
**UHF 电子标签读写器
UHFReaderD840
用户手册 V1.15**

目录

一、通讯接口规格.....	1
二、协议描述.....	1
三、数据的格式.....	2
1. 上位机命令数据块.....	2
2. 读写器响应数据块.....	2
四、操作命令总汇.....	3
1. EPC C1 G2 (ISO18000-6C) 命令.....	3
2. 18000-6B 命令.....	4
3. 读写器自定义命令.....	4
五、命令执行结果状态值.....	5
六、电子标签返回错误代码.....	9
七、标签存储区及需要注意的问题.....	10
八、操作命令详细描述.....	10
8.1 命令概述.....	10
8.2 EPC C1G2 命令.....	11
8.2.1 查询标签.....	11
8.2.2 读数据.....	14
8.2.3 写数据.....	15
8.2.4 写 EPC 号.....	17
8.2.5 销毁标签.....	17
8.2.6 设定存储区读写保护状态.....	18
8.2.7 块擦除.....	20
8.2.8 读保护设置(根据 EPC 号设定).....	21
8.2.9 读保护设置(不需要 EPC 号).....	22
8.2.10 解锁读保护.....	23
8.2.11 测试标签是否被设置读保护.....	23
8.2.12 EAS 报警设置.....	24
8.2.13 EAS 报警检测.....	25
8.2.14 查询单张标签.....	25
8.2.15 块写命令.....	25
8.2.16 读取 Monza4QT 工作参数.....	27
8.2.17 设置 Monza4QT 工作参数.....	28
8.2.18 指定掩码扩展读数据.....	29
8.2.19 指定掩码扩展写数据.....	30
8.2.20 带缓存查询.....	32
8.2.21 混合查询.....	34
8.2.22 指定 EPC 号查询.....	37
8.2.23 QT 查询.....	39
8.3 18000-6B 命令.....	41
8.3.1 寻查命令(单张).....	41
8.3.2 按条件寻查标签.....	42
8.3.3 读数据.....	43

8.3.4 写数据.....	43
8.3.5 锁定检测.....	44
8.3.6 锁定.....	44
8.4 读写模块自定义命令.....	45
8.4.1 读取读写器信息.....	45
8.4.2 设置读写器工作频率.....	46
8.4.3 设置读写模块地址.....	47
8.4.4 设置读写模块查询时间.....	47
8.4.5 设置串口波特率.....	48
8.4.6 调整功率.....	48
8.4.7 声光控制命令.....	49
8.4.8 配置天线.....	49
8.4.9 蜂鸣器设置.....	50
8.4.10 GPIO 控制命令.....	50
8.4.11 读取 GPIO 状态.....	51
8.4.12 读写器唯一序列号获取.....	51
8.4.13 标签自定义功能设置.....	51
8.4.14 设置天线检测.....	52
8.4.15 设置通信接口.....	52
8.4.16 天线检测回损设置/读取命令.....	53
8.4.17 设置缓存的 EPC/TID 长度.....	53
8.4.18 获取缓存的 EPC/TID 长度.....	54
8.4.19 缓存数据获取.....	54
8.4.20 清缓存.....	55
8.4.21 查询缓存区标签数量.....	55
8.4.22 设置实时查询参数.....	55
8.4.23 设置工作模式.....	57
8.4.24 读取工作模式参数.....	59
8.4.25 读取/设置实时查询心跳包时间.....	60
8.4.26 设置写功率.....	61
8.4.27 读取写功率.....	61
8.4.28 读取/设置写重试次数.....	62
8.4.29 标签自定义功能用户密码设置.....	63
8.4.30 标签自定义功能用户密码读取.....	63
8.4.31 读写器 profile 设置/读取命令.....	63
8.4.32 同步 EM4325 时间戳.....	64
8.4.33 获取 EM4325 温度数据.....	65
8.4.34 获取 EM4325 的 SPI 外部数据.....	66
8.4.35 复位 EM4325 警报.....	68
8.4.36 DRM 设置/读取命令.....	69
8.4.37 测量天线口的回波损耗.....	70
8.4.38 测量读写器当前工作温度.....	71

一、通讯接口规格

读写器通过 UART 或者 USB 接口与上位机串行通讯，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一个起始位，8 个数据位，一个停止位，无奇偶校验位，缺省波特率 57600。在串行通讯过程中，每个字节的最低有效位最先传输。

二、协议描述

通讯过程由上位机发送命令及参数给读写器，然后读写器将命令执行结果状态和数据返回给上位机。读写器接收一条命令执行一条命令，只有在读写器执行完一条命令后，才能接收下一条命令。在读写器执行命令期间，如果向读写器发送命令，命令将丢失。

上位机发送过程如下：

上位机	数据传递方向	读写器
命令数据块	→	

说明：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 **15ms**。在上位机的命令数据块发送过程中，如果相邻字符间隔大于 15ms，则之前接收到的数据均被当作无效数据丢弃，然后从下一个字节开始，重新接收。

读写器接收到正确查询命令后，在不超过查询时间的范围内（不包括数据发送过程，仅仅是读写器执行命令的时间），会返回给读写器一个响应。

读写器发送过程如下：

读写器	数据传递方向	上位机
响应数据块	→	

说明：读写器发送响应数据期间，相邻字节之间的发送时间间隔小于 15ms

完整的一次通讯过程是：上位机发送命令给读写器，并等待读写器返回响应；读写器接收命令后，开始执行命令，然后返回响应；之后上位机接收读写器的响应。一次通讯结束。

三、数据的格式

1. 上位机命令数据块

Len	Adr	Cmd	Data[]	LSB-CRC16	MSB-CRC16
-----	-----	-----	--------	-----------	-----------

