HYB630 系列高频大中功率
ISO18000-3M3 协议电子标签读写器
用户手册 V1.01

目录

1. 通讯接口规格

HYB630 系列读写器通过 RS232 串行通讯接口或网络接口与上位机(单片机，微处理器，控制器等)实现数据通讯，按上位机的命令要求完成相应操作。串行通讯接口的数据帧为 1 个起始位、8 个数据位、1 个停止位，无奇偶效验位，默认波特率 19200。在串行通讯过程中，最低有效字节最先传输，每个字节的最低有效位最先传输。网络的默认的 IP 地址为 192.168.1.192，工作在 TCP server 模式下，本地服务器端口为 6000。

2. 协议描述

通讯过程必须先由上位机发送命令和数据给读写器，然后读写器将命令执行结果状态和数据返回给上位机。

主机的命令发送过程如下表：

上位机	数据传递方向	读写器	说明
命令数据块	→		串行接口中，上位机发送的数据串中，每两个相邻字节之间的发送时间间隔必须小于 10ms。在上位机的命令数据块发送过程中，如果接收到任何读写器的数据，均表示上位机和下位机通讯失步，上位机停止发送数据，等待 15ms 未接收到读写器的数据后重新发送命令数据块。 网络接口中，上位机发送的数据串中，每两个相邻字节之间的发送时间间隔必须小于 300ms。超过此时间，将会丢弃之前的接收到的数据。

上位机发给读写器的命令数据块必须符合该协议的格式规定，将包含读写器地址、操作命令符、操作控制符、命令操作数、CRC-16 等的命令数据块发送至读写器，然后等待其返回命令执行结果。

读写器在收到主机命令（询查 Inventory 命令和集合询查命令例外）后的 1.5s（不包括与上位机传送数据的时间）内完成命令执行，然后返回结果。在这段时间内，读写器不对上位机发送的数据进行处理的。命令执行结果的返回过程如下表：

读写器	数据传递方向	上位机	说明
响应数据块	→		每两个相邻字节之间的发送时间间隔必须小于 10ms（串口，网络接口为 80ms）。

读写器执行命令，得到结果后，将包含读写器地址、命令执行结果状态值、响应数据等的响应数据块发送至上位机。至此，一次完整的通讯过程结束。

3. 数据块的格式

A. 命令数据块

Len	Com_adr	Cmd	State	Data[]	LSB-CRC16	MSB-CRC16

Len： 长度为 1 个字节的命令数据块长度（不包括自身的一个字节），取值范围 5～25。Len 的长度等于（5+Data[]）的长度。注意，Len 的值必须和后面所跟的实际数据个数相符。

Com_adr： 长度为 1 个字节的读写器地址。取值为 0～254 时，只有与此地址相符的读写器会对该命令数据块有响应。取值为 255 是广播地址，所有读写器都会对命令数据块有响应。

Cmd： 长度为 1 个字节的操作命令符。

State： 长度为 1 个字节的操作控制符，取值含义详见每条命令。

Data[]： 命令操作数，给出运行命令所必须的数据。若 Len=5 则无此项。

CRC16： 长度为 2 个字节的 CRC-16 效验和。低字节在前。

B. 响应数据块

Len	Com_adr	Status	Data[]	LSB-CRC16	MSB-CRC16

Len： 长度为 1 个字节的响应数据块长度，取值范围 4～255，为 4 表示无操作数。Len 的长度等于（4+Data[]）的长度。

Com_adr： 长度为 1 个字节的读写器地址，取值为 0～254。

Status： 长度为 1 个字节的命令执行结果状态值，它的含义详见后面的表说明。

Data[]： 响应数据，运行命令后得到的电子标签信息。若 Len=4 则无此项。

CRC16： 长度为 2 个字节的 CRC-16 效验和。低字节在前。

注意，当命令数据块不符合要求的时候，读写器将不会有任何响应。

读写器地址 Com_adr 的缺省配置是 0x00。用户可以通过读写器自定义命令中的“Write Com_adr”来改变。

循环冗余码校验（CRC）的计算包括了从 Len 开始的全部数据，得到的 CRC 在传送时低字节在前。所用的 CRC 生成多项式同 ISO/IEC 15693 协议中定义的一样，但是需要注意，这里的计算结果不取反。例子：我们给定一个数据块 0x05,0xFF,0x01,0x00,LSB-CRC,MSB-CRC，通过 CRC 计算得到的数据是 LSB-CRC＝0x5D，MSB-CRC＝0xB2。这样，当收到 0x05,0xFF,0x01,0x00,0x5D,0xB2 这样的数据块时，对它们（全部的 6 个字节）

进行 CRC 计算，如果所得到的值是 0x00 和 0x00 就通过了校验。下面给出一个 C 语言的 CRC 计算程序供参考：

```
Polynomial:       POLYNOMIAL=0x8408;
Start Value:      PRESET_VALUE=0xffff;
C-Example:
    int                     i,j;
    unsigned      int       current_crc_value=PRESET_VALUE;

    for(i=0;i<len;i++)    /*len=number of protocol bytes without CRC*/
    {
        current_crc_value=current_crc_value^((unsigned    int)pData[i]);
        for(j=0;j<8;j++)
        {
            if(current_crc_value&0x0001)
            {
                current_crc_value=(current_crc_value>>1)^POLYNOMIAL;
            }
            else
            {
                current_crc_value=(current_crc_value>>1);
            }
        }
    }
        pData[i++]=(unsigned char)(current_crc_value&0x00ff);
        pData[i]=(unsigned char)((current_crc_value>>8)&0x00ff);
```

4. 命令执行结果状态值(Status)列表

下面给出了在 ISO/IEC15693 和 ISO18000-3 协议的情况下，包含不同的状态值时的响应数据块以及它们的含义和说明。

响应数据块					Status 含义	说明
Len	Com_adr	**Status**	Data[]	CRC-16		
4+Data[]部分的字节数	0xXX	**0x00**	……	LSM+MSB	操作成功	当成功执行命令后返回给上位机的状态值。数据块包含了所要信息
4	0xXX	**0x01**	无此项	LSM+MSB	命令操作数长度错误	上位机发送的命令数据块中的命令操作数长度不符合此命令要求时返回给上位机的状态值
4	0xXX	**0x02**	无此项	LSM+MSB	操作命令不支持	上位机发送的命令数据块的操作命令不被读写器支持时返回给上位机的状态值
4	0xXX	**0x03**	无此项	LSM+MSB	操作数范围不符	上位机发送的命令数据块中的命令操作数，如果某些字节具有特殊含义时，当给出的这些数据不在允许的范围之内时返回给上位机的状态值
4	0xXX	**0x05**	无此项	LSM+MSB	感应场处于关闭状态	上位机发送命令数据块，要执行 ISO/IEC 15693 命令，但感应场处于关闭状态时返回给上位机的状态值
4	0xXX	**0x06**	无此项	LSM+MSB	EEPROM 操作出错	上位机发送命令数据块，要向 EEPROM 中写入数据，但是操作失败时返回给上位机的状态值
4	0xXX	**0x0A**	无此项	LSM+MSB	指定的 Inventory-Scan-Time 溢出	上位机发送命令数据块，读写器执行 Inventory 时，当在用户指定的时间 Inventory-Scan-Time 溢出前还没有获得一张电子标签时返回给上位机

