1 代表周一，以此类推) 此处时间为 UTC 时间
注 1：二维码超时时间是用于设置二维码失效的上限时间。 注 2：修改设备波特率，PC 接收到设备回复后，PC 端需延时 2 秒再发下一条指令				

例：

获取 Device Id 为 0x01 的设备时间

PC-->Reader : 01 33 01 30 04 00 03 00 00 03 6F 04

Reader-->PC : 01 33 01 30 09 14 07 15 07 28 39 02 90 00 03 9B 04

14H ==>> year- 2020

07H==>> month- 07

15H ==>> date- 21

07H==>> hour- 07

28H==>> minute- 40

39H==>> second- 57

02H==>> Tuesday- 02

即：2020 年 07 月 21 日 星期二 07:40:57 UTC

设置 Device Id 为 0x01 的波特率为 19200

PC-->Reader : 01 33 01 30 08 00 01 00 04 00 00 4b 00 03 C0 04

Reader-->PC : 01 33 01 30 02 90 00 03 FA 04

设置 Device Id 为 0x01 的波特率为 115200

PC-->Reader : 01 33 01 30 08 00 01 00 04 00 01 C2 00 03 38 04

Reader-->PC : 01 33 01 30 02 90 00 03 FA 04

Function Code: 50H			Function: Read A Block From M1 Card	
说明： 秘钥类型：0x60 表示采用 A 秘钥认证，0x61 表示采用 B 秘钥认证。				
注 1： 块号：S50 卡为 0~63；S70 卡为 0~255。				
注 2： 标识字：0x00 表示成功，0xFF 表示失败或无卡。				
注 3： 读取 M1 卡某块数据成功，读卡器返回数据长度为 11H，即标识字+16bytes 数据。 读取失败或无卡时返回数据长度为 01H，1 byte 标识字。				
序 号	PC→Reader(Send)		Reader→PC(Receive)	
	Description	Content	Description	Content
01	SOH	01H	SOH	01H
02	Type	33H	Type	33H
03	ID	01H-FFH	ID	01H-FFH
04	命令(FC)	50H	命令(FC)	50H
05	数据长(length)	08H	数据长度(length)	01H/11H
06	秘钥类型	1 byte	标识字(注 2)	1byte
07	块号(注 1)	1 byte	数据域(注 3)	16 bytes
08	秘钥	6 bytes	数据结束(ETX)	03H
09	数据结束(ETX)	03H	校 验(Check Sum)	以上求和
10	校 验(Check Sum)	以上求和	结束字(EOT)	04H
11	结束字符(EOT)	04H		

例：

读测试卡的第 01 扇区 01 块

PC-->Reader : 01 33 01 50 08 60 04 FF FF FF FF FF FF 03 EE 04

失败或无卡

Reader-->PC : 01 33 01 50 01 FF 03 88 04

读块成功

Reader-->PC : 01 33 01 50 11 00 29 23 BE 84 E1 6C D6 AE 52 90 49 F1 F1 BB E9 EB 03 94 04

Function Code: 52H			Function: Write Data To A Block Of M1 Card	
说明： 秘钥类型：0x60 表示采用 A 秘钥认证，0x61 表示采用 B 秘钥认证。				
注 1： 块号：S50 卡为 0~63；S70 卡为 0~255。				
注 2： 标识字：0x00 表示成功，0xFF 表示失败或无卡。				
注 3： 向 M1 卡某块写入数据， 数据长度(18H)=秘钥类型 1 byte + 块号 1 byte + 密钥 6 bytes + 待写入数据 16 bytes。				
序 号	PC→Reader(Send)		Reader→PC(Receive)	
	Description	Content	Description	Content
01	SOH	01H	SOH	01H
02	Type	33H	Type	33H
03	ID	01H-FFH	ID	01H-FFH
04	命令(FC)	52H	命令(FC)	52H
05	数据长度(length)	18H(注 3)	数据长度(length)	01H
06	秘钥类型	1 byte	标识字(注 2)	1 byte
07	块号(注 1)	1 byte	数据结束(ETX)	03H
08	秘钥	6 bytes	校 验(Check Sum)	以上求和
09	写入的数据	16 bytes	结束字符(EOT)	04H
10	数据结束(ETX)	03H		
11	校 验(Check Sum)	以上求和		
12	结束字符(EOT)	04H		

例：

写测试卡的第 01 扇区 02 块

PC-->Reader :