数据各部分说明如下：

	长度(字节)	说明
Len	1	命令数据块的长度,但不包括 Len 本身。即数据块的长度等于 4 加 Data[] 的长度。Len 允许的最大值为 255, 最小值为 4。
Adr	1	读写器地址。地址范围: 0x00~0xFE, 0xFF 为广播地址, 读写器只响应和自身地址相同及地址为 0xFF 的命令。读写器出厂时地址为 0x00。
Cmd	1	命令代码。
Data[]	不定	参数域。在实际命令中, 可以不存在。
LSB-CRC16	1	CRC16 低字节。CRC16 是从 Len 到 Data[] 的 CRC16 值
MSB-CRC16	1	CRC16 高字节。

2. 读写器响应数据块

Len	Adr	reCmd	Status	Data[]	LSB-CRC16	MSB-CRC16
-----	-----	-------	--------	--------	-----------	-----------

数据各部分说明如下：

	长度(字节)	说明
Len	1	响应数据块的长度,但不包括 Len 本身。即数据块的长度等于 5 加 Data[] 的长度。
Adr	1	读写器地址。
reCmd	1	指示该响应数据块是哪个命令的应答。如果是对不可识别的命令的应答, 则 reCmd 为 0x00。
Status	1	命令执行结果状态值。
Data[]	不定	数据域, 可以不存在。
LSB-CRC16	1	CRC16 低字节。CRC16 是从 Len 到 Data[] 的 CRC16 值。
MSB-CRC16	1	CRC16 高字节。

CRC16 的 C 语言算法：

```
#define PRESET_VALUE 0xFFFF
```

```

#define POLYNOMIAL 0x8408
unsigned int uiCrc16Cal(unsigned char const * pucY, unsigned char ucX)
{
    unsigned char ucI,ucJ;
    unsigned short int uiCrcValue = PRESET_VALUE;
    for(ucI = 0; ucI < ucX; ucI++)
    {
        uiCrcValue = uiCrcValue ^ *(pucY + ucI);
        for(ucJ = 0; ucJ < 8; ucJ++)
        {
            if(uiCrcValue & 0x0001)
            {
                uiCrcValue = (uiCrcValue >> 1) ^ POLYNOMIAL;
            }
            else
            {
                uiCrcValue = (uiCrcValue >> 1);
            }
        }
    }
    return uiCrcValue;
}

```

pucY 是要计算 CRC16 的字符数组的入口， ucX 是字符数组中字符个数。

上位机收到数据的时候，只要把收到的数据按以上算法进行计算 CRC16，结果为 0x0000 表明数据正确。

四、操作命令总汇

1. EPC C1 G2 (ISO18000-6C) 命令

序号	命令	功能
1	0x01	查询标签
2	0x02	读数据
3	0x03	写数据
4	0x04	写 EPC 号
5	0x05	销毁标签
6	0x06	设定存储区读写保护状态
7	0x07	块擦除

8	0x08	根据 EPC 号设定读保护设置
9	0x09	不需要 EPC 号读保护设定
10	0x0a	解锁读保护
11	0x0b	测试标签是否被设置读保护
12	0x0c	EAS 报警设置
13	0x0d	EAS 报警探测
14	0x0f	查询单标签
15	0x10	块写
16	0x11	读取 Monza4QT 工作参数
17	0x12	设置 Monza4QT 工作参数
18	0x15	指定掩码扩展读数据
19	0x16	指定掩码扩展写数据
20	0x18	带缓存查询
21	0x19	混合查询
22	0x1a	指定 EPC 号查询
23	0x1b	QT 查询

2. 18000-6B 命令

序号	命令	功能
1	0x50	查询命令(单张)。这个命令每次只能查询一张电子标签。不带条件查询。
2	0x51	条件查询命令(多张)。这个命令根据给定的条件进行查询标签, 返回符合条件的电子标签的 UID。可以同时查询多张电子标签。
3	0x52	读数据命令。这个命令读取电子标签的数据, 一次最多可以读 32 个字节。
4	0x53	写数据命令。写入数据到电子标签中, 一次最多可以写 32 个字节。
5	0x54	检测锁定命令。检测某个存储单元是否已经被锁定。
6	0x55	锁定命令。锁定某个尚未被锁定的电子标签。

3. 读写器自定义命令

序号	命令	功能
1	0x21	读取读写器信息
2	0x22	设置读写器工作频率
3	0x24	设置读写模块地址
4	0x25	设置读写模块查询时间
5	0x28	设置串口波特率
6	0x2f	调整功率
7	0x33	声光控制命令
8	0x3f	配置天线

9	0x40	蜂鸣器设置
10	0x46	GPIO 控制命令
11	0x47	读取 GPIO 状态
12	0x4c	读写器唯一序列号获取
13	0x3a	标签自定义功能设置
14	0x66	设置天线检测
15	0x6a	设置通信接口
16	0x6e	天线检测回损设置/读取命令
17	0x70	设置缓存的 EPC/TID 长度
18	0x71	获取缓存的 EPC/TID 长度
19	0x72	缓存数据获取
20	0x73	清缓存
21	0x74	查询缓存区标签数量
22	0x75	设置实时查询参数
23	0x76	设置工作模式
24	0x77	读取工作模式参数
25	0x78	读取/设置实时查询心跳包时间
26	0x79	设置写功率
27	0x7a	读取写功率
28	0x7b	读取/设置写重试次数
29	0x7d	标签自定义功能用户密码设置
30	0x7e	标签自定义功能用户密码读取
31	0x7f	读写器 profile 设置/读取命令
32	0x85	同步 EM4325 时间戳
33	0x86	获取 EM4325 温度数据
34	0x87	获取 EM4325 的 SPI 外部数据
35	0x88	复位 EM4325 警报
36	0x90	DRM 设置/读取命令
37	0x91	测量天线口的回波损耗
38	0x92	测量读写器当前工作温度