						的状态值
4	0xXX	**0x0B**	无此项	LSM+MSB	还没得到所有电子标签的 UID，但是指定的 Inventory-Scan-Time 溢出	上位机发送命令数据块，读写器执行 Inventory-Scan 时，当在用户指定的时间 Inventory-Scan-Time 溢出前还没得到所有的 UID 时返回给上位机的状态值
4	0xXX	**0x0C**	无此项	LSM+MSB	ISO error	上位机发送命令数据块，读写器执行相应命令的过程中出现了不符合正常 ISO/IEC 15693 协议规定的现象时返回给上位机的状态值
4	0xXX	**0x0E**	无此项	LSM+MSB	无电子标签可操作	上位机发送命令数据块，读写器在执行相应命令的过程中，感应场内没有电子标签可操作时返回给上位机的状态值
5	0xXX	**0x0F**	Error_code	LSM+MSB	操作出错	当电子标签返回错误代码时，错误代码将由 Error_code 返回给上位机。这种情况对应的状态值为 0F
4+Data[]部分的字节数	0xXX	**0x10**	……	LSM+MSB	后续还有响应数据块	当命令的存在多条响应数据块，且此响应不是最后一个响应数据块时返回给上位机的状态码
4	0xXX	**0x11**	无此项	LSM+MSB	天线异常进入保护状态	上位机发送操作标签的命令时，读写器处于保护状态，并且进入保护状态的原因是天线不存在或者天线品质差时，返回给上位机的命令码
4	0xXX	**0x12**	无此项	LSM+MSB	温度过高进入保护状态	上位机发送操作标签的命令时，读写器处于保护状态，并且进入保护状态的原因是温度过高时，返回给上位机的命令码

4	0xXX	**0x13**	无此项	LSM+MSB	电流过大进入保护状态	上位机发送命令数据块，读写器处于保护状态，并且进入保护状态的原因是电流过大时，返回给上位机的命令码。
4	0xXX	**0x14**	无此项	LSM+MSB	读写器出现严重错误	上位机发送命令数据块，读写器由于电流过大进入保护状态，并且不能够自动恢复到正常状态时，返回给上位机的命令码。
5	0xXX	**0x20**	0xA0	LSM+MSB	网络心跳包	读写通过网络主动上传的心跳包
4	0xXX	**0x21**	无此项	LSM+MSB	标签操作失败	读写器对 ISO18000-3 标签执行读写操作时，标签存在射频场内，但是执行失败时返回给上位机的状态码
4	0x76	**0x22**	无此项	LSM+MSB	销毁密码不能为 0	读写器对 ISO18000-3 标签执行销毁命令时，销毁密码不可以为 0，如果密码是 0，将返回此错误代码。
4	0xXX	**0x23**	无此项	LSM+MSB	访问密码不正确	读写器对 ISO18000-3 标签执行需要密码才能执行的操作，而命令中给出的密码是错误的密码时返回给上位机的状态码
5	0xXX	**0x2F**	Error_code	LSM+MSB	电子标签返回错误代码	ISO18000-3 标签返回错误代码时，错误代码由 Err_code 返回给上位机

- **注意：Status 为“0x00”的响应数据块的长度（Len）和响应数据（Data[]）都会因为命令的不同而有所区别，我们会在每条命令的详细介绍中给出具体的内容。**
- **注意：Status 为“0x0F”的响应数据块的长度是固定的，但内容因错误的不同而有所差异，具体的含义请参看“错误代码(error_code)的定义。**
- **注意：Status 为别的值时，响应数据块的内容和长度都是固定的，所以在后面每条命令的详细介绍中将不会对这些响应数据块进行说明了。**
- **注意：当读写器并且由于多个原因进入保护状态时，返回的状态码优先级为 0x13>0x12>0x11。**
- **注意：当读写器返回的状态码 0x14 时，可以发送检查保护状态命令来检查读写器状态，如果电流正常，将会恢复到正常状态。**

5. 错误代码(error_code)定义

当读写器对电子标签执行操作，而电子标签返回错误代码时，读写器返回给上位机的数据块的状态值(Status)是 0x0F（ISO15693 协议）或 0x2F(ISO18000-3 协议)，后面跟着一个字节的响应数据(Data[])，这个字节的含义是由 ISO18000-3 协议规定的，此处我们给出它们的具体含义。

5.1. ISO18000-3 标签错误代码

错误代码支持	错误代码	错误代码名称	错误描述
特定错误代码	0x00	其它错误	全部捕捉未被其它代码覆盖的错误
	0x03	存储器超限或不被支持的 PC 值	存储位置不存在或标签不支持的 PC 值
	0x04	存储器锁定	存储位置锁定或永久锁定，且不可写入
	0x0b	电源不足	标签电源不足，无法执行存储写入操作
非特定错误代码	0x0f	非特定错误	标签不支持特定错误代码

6. 操作命令的详细描述

HYB630 系列读写器支持命令众多，每个命令又有多种运行模式，以下对 HYB630 系列读写器所支持的这些命令进行详细的介绍。

6.1. 读写器自定义命令

HYB630 系列读写器一共有 31 条自定义命令，方便用户对读写器的操作。上位机在发送这些命令时，操作控制符（State）的高 4 位必须是“F”。

6.1.1. 获得读写器的信息—Get Reader Information

当上位机通过发送命令数据块让读写器执行该命令后，将获得读写器的信息，这其中包括读写器地址（Com_adr）、读写器软件版本（Version）、天线口数量（ant_num，低 5 位有效）、读写器类型代码、读写器协议支持信息和 InventoryScanTime 的信息。

读写器类型代码的值是 0x17，代表的产品是 HYB630。InventoryScanTime 的缺省值是 0x1e（对应的时间是 3s）。读写器协议支持信息的值是 0x00,0x0A，含义见下表：

bit	15	14	13	12	11	10	9	8
Function	—	—	—	—	—	—	—	—
bit	7	6	5	4	3	2	1	0
Function	—	—	—	—	—	—	ISO18000-3	—

Len	Com_adr	Cmd	State	Data[]	CRC-16	
0x05	0xXX	0x00	0xf0	—	LSB	MSB
Len	**Com_adr**	**Status**	**Data[]**		**CRC-16**	
0x0c	0xXX	0x00	Version(2bytes), ant_num, RFU, _Reader_type,_Tr_type(2bytes), _InventoryScanTime		LSB	MSB

6.1.2. 关闭感应场—Close RF

当上位机通过发送命令数据块让读写器执行该命令后，读写器的感应场将会被关闭。这时，如果上位机发送命令数据块让读写器执行 ISO/IEC 15693 和 ISO18000-3 命令，读写器将不会执行任何操作，而只是返回固定的响应数据块来告知感应场处于关闭状态。

Len	Com_adr	Cmd	State	Data[]	CRC-16	
0x05	0xXX	0x01	0xf0	—	LSB	MSB
Len	**Com_adr**	**Status**	**Data[]**		**CRC-16**	
0x04	0xXX	0x00	—		LSB	MSB

6.1.3. 打开感应场—Open RF

当上位机通过发送命令数据块让读写器执行该命令后，读写器的感应场将会被打开。只有在感应场处于打开状态时，ISO/IEC 15693 和 ISO18000-3 协议命令才能被执行。

读写器上电后，感应场处于打开状态。

Len	Com_adr	Cmd	State	Data[]	CRC-16	
0x05	0xXX	0x02	0xf0	—	LSB	MSB
Len	**Com_adr**	**Status**	**Data[]**		**CRC-16**	
0x04	0xXX	0x00	—		LSB	MSB

6.1.4. 写入读写器地址—Write Com_adr

当上位机通过发送命令数据块让读写器执行该命令后，读写器将会把读写器地址改为用户给定的值，并把这个值写入 EEPROM，以后将使用此项新的读写器地址。出厂时缺省值是 0x00。允许用户的修改范围是 0x00~0xfe。当用户写入的值是 0xff 时，读写器将会自动恢复成缺省值 0x00。