01 33 01 52 18 60 05 FF FF FF FF FF FF 12 34 56 78 90 12 34 56 78 90 12 34 56 78 90 12 03 FF 04

失败或无卡

Reader-->PC : 01 33 01 52 01 FF 03 8A 04

写块成功

Reader-->PC : 01 33 01 52 01 00 03 8B 04

注：该指令适用于 V0.5 版本协议，新用户可不必使用该指令进行命令模式设置。

Function Code: 53H			Function: Set NFC Enter CMD Mode	
说明： 只有在命令模式下，NFC 才响应块的读写等操作。 只有关闭了命令模式，刷卡后，才会主动上报卡号。				
注 1： 0x01 模块进入命令模式， 0x00 模块退出命令模式。				
注 2： 0x00 表示成功， 0xFF 表示失败。				
序 号	PC→Reader(Send)		Reader→PC(Receive)	
	Description	Content	Description	Content
01	SOH	01H	SOH	01H
02	Type	33H	Type	33H
03	ID	01H-FFH	ID	01H-FFH
04	命令(FC)	53H	命令(FC)	53H
05	数据长(length)	01H	数据长度(length)	01H
06	数据域(注 1)	1byte	标识字(注 2)	1byte
07	数据结(ETX)	03H	数据结束(ETX)	03H
08	校 验(Check Sum)	以上求和	校 验(Check Sum)	以上求和
09	结束字符(EOT)	04H	结束字符(EOT)	04H

例：

开启命令模式: 01 33 01 53 01 01 03 8D 04

关闭命令模式: 01 33 01 53 01 00 03 8C 04

Function Code: 54H			Function: Send COS CMD	
说明： 用于 ISO14443-4 TYPE A CPU 卡片操作，具体 cos 指令请参阅 Type A CPU 卡数据手册。				
注 1： 0x00 表示成功，0xFF 失败。				
注 2： 标识字非 0x00 时，数据域为空。				
序号	PC→Reader(Send)		Reader→PC(Receive)	
	Description	Content	Description	Content
01	SOH	01H	SOH	01H
02	Type	33H	Type	33H
03	ID	01H-FFH	ID	01H-FFH
04	命令(FC)	54H	命令(FC)	54H
05	数据(length)	1 byte	数据长度(length)	1 byte
08	数据域	COS 指令	标识字(注 1)	1 byte
09	数据结(ETX)	03H	数据域(注 2)	N bytes
10	校 验(Check Sum)	以上求和	数据结束(ETX)	03H
11	结束字(EOT)	04H	校 验(Check Sum)	以上求和
12			结束字符(EOT)	04H

例：

获取 8 位随机数

PC-->Reader : 01 33 01 54 05 00 84 00 00 08 03 1D 04

失败或无卡

Reader-->PC : 01 33 01 54 01 FF 03 8C 04

获取随机数成功

Reader-->PC : 01 33 01 54 0B 00 08 30 73 16 36 0C B4 51 90 00 03 2F 04

Function Code:60H			Function: Pass-Through	
说明：蓝牙数据发送 蓝牙从设备收到的透传数据只包含数据域部分。				
注 1： 连接号为 0x00 时，群发数据，数据会发送到所有已连接的蓝牙设备。 若连接号非 0x00,则表示向指定连接设备发送数据。				
注 2： 0x00 发送成功，0xFF 表示指定设备不存在或发送失败。				
序号	PC→Reader(Send)		Reader→PC(Receive)	
	Description	Content	Description	Content
01	SOH	06H	SOH	06H
02	Type	33H	Type	33H
03	ID	01H-FFH	ID	01H-FFH
04	命令(FC)	09H	命令(FC)	09H
05	数据长(length)	2 bytes	数据长(length)	2 bytes
06	连接号(注 1)	1 byte	标识字(注 2)	1 byte
07	数据域	n bytes	数据结束(ETX)	03H
08	数据结束(ETX)	03H	校验(Check Sum)	以上求和
09	校(CheckSum)	以上求和	结束字符(EOT)	08H
10	结束字符(EOT)	08H		

例：

蓝牙群发数据：

PC-->Reader :06 33 01 09 00 06 01 12 34 56 78 90 03 F1 08

发送成功：

Reader-->PC :06 33 01 09 00 01 00 03 47 08

发送失败：

Reader-->PC :06 33 01 09 00 01 FF 03 46 08

修改记录表

版本号	修改原因	修改类型	修改内容摘要	修改人	修改日期	执行日期	备注
0.4	初版						
0.5	增加操作 IC 卡功能		1、增加 M1 读写扇区 2、CPU 卡 cos 指令				
0.6	增加蓝牙数据透传指令，完善协议		3、废除 06、20H 指令 4、完善协议，更新协议说明 5、增加蓝牙透传指令		2020/07/21		