五、命令执行结果状态值

响应数据块						Status 含义	说明
Len	Adr	reCmd	Status	Data[]	CRC16		
5+Data[] 部分的 长度	0xXX	0xXX	0x00	LSB+MSB	操作成功	当成功执行命令后返 回给上位机的状态 值。Data[]包含了所要 信息

5+Data[] 部分的 长度	0xXX	0x01	0x01	LSB+MSB	查询时间 结束前返 回	上位机发出查询 G2 标签命令时, 读写器 查询电子标签时, 如 果在设定的查询时间 内返回信息给上位 机, 则返回此状态值
5+Data[] 部分的 长度	0xXX	0x01	0x02	LSB+MSB	指定的询 查时间溢 出	上位机发出查询 G2 标签命令时, 当询 查时间溢出时, 读 写器还没有完 成查询操作时返 回给上位机的状 态值
5+Data[] 部分的 长度	0xXX	0x01	0x03	LSB+MSB	本条消息 之后, 还有 消息	上位机发出查询 G2 标签命令时, 如 果查询命令读到 的标签数 量无法在一 条消息内 传 送 完, 将分 多次 发 送。
5+Data[] 部分的 长度	0xXX	0x01	0x04	LSB+MSB	读写器存 储空间已 满	上位机发出查询 G2 标签命令时, 如 果查询到的电 子标签太 多, 超过了读 写器的存 储容 量, 则读 写器返 回读到的电 子标签 EPC 号, 同 时, 也 将返 回此 状 态 值
5	0xXX	0xXX	0x05	无此项	LSB+MSB	访问密码 错误	当读写器执 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 值
5	0xXX	0x05	0x09	无此项	LSB+MSB	销毁标签 失败	当向 G2 标 签进 行销 毁操 作时, 如 果销 毁密 码错 误, 或 是读 写器 与标 签通 讯不 畅, 则 将返 回此 状 态 值
5	0xXX	0x05	0x0a	无此项	LSB+MSB	销毁密 码不 能为全 0	销 毁标 签时, 销 毁密 码为 0 的标 签是无 法销 毁的

5	0xXX	0xXX	0x0b	无此项	LSB+MSB	电子标签不支持该命令	G2 协议中的某些可选命令, 及一些厂商的特定命令, 可能某些标签不支持这些命令, 此时返回此状态值
5	0xXX	0xXX	0x0c	无此项	LSB+MSB	对该命令访问密码不能为全 0	对 NXP UCODE EPC G2X 标签设置读保护及设置 EAS 报警时, 访问密码不能为全 0, 若为全 0, 将返回此状态值
5	0xXX	0x0a	0x0d	无此项	LSB+MSB	电子标签已经被设置了读保护, 不能再次设置	对已经被设置了读保护的 NXP UCODE EPC G2X 标签, 在解除读保护之前, 不能再次设置。此情况下返回这个状态值
5	0xXX	0x0a	0x0e	无此项	LSB+MSB	电子标签没有被设置读保护, 不需要解锁	对 NXP UCODE EPC G2X 标签解锁, 如果标签没有被锁定, 将返回此状态值, 对不支持读保护设定命令的标签发送此命令, 也将返回此状态值
5	0xXX	0x53	0x10	无此项	LSB+MSB	有字节空间被锁定, 写入失败	在向 6B 标签写入数据时, 因为有字节空间被锁定, 使得写入数据失败时, 返回此状态值
5	0xXX	0x55	0x11	无此项	LSB+MSB	不能锁定	当 6B 标签出现不能被锁定的情况, 返回此状态值
5	0xXX	0x55	0x12	无此项	LSB+MSB	已经锁定, 不能再次锁定	对已经锁定的 6B 标签进行再次锁定时, 返回此状态值
5	0xXX	0xXX	0x13	无此项	LSB+MSB	参数保存失败, 但设置的值在读写器断电前有效	对于某些需要保存的参数, 如果保存失败, 则返回此之态

5	0xXX	0xXX	0x14	无此项	LSB+MSB	无法调整	调整功率的时候，在某些情况下，如果出现功率无法调整的错误，则返回此状态值
5+Data[]的长度	0xXX	0x51	0X15	LSB+MSB	查询时间结束前返回	上位机发出查询 6B 标签命令时，读写器查询电子标签时，如果在设定的查询时间内返回信息给上位机，则返回此状态值
5+Data[]的长度	0xXX	0x51	0x16	LSB+MSB	指定的查询时间溢出	上位机发出查询 6B 标签命令时，当查询时间溢出时，读写器还没有完成查询操作时返回给上位机的状态值
5+Data[]的长度	0xXX	0x51	0x17	LSB+MSB	本条消息之后，还有消息	上位机发出查询 6B 标签命令时，如果查询命令读到的标签数量无法在一条消息内传送完，将分多次发送。
5+Data[]的长度	0xXX	0x51	0x18	LSB+MSB	读写器存储空间已满	上位机发出查询 6B 标签命令时，如果查询到的电子标签太多，超过了读写器的存储容量，则读写器返回读到的电子标签 UID 号，同时，也将返回此状态值
5	0xXX	0xXX	0x19	无此项	LSB+MSB	电子标签不支持该命令或者访问密码不能为 0	当设置电子标签的 EAS 报警时，在通信正常的情况下，如果标签无法设置，则可能是电子标签不支持该命令，也可能是电子标签的访问密码不能为 0
5	0xXX	0xXX	0x1A	无此项	LSB+MSB	标签自定义功能执行错误	当特定标签功能启动后某些命令执行失败时返回给上位机的状态值