Len	Com_adr	Cmd	State	Data[]	CRC-16	
0x06	0xXX	0x03	0xf0	_Com_adr	LSB	MSB
Len	**Com_adr**	**Status**	**Data[]**		**CRC-16**	
0x04	0xXX	0x00	—		LSB	MSB

6.1.5. 写入询查命令最大响应时间—Write InventoryScanTime

当上位机通过发送命令数据块让读写器执行该命令后，读写器将会把询查命令最大响应时间改为用户给定的值（3*100ms~255*100ms），并把这个值写入 EEPROM，以后将使用此项新的询查命令最大响应时间。出厂时缺省值是 0x1e（对应的时间为 30*100ms）。用户修改范围是 0x03~0xff（对应时间是 3*100ms~255*100ms）。注意，实际的响应时间可能会比设定值大 0~75ms。当用户写入的值是 0x00~0x02 时，读写器将会自动恢复成缺省值 0x1e（对应的时间为 30*100ms）。

Len	Com_adr	Cmd	State	Data[]	CRC-16	
0x06	0xXX	0x04	0xf0	_InventoryScanTime	LSB	MSB
Len	**Com_adr**	**Status**	**Data[]**		**CRC-16**	
0x04	0xXX	0x00	—		LSB	MSB

6.1.6. 读取通用输入端口状态—Get General Input

用户可以通过发送这一命令数据块，来读取读写器上的 1 个通用输入端口的状态(TTL 电平，内部接 40kΩ上拉电阻至+3.3V)。

Len	Com_adr	Cmd	State	Data[]	CRC-16	
0x05	0xXX	0x06	0xf0	—	LSB	MSB
Len	**Com_adr**	**Status**	**Data[]**		**CRC-16**	
0x05	0xXX	0x00	_Input		LSB	MSB

响应数据块中包含的数据字节(_Input），给出了通用输入端口的状态(TTL 电平)。

	Bit7	Bit6	Bit5	Bit4	Bit3	Bit2	Bit1	Bit0

对应的通用输入端口	—	—	—	—	—	—	—	Input1

6.1.7. 设置继电器状态—Set Relay

用户可以通过发送这一命令数据块，来设置继电器处于释放或吸合状态。上电的默认状态是释放状态。

Len	Com_adr	Cmd	State	Data[]	CRC-16	
0x06	0xXX	0x07	0xf0	_Relay	LSB	MSB
Len	**Com_adr**	**Status**	**Data[]**		**CRC-16**	
0x04	0xXX	0x00	—		LSB	MSB

命令数据块中包含的数据字节(_Relay），是用来给用户配置继电器状态的。

	Bit7	Bit6	Bit5	Bit4	Bit3	Bit2	Bit1	Bit0
继电器状态	—	—	—	—	—	—	—	释放＝1 吸合＝0

6.1.8. 设置当前有效天线—Set Active ANT

用户可以通过发送这一命令数据块，来选择读写器的当前有效天线。上电的默认状态是选择天线 1 作为有效天线。读写器每次只能有 1 个天线处于有效状态。

Len	Com_adr	Cmd	State	Data[]	CRC-16	
0x06	0xXX	0x08	0xf0	_ANT_status	LSB	MSB
Len	**Com_adr**	**Status**	**Data[]**		**CRC-16**	
0x04	0xXX	0x00	—		LSB	MSB

命令数据块中包含的数据字节(_ANT_status），用来给用户选择有效天线。
_ANT_status 的数值表示当前有效天线口。比如 00H 表示天线 1、01H 表示天线 2…0FH 表示天线 16。

6.1.9. 获取读写器天线状态—Get ANT Status

用户可以通过发送这一命令数据块，来获取读写器当前的天线状态。

Len	Com_adr	Cmd	State	Data[]	CRC-16	
0x05	0xXX	0x09	0xf0	—	LSB	MSB
Len	**Com_adr**	**Status**	**Data[]**		**CRC-16**	
0x05	0xXX	0x00	_ANT_status		LSB	MSB

响应数据块中包含的数据字节(_ANT_status），表示当前有效天线口。比如 00H 表示天线 1、01H 表示天线 2…0FH 表示天线 16。

6.1.10. 获取当前接收噪音测量值—Get Noise Measurement Result

用户可以通过发送这一命令数据块，获取当前接收噪音测量值。

Len	Com_adr	Cmd	State	Data[]	CRC-16	
0x05	0xXX	0x12	0xf0	—	LSB	MSB
Len	**Com_adr**	**Status**	**Data[]**		**CRC-16**	
0x05	0xXX	0x00	_VNOISE		LSB	MSB

响应数据块中包含的数据字节(_VNOISE）为接收噪音的测量值。

6.1.11. 设置读写器解析模式—Set Parse Mode

用户可以通过发送这一命令数据块，来设置读写器的解析模式为 DPPM（深度优先）或 WPPM（宽度优先）。读写器将相应地改变解析模式，并把这个模式写入 EEPROM，以后将使用此项新的读写器解析模式。

出厂缺省值是 0xA0（即 100%调制、加速启动、波特率 19200、DPPM 宽度优先）。

Len	Com_adr	Cmd	State	Data[]	CRC-16	
0x06	0xXX	0x70	0xf0	_ParseMode	LSB	MSB
Len	**Com_adr**	**Status**	**Data[]**		**CRC-16**	
0x04	0xXX	0x00	—		LSB	MSB

命令数据块中包含的数据字节(_ParseMode），是用来给用户配置读写器解析模式的。

	Bit7	Bit6	Bit5	Bit4	Bit3	Bit2	Bit1	Bit0
读写器解析模式	100%调制固定为 1	—	设置询查加速功能 0：禁止加速 1：使能加速	—	波特率设置使能位： =1 设置有效 =0 设置无效	波特率设置： 19200=00; 38400=01; 57600=10; 115200=11;		深度优先=1 宽度优先=0

6.1.12. 获取当前读写器解析模式—Get Parse Mode

用户可以通过发送这一命令数据块，来获取当前读写器的解析模式。

Len	Com_adr	Cmd	State	Data[]	CRC-16	
0x05	0xXX	0x71	0xf0	—	LSB	MSB
Len	**Com_adr**	**Status**	**Data[]**		**CRC-16**	
0x05	0xXX	0x00	_ParseMode		LSB	MSB

响应数据块中包含的数据字节(_ParseMode），是读写器当前解析模式状态。

	Bit7	Bit6	Bit5	Bit4	Bit3	Bit2	Bit1	Bit0

读写器解析模式	100%调制 固定为 1	—	设置询查加速功能 0：禁止加速 1：使能加速	—	—	波特率设置： 19200=00; 38400=01; 57600=10; 115200=11;	深度优先=1 宽度优先=0

6.1.13. 设置读写器射频功率数—Set Pwr

用户可以通过发送这一命令数据块，按功率数设置读写器射频输出功率。
这条命令修改后的结果掉电不丢失，一直维持到下次修改时。

Len	Com_adr	Cmd	State	Data[]	CRC-16	
0x06	0xXX	0x20	0xf0	_Pwr	LSB	MSB
Len	**Com_adr**	**Status**	**Data[]**		**CRC-16**	
0x04	0xXX	0x00	—		LSB	MSB

命令数据块中包含的数据字节(_Pwr）用于按功率数设置射频输出功率，单位是 0.5W，范围 0 到 9，取 0 值对应 0.5W，取 9 对应 5W。

6.1.14. 获取读写器射频功率—Get Pwr

用户可以通过发送这一命令数据块，获取读写器射频输出功率数和功率级数值。

Len	Com_adr	Cmd	State	Data[]	CRC-16	
0x05	0xXX	0x22	0xf0	—	LSB	MSB
Len	**Com_adr**	**Status**	**Data[]**		**CRC-16**	
0x06	0xXX	0x00	_Pwr，_RFU		LSB	MSB

响应数据块中包含的数据字节(_Pwr），是读写器当前射频功率数。

	Bit7	Bit6	Bit5	Bit4	Bit3	Bit2	Bit1	Bit0
射频功率数	已标定=0 未标定=1	—	射频功率数值（0 到 9）					

6.1.15. 设置选项字节—Set option byte

用户可以通过发送这一命令数据块，来设置读写器的选项字节。读写器的选项字节决定着读写器一部分的功能和行为。

Len	Com_adr	Cmd	State	Data[]	CRC-16	
0x09	0xXX	0x27	0xf0	Option_byte	LSB	MSB
Len	**Com_adr**	**Status**	**Data[]**		**CRC-16**	
0x04	0xXX	0x00	——		LSB	MSB

Option_byte 是一个包含读写器的策略和功能配置的选项字节。四字节长度，高字节在前。具体功能如下：

	名称	说明	缺省值
Bit0	去重	打开此功能后，读写器在 inventory 命令因 inventoryScanTime 超时而退出时，判断标签 UID 是否有重复，如果有将返回询查结束状态 0x0E，否则返回询查未完状态 0x0B。 关闭此功能后，读写器在上述情况返回 0x0B。	1 (打开)
Bit1	开机 RF 状态	开机后 RF 的状态。0 表示关闭，1 表示打开。在接收到第一条命令时自动的打开 RF。	1（打开）
Bit2	全程过滤	打开此功能后，在一条询查命令之后的询查命令不会再次上传已经在之前的询查中上传过的 UID。在集合询查中表现为一个 UID 在一个集合询查命令中只会被上传一次。 关闭此功能后，询查命令会上传读取到的全部 UID，无论在之前的询查命令中是否被上传过。在集合询查中表现为每个天线都上传该天线读到的全部 UID。	1（打开）
Bit3	补漏	打开此功能后，在询查结束后再补充询查一次，没有得到标签才退出。 关闭此功能后，询查结束后补充一轮，无论是否有标签都退出询查。	1（打开）
Bit3-Bit31	保留		1

6.1.16. 读取选项字节—Get option byte

用户可以通过发送这一命令数据块，来获得读写器的选项字节。

Len	Com_adr	Cmd	State	Data[]	CRC-16	
0x05	0xXX	0x28	0xf0	——	LSB	MSB
Len	**Com_adr**	**Status**	**Data[]**		**CRC-16**	
0x08	0xXX	0x00	Option_byte		LSB	MSB

参数解析：

Option_byte:四个字节的选项字节。

6.1.17. 获取读写器运行状态—Get Run State

用户可以通过发送这一命令数据块，来获取读写器当前的电流电压信息，以监测读写器的运行状态。

Len	Com_adr	Cmd	State	Data[]	CRC-16	
0x05	0xXX	0X40	0xf0	——	LSB	MSB

Len	Com_adr	Status	Data[]	CRC-16	
0x09	0xXX	0x00	PAvolt, PAcur, pwrForward, pwrReverse，Temperature	LSB	MSB

参数解析：

PAvolt：表示 PA 电压。PA 电压等于 PAvolt * 19.8/ 256。

PAcur：表示 PA 电流。PA 电流等于 PAcur * 6.6 / 460.8。

pwrForward：正向功率。

pwrReverse：反向功率。

Temperature：设备温度。单位℃。

6.1.18. 获取天线品质系数—Get Antenna Quality

用户可以通过发送这一命令数据块，来获取当前天线的品质系数。品质系数最优为 1.0，数值越大，表示天线品质越差。

Len	Com_adr	Cmd	State	Data[]	CRC-16	
0x05	0xXX	0X41	0xf0	——	LSB	MSB
Len	**Com_adr**	**Status**	**Data[]**		**CRC-16**	
0x06	0xXX	0x00	AntQ_int, AntQ _dec		LSB	MSB

参数解析：

AntQ _int：表示品质系数的整数部分。

AntQ _dec：表示品质系数的小数部分，小数部分以 BCD 码表示，如 0x26 表示 0.26。

6.1.19. 设置安全保护阈值—Set Protection Threshold

用户可以通过发送这一命令数据块，来设置读写器进入安全保护状态的阈值。

读写器在进入保护状态时，会将射频功率调整到 1W 以保护读写器。

保护阈值的内容将会直接写入内部 EEPROM 内，所以，除非再次使用这条命令来修改配置的内容，否则读写器将一直保持这样的设置运行。

Len	Com_adr	Cmd	State	Data[]	CRC-16	
0x08	0xXX	0X42	0xf0	Temp, AntQ_int, AntQ_dec	LSB	MSB
Len	**Com_adr**	**Status**	**Data[]**		**CRC-16**	
0x04	0xXX	0x00	——		LSB	MSB

参数解析：

Temp：表示温度值阈值。取值为 30-120。缺省值为 80℃。

AntQ_int：表示品质系数的整数部分，整数部分取值为 3-255。缺省值为 8。

AntQ _dec：表示品质系数的小数部分，小数部分取值为 0-9。缺省值为 0。

6.1.20. 读取安全保护阈值—Get Protection Threshold

用户可以通过发送这一命令数据块，来读取读写器进入安全保护状态的阈值。

Len	Com_adr	Cmd	State	Data[]	CRC-16	
0x05	0xXX	0X43	0xf0	——	LSB	MSB
Len	**Com_adr**	**Status**	**Data[]**		**CRC-16**	
0x07	0xXX	0x00	Temperature,SWR_int,SWR_dec		LSB	MSB

参数解析：

Temperature：表示温度值阈值。

SWR_int：表示品质系数的整数部分。

SWR_dec：表示品质系数的小数部分，小数部分取值为 0-9。

6.1.21. 读取序列号—Get Serial Number

用户可以通过发送这一命令数据块，来获得读写器的序列号。

Len	Com_adr	Cmd	State	Data[]	CRC-16	
0x05	0xXX	0x48	0xf0	——	LSB	MSB
Len	**Com_adr**	**Status**	**Data[]**		**CRC-16**	
0x04	0xXX	0x00	Serial_number		LSB	MSB

参数解析：

Serial_number:四个字节的序列号。序列号为 0xFFFFFFFF 表示空序列号。

6.1.22. 读写器重启—Reader reset

用户可以通过发送这一命令数据块，来命令读写器重启。

Len	Com_adr	Cmd	State	Data[]	CRC-16	
0x05	0xXX	0x4B	0xf0	——	LSB	MSB
Len	**Com_adr**	**Status**	**Data[]**		**CRC-16**	
0x04	0xXX	0x00	——		LSB	MSB

读写器在响应数据发送结束之后会立即重启。重启后，天线选通在天线 1 上。

6.1.23. 设置/读取自动关闭 RF—Auto turn off RF setting

读写器在完成一条命令后，一段时间内没有操作可以自动的关闭射频场，用户可以通过发送这一命令数据块来设置此功能是否启用和等待的时间长度。

Len	Com_adr	Cmd	State	Data[]		CRC-16	
0x07	0xXX	0x4D	0xf0	RW	Time	LSB	MSB
Len	**Com_adr**	**Status**	**Data[]**			**CRC-16**	
0x05	0xXX	0x00	Time			LSB	MSB