5+Data[]部分的长度	0xXX	0x01	0x26	LSB+MSB	本条消息为数据统计包	上位机发出查询 G2 标签命令时, 读写器在查询标签结束后, 如果读写器发送统计数据, 则返回此状态值。
5+Data[]部分的长度	0xXX	0xee	0x28	LSB+MSB	本条消息为心跳包	自动实时查询模式下, 心跳包时间间隔内没有读到符合条件的标签, 上传心跳包数据
5	0xXX	0xXX	0xF8	无此项	LSB+MSB	检测天线错误	读写器对电子标签进行操作前, 检测到天线连接出错。
5	0xXX	0xXX	0xF9	无此项	LSB+MSB	命令执行出错	命令执行出错
5	0xXX	0xXX	0xFA	无此项	LSB+MSB	有电子标签, 但通信不畅, 操作失败	当检测到有效范围内存在可操作的电子标签, 但读写器与电子标签之间的通讯质量不好, 而无法完成整个通讯过程时返回给上位机的信息
5	0xXX	0xXX	0xFB	无此项	LSB+MSB	无电子标签可操作	当读写器对电子标签进行操作时, 有效范围内没有可操作的电子标签时返回给上位机的状态值
6	0xXX	0xXX	0xFC	Err_code	LSB+MSB	电子标签返回错误代码	电子标签返回错误代码时, 错误代码由 Err_code 返回给上位机
5	0xXX	0xXX	0xFD	无此项	LSB+MSB	命令长度错误	当上位机输入的命令的实际长度和它应当具有的长度不同时, 返回该状态
5	0xXX	0x00	0xFE	无此项	LSB+MSB	不合法的命令	当上位机输入的命令是不可识别的命令, 如不存在的命令、或是 CRC 错误的命令
5	0xXX	0xXX	0xFF	无此项	LSB+MSB	参数错误	上位机发送的命令中的参数不符合要求时, 返回此状态

六、电子标签返回错误代码

EPC C1G2 (ISO18000 -6C) 电子标签错误代码:

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

七、标签存储区及需要注意的问题

A. EPC C1G2 标签（简称 G2 标签）

G2 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。

B. 18000-6B 标签

6B 标签只有一个存储空间，最低 8 个字节是标签的 UID，并且不能被改写。后面的字节都是可改写的，也可以被锁定，但是一旦锁定后，则不能再次改写，也不能解锁。

八、操作命令详细描述

8.1 命令概述

操作命令有两大类，一类是协议相关命令；另一类是读写器相关命令。

如果上位机输入的命令是不可识别的命令，如不存在的命令、或是 CRC 错误的命令，则返回值如下：

Len	Adr	reCmd	Status	CRC-16	
0x05	0xXX	0x00	0xFE	LSB	MSB

如果命令的长度不对，则返回信息如下：

Len	Adr	reCmd	Status	CRC-16	
0x05	0xXX	0xXX	0xFD	LSB	MSB

有两种命令读写器不会响应：

1. 如果输入的命令的地址出错(地址不是 0xFF，也不是读写器地址)，读写器不会有任何响应。
2. 如果输入的命令是不完整的，即命令的 Len 域指示的命令长度大于实际的命令长度，则读写器将不会做出任何响应。

8.2 EPC C1G2 命令

8.2.1 查询标签

查询命令的作用是检查有效范围内是否有符合协议的电子标签存在。想要对未知 EPC 的新标签进行别的操作前，应先通过查询命令来得到标签的 EPC 号。

在运行查询命令之前，用户可以根据需要先设定好该命令的最大运行时间(查询时间)。读写器在查询时间规定的范围内必须给上位机一个结果，如果读写器尚未查询完有效范围内的所有标签，而查询时间已到，则读写器不再查询其它标签，而是直接把已经查询到得标签返回给上位机，并提示上位机还有标签未读完。然后等待下一个命令。

查询时间的缺省值是 2s，用户可以通过运行读写器自定义命令 **设定查询时间命令** 来修改。允许的范围是：3*100ms~255*100ms(实际的响应时间可能会比设定的值大 0~75ms)。

查询时间如果设定的过短，可能会出现在规定时间内查询不到电子标签的情况。

命令：

Len	Adr	Cmd	Data[]	CRC-16

0xXX	0xXX	0x01	—	LSB	MSB
------	------	------	---	-----	-----

Data 参数如下：

Data[]							
QValue	Session	MaskMem	MaskAdr	MaskLen	MaskData	AdrTID	LenTID
0xXX	0xXX	0xXX	2Bytes	0xXX	变长	0xXX	0xXX

Data[]		
Target	Ant	Scantime
0xXX	0xXX	0xXX

参数解析：

QValue：1个字节。

bit7：统计数据包标志。

0 – 询问结束后，不发送询问过程统计数据包；

1 – 询问结束后，发送询问过程统计数据包。

bit6：策略选择标志。

0 – 通用策略；

1 – 特殊策略。

bit5：FastID 标志。

0 – 不启用 Impinj 的 FastID 功能；

1 – 启用 Impinj 的 FastID 功能。

bit4~bit0：询问 EPC 标签时使用的初始 Q 值，Q 值的设置应为场内的标签数量约等于 2^Q 。Q 值的范围为 0~15，若命令中出现了其它值，将返回参数出错的消息。

Session：1个字节，询问 EPC 标签时使用的 Session 值。

0x00：Session 使用 S0；

0x01：Session 使用 S1；

0x02：Session 使用 S2；

0x03：Session 使用 S3。

0xff：读写器自动配置 Session（仅对 EPC 询问有效）。

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，掩码区。0x01：EPC 存储区；0x02：TID 存储区；0x03：用户存储区。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。

MaskAdr：两个字节，掩码的起始位地址（单位：Bits）。范围 0~16383。

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。

AdrTID: 查询 TID 区的起始字地址。命令中有此参数和 LenTID 时表示查询的是 TID 而不是 EPC 号。

LenTID: 查询 TID 区的数据字数。LenTID 取值为 0~15, 若为其它参数将返回参数错误信息。命令中有此参数和 AdrTID 时表示查询的是 TID 而不是 EPC 号。