RW：Bit7 表示为 1 表示设置参数，为 0 表示读取参数。

Time：bit7 为 1 表示此功能打开，为 0 表示此功能关闭。Bit[0-6]表示命令执行结束后等待关闭射频场的延时等待时间。单位为秒，参数为 0 表示命令执行结束后立即关闭射频场。

6.1.24. 停止询查—Stop inventory

读写器在执行询查标签的命令时，可以发送此命令停止询查标签过程。

读写器在接收到此命令后，会在 100ms 内停止询查标签，并返回状态码为 0x0E 的结束帧。

注意：此命令只在串口上有效。也只能停止由来自串口的询查命令。

Len	Com_adr	Cmd	State	Data[]	CRC-16	
0x05	0xXX	0x4E	0xf0	—	LSB	MSB

此命令没有响应帧，接收到询查命令的结束帧，表示命令执行成功。

6.1.25. 设置读写器网络参数— Set network parameters

用户可以通过发送这一命令数据块，来设置读写器的网络参数。该命令不会影响当前的网络通讯，要使其保存和生效，需要配置好所有参数后发送“网络参数保存并重启”命令。

Len	Com_adr	Cmd	State	Data[]	CRC-16	
0x06+n	0xXX	0x60	0xf0	_ItemNo, _ItemData(n bytes)	LSB	MSB
Len	**Com_adr**	**Status**	**Data[]**		**CRC-16**	
0x04	0xXX	0x00	—		LSB	MSB

命令数据块中包含的_ItemNo，用来指定要设置的网络参数的序号。_ItemData 是该网络参数新的数值。详见下表。

序号	网络参数	描述	长度
0	IPAddr[4]	本地 IP	4 字节
1	MaskAddr[4]	子网掩码	4 字节
2	GWAddr[4]	网关	4 字节
3	DNSAddr[4]	保留，读为 0	4 字节
4	MacAddr[6]	MAC 地址（只读）	6 字节
5	ConnectionMode	连接模式(0=TCP server, 1= TCP client, 2= UDP)	1 字节
6	RemoteAddr①	远程 IP(作为 TCP client 时连接到的远程 IP)	文本格式：最长 15 字节
7	RemotePort	远程端口(作为 TCP client 时连接到的远程 IP)	2 字节(高字节在前)
8	LocalPort	本地端口(作为 TCP server 或者 UDP 时使用的本地端口)	2 字节(高字节在前)
9	TCPTimeOut	作为 TCP service 时，连续未接收到客户端的数据依然保持连接的时间。单位：秒	2 字节(高字节在前)

10	TCPReconnectMode	作为客户端时，主动连接到远程服务器的方式。0=立即连接，1=有数据才连接。	1 字节
11	Connection speed	0=Auto,1=100Mbps, 2=10Mbps	1 字节
12	DHCP	0=关闭 DHCP， 1 表示开启 DHCP	1 字节
13	RemoteAddr①	远程 IP(作为 TCP client 时连接到远服务器的 IP 地址)	4 字节

①:6 号参数和 13 号参数含义完全相同，只是参数的数据格式不同，6 号的参数格式是文本格式，13 号的参数格式是 16 进制格式。

6.1.26. 读取读写器网络参数—Get network parameters

用户可以通过发送这一命令数据块，来获取当前读写器的网络参数。

Len	Com_adr	Cmd	State	Data[]	CRC-16	
0x06	0xXX	0x61	0xf0	_ItemNo	LSB	MSB
Len	**Com_adr**	**Status**	**Data[]**		**CRC-16**	
0x04+n	0xXX	0x00	_ItemData(n bytes)		LSB	MSB

命令数据块中包含的_ItemNo，用来指定要读取的网络参数的序号。响应数据块中包含的_ItemData 是该网络参数的数值返回。

6.1.27. 网络参数保存并重启—Network parameters are saved and restarted

用户可以通过发送这一命令数据块，将当前配置好的网络参数保存到 EEPROM，然后重启设备并用新的参数重新初始化网络。

Len	Com_adr	Cmd	State	Data[]	CRC-16	
0x05	0xXX	0x62	0xf0	—	LSB	MSB
Len	**Com_adr**	**Status**	**Data[]**		**CRC-16**	
0x04	0xXX	0x00	—		LSB	MSB

6.1.28. 恢复网络参数到出厂设置并重启—Network parameters to default and restart

用户可以通过发送这一命令数据块，将网络参数恢复到出厂设置，然后重启设备并用新的参数重新初始化网络。

Len	Com_adr	Cmd	State	Data[]	CRC-16	
0x05	0xXX	0x63	0xf0	—	LSB	MSB
Len	**Com_adr**	**Status**	**Data[]**		**CRC-16**	
0x04	0xXX	0x00	—		LSB	MSB

6.1.29. 读取网络状态—Read network status

用户可以通过发送这一命令数据块，将读取当前网络的连接状态。

Len	Com_adr	Cmd	State	Data[]	CRC-16	
0x05	0xXX	0x64	0xf0	—	LSB	MSB
Len	**Com_adr**	**Status**	**Data[]**		**CRC-16**	
0x17	0xXX	0x00	Data		LSB	MSB

Data 字段的详细说明：

描述	说明	长度
IPAddr[4]	本地 IP	4 字节
MaskAddr[4]	子网掩码	4 字节
GWAddr[4]	网关 IP	4 字节
ClientAddr[4]	客户端 IP	4 字节
ClientPort	客户端端口	2 字节
ConnectStatus	连接状态	1 字节

当读写器作为 TCP Client 时，客户端 IP 为本机 IP，客户端端口表示连接到远程服务器使用的本地端口。

当读写器作为 TCP service 或使用 UDP 时，客户端 IP 为连接到读写器的远程客户端的 IP， 客户端端口表示远程客户端使用的端口。

连接状态：0-未插入网线
1-未连接
2-已连接

6.1.30. 设置网络心跳包和 TCP keepalive - Setting network heartbeat and TCP keepalive

用户可以通过发送这一命令数据块，来设置读写的网络心跳包的时间间隔和 TCP keepalive 的时间间隔。

网络心跳包，读写器检测到网络超过一段时间没有数据传输，就会向连接的对端发送一段数据。读写器通过检查是否收到对端的 ACK，来判断当前网络连接是否正常。对端的应用层能够收到心跳包的数据，所以用户可以也使用心跳包判断读写器的网络连接是否正常。

Keepalive 是 TCP 协议内嵌的一种机制。读写器检测到网络超过一段时间没有数据传输，就会向对端发送 keep-alive 包。读写器通过检查是否收到对端的 ACK，来判断当前网络连接是否正常。Keepalive 协议规定，要想让 keepalive 机制生效，必须让读写器向对端发送过数据，所以建议在连接上读写器的网络之后立即向读写器发送一条命令，以确保 keepalive 机制生效。Keepalive 是 TCP 协议的一种机制，所以应用层无法察觉到 keepalive 的存在。

断开连接后，按照断线重连的设置的决定下次连接的时机。

Len	Com_adr	Cmd	State	Data[]	CRC-16	
0x07	0xXX	0x65	0xf0	Heartbeat_Time, keepalive_time	LSB	MSB
Len	**Com_adr**	**Status**	**Data[]**		**CRC-16**	
0x04	0xXX	0x00	-		LSB	MSB

Heartbeat_time:1 字节。高字节在前。心跳包上传的时间间隔。单位为秒，设置为 0 关闭心跳包功能。默认关闭。

keepalive_time:1 字节。高字节在前。Keepalive 的时间间隔。单位为秒，设置为 0 表示关闭 keeplive。默认值为 10 秒。

心跳包格式：

Len	Com_adr	Status	Data[]	CRC-16	
0x05	0xXX	0x20	0xA0	LSB	MSB

6.1.31. 读取网络心跳包和 TCP keepalive

用户可以通过发送这一命令数据块，来读取读写的网络心跳包的时间间隔和 TCP keepalive 的时间间隔的设置。

Len	Com_adr	Cmd	State	Data[]	CRC-16	
0x05	0xXX	0x66	0xf0	–	LSB	MSB
Len	**Com_adr**	**Status**	**Data[]**		**CRC-16**	
0x06	0xXX	0x00	Heartbeat_Time, keepalive_time		LSB	MSB

6.2. ISO18000-3 命令协议

HYB630 系列读写器支持 ISO18000-3 协议标签，以下命令为 ISO18000-3 协议的操作命令。

HYB630 读写器询查 ISO18000-3 标签速度快，以至于串口不能实时上传数据，影响读卡体验。建议在盘点 ISO18000-3 标签时，将读写器的串口波特率修改为 57600 以上，否则严重影响盘点速度。

6.2.1. 询查命令

命令：

Len	Com_adr	Cmd	State	Data[]			CRC-16	
0x08	0xXX	0x71	0x20	Flag	Session	QValue	LSB	MSB
				0xXX	0xXX	0xXX		

Flag: 一个字节。bit0 置 1 表示发送 select 命令，唤醒全部标签，0 表示不发送 Select 命令，只盘点新来的标签。Bit1 表示高精度盘点，此选项会提高读取标签的准确率，但是会降低读卡速度。Bit[2-7]保留，请保持为 0。

Session: 一个字节。使用的 Session 值。

0x00 表示 S0;

0x02 表示 S2。其他值返回参数错误。

QValue: 一个字节。初始 Q 值。取值范围 0-15。其他值返回参数错误。

应答：

Len	Com_adr	Status	Data[]	CRC-16	
0xXX	0xXX	0x00	EPC,RSSI	LSB	MSB
0xXX	0xXX	0x00	EPC,RSSI	LSB	MSB
……					
0x04	0xXX	0x0E		LSB	MSB

EPC：变长。返回的标签 EPC 号。

RSSI：一个字节。标签的信号强度。

6.2.2. 选择命令

本命令可从多个指定天线口发送选择命令。

命令：

Len	Adr	Cmd	State	Data[]	CRC-16	
0xXX	0xXX	0x72	0x20	——	LSB	MSB

Data 参数如下：

Data[]							
Ant	SelTarget	SelAction	MaskMem	MaskAdr	MaskLen	MaskData	Truncate
4byte	0xXX	0xXX	0xXX	2Bytes	0xXX	变长	0xXX

参数解析：

Ant：4 个字节，高字节在前。表示要发送选择命令的一个或多个天线号，每个 Bit 代表一个天线号。例如 0x0000010F,表示此次询查的天线为 1、2、3、4、9。如果参数为 0x00000000，则表示只在当前天线上发送选择命令。

SelTarget：1 个字节，选择命令中的 Target 参数。
0x00：Target 使用 S0；
0x01：Target 使用 S1；
0x02：Target 使用 S2；
0x03：Target 使用 S3。
0x04：Target 使用 SL。
0x05~0x07：RFU 保留值，目前不能使用。
其它值保留。若命令中出现了其它值，将返回参数出错的消息。

SelAction：1 个字节，选择命令中的 Action 参数。参数范围 0~7，对应的功能如下：

Action	选择条件匹配	选择条件不匹配
0x00	置位 SL 标志或 Target 参数指定的 Session 强制回 A	取消 SL 标志或 Target 参数指定的 Session 强制回 B
0x01	置位 SL 标志或 Target 参数指定的 Session 强制回 A	不做任何操作
0x02	不做任何操作	取消 SL 标志或 Target 参数指定的 Session 强制回 B
0x03	SL 标志翻转或 Target 参数指定的 Session 强制 AB 翻转（即 A 变 B，B 变 A）	不做任何操作
0x04	取消 SL 标志或 Target 参数指定的 Session 强制回 B	置位 SL 标志或 Target 参数指定的 Session 强制回 A
0x05	取消 SL 标志或 Target 参数指定的 Session 强制回 B	不做任何操作
0x06	不做任何操作	置位 SL 标志或 Target 参数指定的 Session 强制回 A
0x07	不做任何操作	SL 标志翻转或 Target 参数指定的 Session 强制 AB 翻转（即 A 变 B，B 变 A）

其它值保留。若命令中出现了其它值，将返回参数出错的消息。

MaskMem：一个字节，选择条件的掩码区。0x01：EPC 存储区；0x02：TID 存储区；0x03：用户存储区。其他值保留。若命令中出现了其它值，将返回参数出错的消息。

MaskAdr：两个字节，高字节在前。选择条件的掩码起始位地址（单位：Bits）。

MaskLen：一个字节，选择条件的掩码位长度（单位：Bits）。

MaskData：选择条件的掩码数据。MaskData 数据字节长度是(MaskLen+7)/8。即如果 MaskLen 不是 8 的整数倍，则 MaskData 数据字节长度为[MaskLen/8]取整再加 1。不够的在低位补 0。

注：如果 MaskLen 长度为 0，MaskData 参数不存在，此时表示匹配所有标签。

Truncate：1 个字节，截短标志。建议禁止截短功能。

0 - 禁止截短功能。

1 - 使能截短功能。

应答：

Len	Adr	Status	Data[]	CRC-16	
0x04	0xXX	0xXX	——	LSB	MSB

6.2.3. 读数据

这个命令读取标签的保留区、EPC 存储区、TID 存储区或用户存储区中的数据。从指定的地址开始读，以字为单位。1 字为 2 字节。

命令：

Len	Adr	Cmd	State	Data[]	CRC-16	
0xXX	0xXX	0x73	0x20	——	LSB	MSB

Data 参数如下：

Data[]									
ENum	EPC	Mem	WordPtr	Num	Pwd	MaskMem	MaskAdr	MaskLen	MaskData
0xXX	变长	0xXX	2Bytes	0xXX	4Byte	0xXX	2Bytes	0xXX	变长

参数解析：

ENum：在(0x00~0x0f)范围内表示 EPC 号长度，以字为单位。EPC 的长度在 15 个字以内。此时无 MaskMem、MaskAdr 、MaskLen、MaskData 参数项。ENum 为 0xff 时有 MaskMem、MaskAdr 、MaskLen、MaskData 参数项，无 EPC 参数项。如果为其它值将返回参数错误信息。

EPC：要读取数据的标签的 EPC 号。长度根据所给的 EPC 号决定，EPC 号以字为单位，且必须是整数长度。高字在前，每个字的高字节在前。这里要求给出的是完整的 EPC 号。

Mem：一个字节。选择要读取的存储区。0x00：保留区；0x01：EPC 存储区；0x02：TID 存储区；0x03：用户存储区。其他值保留。若命令中出现了其它值，将返回参数出错的消息。

WordPtr：两个字节。指定要读取的字起始地址。0x00 表示从第一个字(第一个 16 位存储区)开始读，0x01 表示从第 2 个字开始读，依次类推。

Num：一个字节。要读取的字的个数。不能设置为 0x00，否则将返回参数错误信息。Num 不能超过 120，即最多读取 120 个字。若 Num 设置为 0 或者超过了 120，将返回参数出错的消息。

Pwd：四个字节，这四个字节是访问密码。32 位的访问密码的最高位在 Pwd 的第一字节的最高位，访问密码最低位在 Pwd 第四字节的最低位，Pwd 的前两个字节放置访问密码的高字。只有当读保留区，并且相应存储区设置为密码锁、且标签的访问密码为非 0 的时候，才需要使用正确的访问密码。在其他情况下，Pwd 为零或正确的访问密码。