Target (可选参数) : 1 个字节, 查询 EPC 标签时使用的 Target 值。

0x00: Target 值使用 A。

0x01: Target 值使用 B。

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。

Ant (可选参数) : 1 个字节, 本次要进行查询的天线号。

0x80 – 天线 1;

0x81 – 天线 2;

0x82 – 天线 3;

0x83 – 天线 4。

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。

ScanTime (可选参数) : 1 个字节。本次命令查询时间。读写器将会把查询命令最大响应时间设置为 ScanTime*100ms。

注:

①当 MaskMem、MaskAdr、MaskLen、MaskData 为空时表示无掩膜条件。

②Target、Ant、ScanTime 为可选参数, 命令中必须同时带有这三个参数或同时不带这三个参数。当命令中没有带这三个参数时, 设备使用预先设定的 Target、Ant、ScanTime 参数查询标签; 当命令中带有这三个参数时, 设备使用这三个指定的参数值查询标签。

③FastID 功能仅对 Impinj 公司支持 FastID 的芯片有效。

(1) 当应答状态 Status 为 0x26 时, 应答如下:

Len	Adr	reCmd	Status	Data[]			CRC-16	
				Ant	ReadRate	TotalCount		
0xXX	0xXX	0x01	0x26	0xXX	2Bytes	4Bytes	LSB	MSB

参数解析:

Status 是应答的状态, 其代表的意义如下表所述:

Status	说明
0x26	查询结束后, 返回本次查询过程的统计数据。

参数解析:

Ant: 表示有哪些天线查询到标签。如 0x04, 二进制为 0000 0100, 表示天线 3 查询到该标签; 如 0x08, 二进制为 0000 1000, 表示天线 4 查询到标签。

ReadRate: 此次执行命令的标签识别速度(成功读取标签的次数/秒)。不区分是否多次读取同一张标签。

TotalCount: 此次执行命令的总读取标签次数，不区分是否多次读取同一张标签。

(2) 当应答状态 Status 为除 0x26 以外的状态时，应答如下：

应答：

Len	Adr	reCmd	Status	Data[]			CRC-16	
				Ant	Num	EPC ID		
0xXX	0xXX	0x01	0xXX	0xXX	0xXX	EPC-1, EPC-2, EPC-3...	LSB	MSB

参数解析：

Status 是应答的状态，其代表的意义如下表所述：

Status	说明
0x01	命令执行结束，同时返回查询到的电子标签数据
0x02	查询时间结束，命令执行强制退出，同时返回已查询到的标签数据
0x03	如果读到的标签数量无法在一条消息内传送完，将分多次发送。如果 Status 为 0x03，则表示这条数据结束后，还有数据。
0x04	还有电子标签未读取，电子标签数量太多，读写器的存储区已满，返回此状态值，同时返回已查询到得电子标签数据。
0xF8	天线连接检测错误，当前天线连接可能已经断开。

Ant: 表示有哪些天线查询到该标签。如 0x04，二进制为 0000 0100，表示天线 3 查询到该标签；如 0x08，二进制为 0000 1000，表示天线 4 查询到该标签。

Num: 本次应答中包含的电子标签的 EPC/TID 的个数。

EPC ID: 读到的电子标签的 EPC/TID 数据，EPC-1 是第一张标签的 **EPC/TID 长度**+第一张标签的 EPC 号或 TID 数据+第一张标签的 **RSSI 值**，依此类推。每个电子标签 EPC 号或 TID 数据高字(EPC C1 G2 中数据以字为单位)在前，每一个字的高字节在前。**EPC/TID 长度**以一个字节表示。**RSSI 值**长度以一个字节表示。

如果启用了 FastID 功能，EPC ID 每一段内容为标签的 **EPC+TID 长度 (1 个字节)** + 标签 EPC 号+12 字节 TID 数据+标签的 **RSSI 值**，其中 **EPC+TID 长度**的最高位表示数据中是否含有 TID。注意 FastID 功能仅对 Impinj 公司支持 FastID 的芯片有效。

EPC ID 具体说明如下：

EPC ID					
EPC-1			EPC-2		
数据长度	数据	RSSI	数据长度	数据	RSSI
1 byte	N byte	1 byte	1 byte	N byte	1 byte
Bit7: 0 – 数据为 EPC 或 TID。 1 – 数据为					

EPC+TID (FastID 开启有效)。 Bit6~0: 数据长度 N。				
---	--	--	--	--

8.2.2 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。

命令：

Len	Adr	Cmd	Data[]	CRC-16	
0xXX	0xXX	0x02	—	LSB	MSB

Data 参数如下：

Data[]									
ENum	EPC	Mem	WordPtr	Num	Pwd	MaskMem	MaskAdr	MaskLen	MaskData
0xXX	变长	0xXX	0xXX	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: 一个字节。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(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。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)。范围 0~16383。

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	reCmd	Status	Data[]	CRC-16	
0xXX	0xXX	0x02	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。

8.2.3 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	Data[]	CRC-16	
0xXX	0xXX	0x03	——	LSB	MSB

Data 参数如下:

Data[]					
WNum	ENum	EPC	Mem	WordPtr	Wdt
0xXX	0xXX	变长	0xXX	0xXX	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: 一个字节, 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)。范围 0~16383。

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	reCmd	Status	Data[]	CRC-16	
0x05	0xXX	0x03	0x00	——	LSB	MSB

8.2.4 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。

命令:

Len	Adr	Cmd	Data[]			CRC-16	
			ENum	Pwd	WEPC		
0xXX	0xXX	0x04	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 31, 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 1 个字, 最多 31 个字, 否则返回参数错误信息。

应答:

Len	Adr	reCmd	Status	Data[]	CRC-16	
0x05	0xXX	0x04	0x00	——	LSB	MSB

8.2.5 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	Data[]	CRC-16	
0xXX	0xXX	0x05	——	LSB	MSB

Data 参数如下:

Data[]						
ENum	EPC	Killpwd	MaskMem	MaskAddr	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 、 MaskAddr 、 MaskLen 、 MaskData 参数项。ENum 为 0xff 时 有 MaskMem 、 MaskAddr 、 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)。范围 0~16383。

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	reCmd	Status	Data[]	CRC-16	
0x05	0xXX	0x05	0x00	—	LSB	MSB

8.2.6 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读写保护设定。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	Data[]	CRC-16	
0xXX	0xXX	0x06	—	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）。范围 0~16383。

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	reCmd	Status	Data[]	CRC-16	
0x05	0xXX	0x06	0x00	—	LSB	MSB

8.2.7 块擦除

此命令可以擦除标签的保留区、EPC 存储区、TID 存储区或用户存储区的若干字。

命令：

Len	Adr	Cmd	Data[]	CRC-16	
0xXX	0xXX	0x07	—	LSB	MSB

Data 参数如下：

Data[]									
ENum	EPC	Mem	WordPtr	Num	Pwd	MaskMem	MaskAdr	MaskLen	MaskData
0xXX	变长	0xXX	0xXX	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。

Mem: 1 个字节, 选择要读取的存储区。0x00: 保留区; 0x01: EPC 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, 则返回参数错误信息。

WordPtr: 1 个字节, 指定要擦除的字起始地址。0x00 表示从第一个字(第一个 16 位存储体)开始擦除, 0x01 表示从第 2 个字开始擦除, 依次类推。当擦除 EPC 区时, WordPtr 必须大于等于 0x01, 若小于 0x01, 则返回参数错误消息。

Num: 1 个字节, 指定要擦除的字的个数。从 WordPtr 指定的地址开始擦除, 擦除 Num 指定个数的字。若 Num 为 0x00, 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。当进行擦除操作时, 并且相应存储区设置为密码锁的时候, 才必须使用正确的访问密码。其它情况下, 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)。范围 0~16383。

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	reCmd	Status	Data[]	CRC-16	
0x05	0xXX	0x07	0x00	——	LSB	MSB

8.2.8 读保护设置(根据 EPC 号设定)

这个命令根据电子标签的 EPC 号, 对标签设置读保护, 使得电子标签不能被任何命令读写对标签进行查询操作, 也无法得到电子标签的 EPC 号。仅对 **NXP UCODE EPC G2X** 标签有效。

命令:

Len	Adr	Cmd	Data[]	CRC-16	
0xXX	0xXX	0x08	——	LSB	MSB

Data 参数如下:

Data[]						
ENum	EPC	Pwd	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。

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。待设定读保护的电子标签访问密码必须不为 0, 访问密码为 0 的电子标签是无法设置读保护的, 在命令中, 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)。范围 0~16383。

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	reCmd	Status	Data[]	CRC-16	
0x05	0xXX	0x08	0x00	——	LSB	MSB

8.2.9 读保护设置 (不需要 EPC 号)

这个命令可以为有效范围内的电子标签设定读保护。这个命令与前面一个命令的区别是, 当有效范围内存在多张标签的时候, 无法知道这个命令操作的是哪一张电子标签。如果要同时对多张标签进行操作, 则标签的访问密码最好是相同的。仅对 **NXP UCODE EPC G2X** 标签有效。

命令:

Len	Adr	Cmd	Data[]	CRC-16		
			Pwd			
0x08	0xXX	0x09	4Byte	LSB	MSB	

参数解析:

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。待设定读保护的电子标签访问密码必须不为 0, 访问密码为 0 的电子标签是无法设置读保护的, 在命令中, 必须给出正确的访问密码。

应答:

Len	Adr	reCmd	Status	Data[]	CRC-16	
0x05	0xXX	0x09	0x00	——	LSB	MSB

8.2.10 解锁读保护

这个命令用来解锁已设置读保护的标签。用这个命令时, 天线有效范围内只能放置一张要被解锁的电子标签。仅对 **NXP UCODE EPC G2X** 标签有效。

命令:

Len	Adr	Cmd	Data[]	CRC-16		
			Pwd			
0x08	0xXX	0x0a	4Byte	LSB	MSB	

参数解析:

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。命令中必须给出正确的访问密码。

应答:

Len	Adr	reCmd	Status	Data[]	CRC-16	
0x05	0xXX	0x0a	0x00	——	LSB	MSB

说明: 对于不支持读保护设定的标签, 认为没有被锁定。

8.2.11 测试标签是否被设置读保护

这个命令不能测试标签是否支持读保护锁定命令, 只能测试标签是否被读保护锁定。对于不支持读保护锁定的电子标签, 一致认为没有被锁定。

这个命令只能对单张电子标签进行操作, 确保天线有效范围内只存在一张电子标签。仅对 **NXP 的 UCODE EPC G2X** 标签有效。

命令:

Len	Adr	Cmd	Data[]	CRC-16	
0x04	0xXX	0x0b	——	LSB	MSB

应答:

Len	Adr	reCmd	Status	Data[]	CRC-16	
0x06	0xXX	0x0b	0x00	ReadPro	LSB	MSB

参数解析:

ReadPro	说明
0x00	电子标签没有被设置为读保护。
0x01	电子标签被设置读保护。

说明: 对于不支持读保护设定的标签, 认为没有被设置读保护。

8.2.12 EAS 报警设置

对电子标签的 EAS 状态位进行设置或复位。仅对 **NXP UCODE EPC G2** 标签有效。

命令:

Len	Adr	Cmd	Data[]	CRC-16	
0xXX	0xXX	0x0c	——	LSB	MSB

Data 参数如下:

Data[]							
ENum	EPC	Pwd	EAS	MaskMem	MaskAdr	MaskLen	MaskData
0xXX	变长	4Byte	0xXX	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。