MaskMem：一个字节，掩码区。0x01：EPC 存储区；0x02：TID 存储区；0x03：用户存储区。其他值保留。若命令中出现了其它值，将返回参数出错的消息。

MaskAdr：两个字节，掩码的起始位地址（单位：Bits）。

MaskLen：一个字节，掩码的位长度（单位：Bits）。

MaskData：掩码数据。MaskData 数据字节长度是 MaskLen/8。如果 MaskLen 不是 8 的整数倍，则 MaskData 数据字节长度为[MaskLen/8]取整再加 1。不够的在低位补 0。

注：当 MaskMem、MaskAdr 、MaskLen、MaskData 为空时表示以完整的 EPC 号掩膜。

应答：

Len	Adr	Status	Data[]	CRC-16	
0xXX	0xXX	0x00	Word1，Word2,…	LSB	MSB

参数解析：

Word1, Word2...： 以字为单位。每个字都是 2 个字节，高字节在前。Word1 是从起始地址读到的字，Word2 是起始地址后一个字地址上读到的字，以此类推。

6.2.4. 写数据

这个命令可以一次性往保留区、TID 存储区或用户存储区中写入若干个字。

命令：

Len	Adr	Cmd	State	Data[]	CRC-16	
0xXX	0xXX	0x74	0x20	——	LSB	MSB

Data 参数如下：

Data[]					
WNum	ENum	EPC	Mem	WordPtr	Wdt
0xXX	0xXX	变长	0xXX	2Bytes	变长
Pwd	MaskMem	MaskAdr	MaskLen	MaskData	
4Byte	0xXX	2Bytes	0xXX	变长	

参数解析：

WNum：待写入的字个数，一个字为 2 个字节。这里字的个数必须和实际待写入的数据个数相等。WNum 必须大于 0，最大为 32。若上位机给出的 WNum 为 0 或者 WNum 和实际字个数不相等，将返回参数错误的消息。

ENum：在(0x00~0x0f)范围内表示 EPC 号长度，以字为单位。EPC 的长度在 15 个字以内。此时无 MaskMem、MaskAdr 、MaskLen、MaskData 参数项。ENum 为 0xff 时有 MaskMem、MaskAdr 、MaskLen、MaskData 参数项，无 EPC 参数项。如果为其它值将返回参数错误信息。

EPC：要写入数据的标签的 EPC 号。长度由所给的 EPC 号决定，EPC 号以字为单位。高字在前，每个字的高字节在前。这里要求给出的是完整的 EPC 号。

Mem：一个字节，选择要写入的存储区。0x00：保留区；0x01：EPC 存储区；0x02：TID 存储区；0x03：用户存储区。其他值保留。若命令中出现了其它值，将返回参数出错的消息。

WordPtr：两个字节，指定要写入数据的起始地址。

Wdt：待写入的字，字的个数必须与 WNum 指定的一致。这是要写入到存储区的数据。每个字的高字节在前。Data[]中前面的字写在标签的低地址中，后面的字写在标签的高地址中。比如，WordPtr 等于 0x02，则 Data[]中第一个字(从左边起)写在 Mem 指定的存储区的地址 0x02 中，第二个字写在 0x03 中，依次类推。

Pwd：4 个字节的访问密码。32 位的访问密码的最高位在 Pwd 的第一字节(从左往右)的最高位，访问密码最低位在 Pwd 第四字节的最低位，Pwd 的前两个字节放置访问密码的高字。在写操作时，应给出正确的访问密码，当相应存储区未设置成密码锁时 Pwd 可以为零。

MaskMem：一个字节，掩码区。0x01：EPC 存储区；0x02：TID 存储区；0x03：用户存储区。其他值保留。若命令中出现了其它值，将返回参数出错的消息。

MaskAdr：两个字节，掩码的起始位地址（单位：Bits）。

MaskLen：一个字节，掩码的位长度（单位：Bits）。

MaskData：掩码数据。MaskData 数据字节长度是 MaskLen/8。如果 MaskLen 不是 8 的整数倍，则 MaskData 数据字节长度为[MaskLen/8]取整再加 1。不够的在低位补 0。

注：当 MaskMem、MaskAdr 、MaskLen、MaskData 为空时表示以完整的 EPC 号掩膜。

应答：

Len	Adr	Status	Data[]	CRC-16	
0x04	0xXX	0x00	——	LSB	MSB

6.2.5. 写 EPC 号

这个命令向电子标签写入 EPC 号。写入的时候，天线有效范围内只能有一张电子标签。如果存在多张标签，将随机写入一张标签。

命令：

Len	Adr	Cmd	State	Data[]			CRC-16	
				ENum	Pwd	WEPC		
0xXX	0xXX	0x75	0x20	0xXX	4Byte	变长	LSB	MSB

参数解析：

ENum：1 个字节。要写入的 EPC 的长度，以字为单位。可以为 0，不能超过 29，否则返回参数错误信息。

Pwd：4 个字节的访问密码。32 位的访问密码的最高位在 Pwd 的第一字节(从左往右)的最高位，访问密码最低位在 Pwd 第四字节的最低位，Pwd 的前两个字节放置访问密码的高字。在本命令中，当 EPC 区设置为密码锁、且标签访问密码为非 0 的时候，才需要使用访问密码。在其他情况下，Pwd 为零或正确的访问密码。

WEPC：要写入的 EPC 号，长度必须和 ENum 说明的一样。WEPC 最小 0 个字，最多 29 个字，否则返回参数错误信息。

应答：

Len	Adr	Status	Data[]	CRC-16	
0x04	0xXX	0x00	——	LSB	MSB

6.2.6. 销毁标签

这个命令用来销毁标签。标签销毁后，永远不会再处理读写器的命令。

命令：

Len	Adr	Cmd	State	Data[]	CRC-16	
0xXX	0xXX	0x76	0x20	——	LSB	MSB

Data 参数如下：

Data[]						
ENum	EPC	Killpwd	MaskMem	MaskAdr	MaskLen	MaskData
0xXX	变长	4Byte	0xXX	2Bytes	0xXX	变长

参数解析：

ENum：在(0x00~0x0f)范围内表示 EPC 号长度，以字为单位。EPC 的长度在 15 个字以内。此时无 MaskMem、MaskAdr 、MaskLen、MaskData 参数项。ENum 为 0xff 时有 MaskMem、MaskAdr 、MaskLen、MaskData 参数项，无 EPC 参数项。如果为其它值将返回参数错误信息。

EPC：要写入数据的标签的 EPC 号。长度根据所给的 EPC 号决定，EPC 号以字为单位，且必须是整数个长度。高字在前，每个字的高字节在前。这里要求给出的是完整的 EPC 号。

Killpwd：4 个字节的销毁密码。32 位的销毁密码的最高位在 Killpwd 的第一字节(从左往右)的最高位，销毁密码最低位在 Killpwd 第四字节的最低位，Killpwd 的前两个字节放置销毁密码的高字。要销毁标签，则销毁密码必须为非 0，因为密码为 0 的标签是无法销毁的。如果命令中的销毁密码为 0，则返回参数错误的应答。

MaskMem：一个字节，掩码区。0x01：EPC 存储区；0x02：TID 存储区；0x03：用户存储区。其他值保留。若命令中出现了其它值，将返回参数出错的消息。

MaskAdr：两个字节，掩码的起始位地址（单位：Bits）。

MaskLen：一个字节，掩码的位长度（单位：Bits）。

MaskData：掩码数据。MaskData 数据字节长度是 MaskLen/8。如果 MaskLen 不是 8 的整数倍，则 MaskData 数据字节长度为[MaskLen/8]取整再加 1。不够的在低位补 0。