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。待设置的标签的访问密码必须不为 0, 访问密码为 0 的电子标签是无法设置 EAS 报警的。Pwd 必须是正确的访问密码。

EAS: 1 个字节。Bit0 位为 0, 表示设置为关闭 EAS 报警; 为 1, 表示设置为打开 EAS 报警。Bit1 – Bit7 位保留, 默认为 0。

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)。范围 0~16383。

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	reCmd	Status	Data[]	CRC-16	
0xXX	0xXX	0x0c	0x00	---	LSB	MSB

8.2.13 EAS 报警检测

该命令检测电子标签的 EAS 报警。仅对 **NXP UCODE EPC G2** 标签有效。

命令:

Len	Adr	Cmd	Data[]	CRC-16	
0x04	0xXX	0x0d	---	LSB	MSB

应答:

Len	Adr	reCmd	Status	Data[]	CRC-16	
0x05	0xXX	0x0d	0x00	---	LSB	MSB

无 EAS 报警的时候, 返回“无电子标签可操作”消息。

8.2.14 查询单张标签

命令:

Len	Adr	Cmd	Data[]	CRC-16
0xXX	0xXX	0x0d	---	---

0x04	0xXX	0x0f	—	LSB	MSB
------	------	------	---	-----	-----

应答：

Len	Adr	reCmd	Status	Data[]			CRC-16	
				Ant	Num	EPC ID		
0xXX	0xXX	0x0f	0x01	0xXX	0x01	EPC-1	LSB	MSB

Ant: 表示有哪些天线查询到该标签。如 0x04, 二进制为 0000 0100, 表示天线 3 查询到该标签；如 0x08, 二进制为 0000 1000, 表示天线 4 查询到该标签。

Num: 本次应答中包含的电子标签的 EPC 的个数。

EPC ID: 读到的电子标签的 EPC 数据, EPC-1 是第一张标签的 **EPC 长度**+第一张标签的 EPC 号+第一张标签的 **RSSI 值**。电子标签 EPC 号高字(EPC C1 G2 中数据以字为单位)在前, 每一个字的高字节在前。 **EPC 长度**以一个字节表示。 **RSSI 值**长度以一个字节表示。

8.2.15 块写命令

该命令一次能将多个字写入标签的保留区、EPC 区、TID 区或用户区。

命令：

Len	Adr	Cmd	Data[]	CRC-16	
0xXX	0xXX	0x10	—	LSB	MSB

Data 参数如下：

Data[]					
WNum	ENum	EPC	Mem	WordPtr	Wdt
0xXX	0xXX	变长	0xXX	0xXX	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, 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，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。

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: 一个字节，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)。范围 0~16383。

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	reCmd	Status	Data[]	CRC-16	
0x05	0xXX	0x10	0x00	——	LSB	MSB

8.2.16 读取 Monza4QT 工作参数

该命令用于读取标签当前设置的工作参数。仅对 **Impinj** 的 **Monza 4QT** 标签有效。

命令：

Len	Adr	Cmd	Data[]	CRC-16	
0xXX	0xXX	0x11	——	LSB	MSB

Data 参数如下：

ENum	EPC	Pwd	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。

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。命令中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)。范围 0~16383。

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	reCmd	Status	Data[]		CRC-16	
0x07	0xXX	0x11	0x00	NC	QTcontrol	LSB	MSB

参数解析:

QTcontrol: 标签工作参数。

Bit0: 标签当前使用的镜像页。Bit0 = 0 时表示 private; Bit0 = 1 时表示 public。
Bit1: 标签是否使能距离保护。Bit1 = 0 时表示不使能; Bit1 = 1 时表示使能。
其他值保留。

8.2.17 设置 Monza4QT 工作参数

该命令用于配置标签的工作参数。仅对 **Impinj** 的 **Monza 4QT** 标签有效。

命令:

Len	Adr	Cmd	Data[]	CRC-16
-----	-----	-----	--------	--------

0xXX	0xXX	0x12	——	LSB	MSB
------	------	------	----	-----	-----

Data 参数如下：

ENum	EPC	QTcontrol1	QTcontrol0	Pwd	MaskMem	MaskAdr	MaskLen	MaskData
0xXX	变长	0x00	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。

QTcontrol1: 保留字节, 取定值 0x00。

QTcontrol0: 标签工作参数。

Bit0: 标签当前使用的镜像页。Bit0 = 0 时表示 private; Bit0 = 1 时表示 public。

Bit1: 标签是否使能距离保护。Bit1 = 0 时表示不使能; Bit1 = 1 时表示使能。
其他值保留。

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。命令中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)。范围 0~16383。

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	reCmd	Status	Data[]	CRC-16	
0x05	0xXX	0x12	0x00	——	LSB	MSB

8.2.18 指定掩码扩展读数据

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。

命令：

Len	Adr	Cmd	Data[]	CRC-16	
0xXX	0xXX	0x15	——	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，高字节在前。指定要读取的字起始地址。0x0000 表示从第一个字(第一个 16 位存储区)开始读，0x0001 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(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。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)。范围 0~16383。

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	reCmd	Status	Data[]	CRC-16	
0xXX	0xXX	0x15	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。

8.2.19 指定掩码扩展写数据

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	Data[]	CRC-16	
0xXX	0xXX	0x16	——	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, 高字节在前, 指定要写入数据的字起始地址。

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)。范围 0~16383。

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	reCmd	Status	Data[]	CRC-16	
0x05	0xXX	0x16	0x00	—	LSB	MSB