注：当 MaskMem、MaskAdr 、MaskLen、MaskData 为空时表示以完整的 EPC 号掩膜。

应答：

Len	Adr	Status	Data[]	CRC-16	
0x04	0xXX	0x00	——	LSB	MSB

6.2.7. 设定存储区读写保护状态

这个命令可以设定保留区为无保护下的可读可写、永远可读可写、带密码可读可写、永远不可读不可写；可以分别设定 EPC 存储区、用户存储区为无保护下的可写、永远可写、带密码可写、永远不可写；TID 存储区是只读的，永远都不可写。EPC 存储区、TID 存储区和用户存储区是永远可读的。

标签的保留区一旦设置为永远可读写或永远不可读写，则以后不能再更改其读写保护设定。标签的 EPC 存储区、TID 存储区或用户存储区若是设置为永远可写或永远不可写，则以后不能再更改其写保护设定。如果强行发命令欲改变以上几种状态，则电子标签将返回错误代码。

在把某个存储区设置为带密码可读写、带密码可写或把带密码锁状态设置为其它非密码锁状态时，必须给出访问密码，所以，在进行此操作前，必须确保电子标签已设置了访问密码。

命令：

Len	Adr	Cmd	State	Data[]	CRC-16	
0xXX	0xXX	0x77	0x20	——	LSB	MSB

Data 参数如下：

Data[]								
ENum	EPC	Select	SetProtect	Pwd	MaskMem	MaskAdr	MaskLen	MaskData
0xXX	变长	0xXX	0xXX	4Byte	0xXX	2Bytes	0xXX	变长

参数说明：

ENum：在(0x00~0x0f)范围内表示 EPC 号长度，以字为单位。EPC 的长度在 15 个字以内。此时无 MaskMem、MaskAdr 、MaskLen、MaskData 参数项。ENum 为 0xff 时有 MaskMem、MaskAdr 、MaskLen、MaskData 参数项，无 EPC 参数项。如果为其它值将返回参数错误信息。

EPC：要写入数据的标签的 EPC 号。长度由所给的 EPC 号决定，EPC 号以字为单位，且必须是整数个长度。高字在前，每个字的高字节在前。这里要求给出的是完整的 EPC 号。

Select：一个字节。定义如下：

Select 为 0x00 时，控制 Kill 密码读写保护设定。

Select 为 0x01 时，控制访问密码读写保护设定。

Select 为 0x02 时，控制 EPC 存储区读写保护设定。

Select 为 0x03 时，控制 TID 存储区读写保护设定。

Select 为 0x04 时，控制用户存储区读写保护设定。

其它值保留，若读写器接收到了其他值，将返回参数出错的消息，并且不执行命令。

SetProtect：SetProtect 的值由 Select 的值而确定。

当 Select 为 0x00 或 0x01，即当设置 Kill 密码区或访问密码区的时候，SetProtect 的值代表的意义如下：

0x00：设置为无保护下的可读可写

0x01：设置为永远可读可写

0x02：设置为带密码可读可写

0x03：设置为永远不可读不可写

当 Select 为 0x02、0x03、0x04 的时候，即当设置 EPC 区、TID 区及用户区的时候，SetProtect 的值代表的意义如下：

0x00：设置为无保护下的可写

0x01：设置为永远可写

0x02：设置为带密码可写

0x03：设置为永远不可写

当 Select 与 SetProtect 出现了其他值的时候，将返回参数出错的消息，并且不执行命令。

Pwd：4 个字节的访问密码。32 位的访问密码的最高位在 Pwd 的第一字节(从左往右)的最高位，访问密码最低位在 Pwd 第四字节的最低位，Pwd 的前两个字节放置访问密码的高字。必须给出正确的访问密码。

MaskMem：一个字节，掩码区。0x01：EPC 存储区；0x02：TID 存储区；0x03：用户存储区。其他值保留。若命令中出现了其它值，将返回参数出错的消息。

MaskAdr：两个字节，掩码的起始位地址（单位：Bits）。

MaskLen：一个字节，掩码的位长度（单位：Bits）。

MaskData：掩码数据。MaskData 数据字节长度是 MaskLen/8。如果 MaskLen 不是 8 的整数倍，则 MaskData 数据字节长度为[MaskLen/8]取整再加 1。不够的在低位补 0。

注：当 MaskMem、MaskAdr 、MaskLen、MaskData 为空时表示以完整的 EPC 号掩膜。

应答：

Len	Adr	Status	Data[]	CRC-16	
0x04	0xXX	0x00	——	LSB	MSB

网络配置说明

6.3. 网络参数设置

HYB630 系列读写器的网络参数支持多种设置方式，以方便客户的灵活使用。

1.命令设置方式

通过 RS232 接口或者网络接口，发送上文所述的设置网络参数的命令，可以配置读写器的所有参数。

2.网页设置方式

在计算机的网页浏览器的地址栏输入读写器的 IP 地址，就可以进入读写器的网页配置页面。

6.4. 搜索设备

在与读写器以网络建立连接之前，必须要知道读写器的 IP 地址，否则无法建立连接和设置网络参数。所以我们提供了一种可以搜索当前网络内读写器 IP 地址的方法。

65535 端口是读写器指定的 UDP 广播端口，写器在此端口上接收到数据如果有效，将把响应数据以 UDP 广播的方式发送出去。由于是基于 UDP 广播的通信，所以数据包不能跨过路由器，只能在同一个物理链路内通信。

例如：>>[255.255.255.255:65535] 58

<<[255.255.255.255:65535] C0 A8 01 02 00 7F 23 00 00 01

向 255.255.255.255:65535 发送数据 0x58(字符‘X’)，接收到响应数据 C0 A8 01 02 00 7F 23 00 00 01 ，表示 IP 地址为 192.168.1.2， MAC 为 00-7F-23-00-00-01

向读写器广播发送’X’,得到响应：10byte。

IP(4byte)
MAC(6byte)

向读写器广播发送’P’,得到响应：25byte。

IP(4byte)
子网掩码(4byte)
网关(4byte)
服务器 IP(4byte)
服务器端口(2byte)
MAC(6byte)
协议类型(1byte)

读写器在作为 TCP Client 的时候，服务器 IP 是指连接到远程服务器的 IP，服务器端口是指远程服务器的端口。

读写器作为 TCP Server 或者 UDP 方式运行时，服务器 IP 是指本机的 IP，服务器端口是指本机的端口。因为此时本机就是服务器。

协议类型。0=TCP server， 1= TCP client， 2= UDP。

附录 1

18000-3 标签存储结构：

18000-3 标签分 4 个区：**保留区**（又称密码区），**EPC 区**，**TID 区**和 User 区。

保留区：保留区 4 个字。前两个字是销毁密码，后两个字是访问密码。可读可写，保留区的两个密码区的读写保护特性可以分别设置。

EPC 区：标签 EPC 号存储在该区，其中第 **0** 个字是 PC 值和标签 EPC 号的 CRC16。第 **1** 个字是 PC 值，该值指示标签 EPC 号长度，从第 **2** 个字开始才是标签的 EPC 号数据。可读可写。

TIC 区：该区存储的数据是由标签生产商设定的 ID 号。可读不可写。

User 区：是用户数据区。可读可写。

G2 命令中很多地方要求给出数据长度，这里要注意字与字节的区别。1 个字等于 2 个字节。

有些命令需要访问密码，如果没有密码设置，则用 0 填充密码区，而不能为空。