8.2.20 带缓存查询

上位机发送该命令进行多标签识别操作, 同时将标签数据存入读写器缓存区。

和 8.2.1 “查询标签” 命令不同的是, 读写器在预先设定好的**查询时间**内连续地查询标签, 将标签数据存储到内部的缓存区中 (缓存区可以设定为 EPC 最大长度 128bit 或 496bit 两种格式), 在查询时间到来后结束查询, 并返回缓存区中标签总数和本次查询的标签次数 (相同标签多次读到将被多次计数)。用户可以通过缓存数据提取、清空缓存和查询缓存区标签数量等命令来访问缓存中的数据。

查询时间的缺省值是 2s, 用户可以通过运行读写器自定义命令**设定查询时间命令**来修改, 也可以通过附带可选参数来临时设置。允许的范围是: 3*100ms~255*100ms(实际的响应时间可能会比设定的值大 0~75ms)。

查询时间如果设定的过短, 可能会出现在规定时间内查询不到电子标签的情况。

注: 上位机一旦执行 8.2.1 “查询标签” 命令, 之前缓存区的数据将被清空。

命令:

Len	Adr	Cmd	Data[]	CRC-16	
0xXX	0xXX	0x18	——	LSB	MSB

Data 参数如下：

Data[]							
QValue	Session	MaskMem	MaskAdr	MaskLen	MaskData	AdrTID	LenTID
0xXX	0xXX	0xXX	2Bytes	0xXX	变长	0xXX	0xXX

Data[]		
Target	Ant	Scantime
0xXX	0xXX	0xXX

参数解析：

QValue: 1 个字节。

bit7: 保留, 置 0。

bit6: 策略选择标志。

0 – 通用策略；

1 – 特殊策略。

bit5~bit0: 询问 EPC 标签时使用的初始 Q 值, Q 值的设置应为场内的标签数量约等于 2^Q 。Q 值的范围为 0~15, 若命令中出现了其它值, 将返回参数出错的消息。

Session: 1 个字节, 询问 EPC 标签时使用的 Session 值。

0x00: Session 使用 S0;

0x01: Session 使用 S1;

0x02: Session 使用 S2;

0x03: Session 使用 S3。

0xff: 读写器自动配置 Session (仅对 EPC 询问有效)。

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, 掩码区。0x01: EPC 存储区; 0x02: TID 存储区; 0x03: 用户存储区。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。

MaskAdr: 两个字节, 掩码的起始位地址 (单位: Bits)。范围 0~16383。

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。

AdrTID: 询问 TID 区的起始字地址。命令中有此参数和 LenTID 时表示询问的是 TID 而不是 EPC 号。

LenTID: 询问 TID 区的数据字数。LenTID 取值为 0~15, 若为其它参数将返回参数错误信

息。命令中有此参数和 AdrTID 时表示查询的是 TID 而不是 EPC 号。

Target (可选参数)：1 个字节，查询 EPC 标签时使用的 Target 值。

0x00：Target 值使用 A。

0x01：Target 值使用 B。

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。

Ant (可选参数)：1 个字节，本次要进行查询的天线号。

0x80 – 天线 1；

0x81 – 天线 2；

0x82 – 天线 3；

0x83 – 天线 4。

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。

ScanTime (可选参数)：1 个字节。本次命令查询时间。读写器将会把查询命令最大响应时间设置为 ScanTime*100ms。

注：

① 当 MaskMem、MaskAdr、MaskLen、MaskData 为空时表示无掩膜条件。

② Target、Ant、ScanTime 为可选参数，命令中必须同时带有这三个参数或同时不带这三个参数。当命令中没有带这三个参数时，设备使用预先设定的 Target、Ant、ScanTime 参数查询标签；当命令中带有这三个参数时，设备使用这三个指定的参数值查询标签。

应答：

Len	Adr	reCmd	Status	Data[]		CRC-16	
				BufferCount	TagNum		
0x09	0xXX	0x18	0x00	2bytes	2bytes	LSB	MSB

参数解析：

BufferCount：2 个字节，缓存中记录的标签总数，相同 EPC/TID 数据的标签将被视为同一张标签。若未清空缓存，标签数量为多次查询操作的数量累加。

TagNum：2 个字节，本次查询中读取标签的次数，不区分是否多次读取同一张标签。

8.2.21 混合查询

混合查询命令的作用是检查有效范围内是否有符合协议的电子标签存在，并在查询到标签 EPC 号的同时读取指定的标签数据。

在运行混合查询命令之前，用户可以根据需要先设定好该命令的最大运行时间(查询时间)读写器在查询时间规定的范围内必须给上位机一个结果，如果读写器尚未读完有效范围内的所有标签，而查询时间已到，则读写器不再查询其它标签，而是直接把已经查询到得标签返回

给上位机，并提示上位机还有标签未读完。然后等待下一个命令。

查询时间的缺省值是 2s，用户可以通过运行读写器自定义命令**设定查询时间命令**来修改。允许的范围是：3*100ms~255*100ms(实际的响应时间可能会比设定的值大 0~75ms)。

查询时间如果设定的过短，可能会出现在规定时间内查询不到电子标签的情况。

命令：

Len	Adr	Cmd	Data[]	CRC-16	
0xXX	0xXX	0x19	——	LSB	MSB

Data 参数如下：

Data[]					
QValue	Session	MaskMem	MaskAdr	MaskLen	MaskData
0xXX	0xXX	0xXX	2Bytes	0xXX	变长

Data[]						
ReadMem	ReadAdr	ReadLen	Pwd	Target	Ant	Scantime
0xXX	2Bytes	0xXX	4Bytes	0xXX	0xXX	0xXX

参数解析：

QValue：1 个字节。

bit7：统计数据包标志。

0 – 询问结束后，不发送统计数据包；

1 – 询问结束后，发送统计数据包。

bit6~bit0：询问 EPC 标签时使用的初始 Q 值，Q 值的设置应为场内的标签数量约等于 2^Q 。Q 值的范围为 0~ 15，若命令中出现了其它值，将返回参数出错的消息。

Session：1 个字节，询问 EPC 标签时使用的 Session 值。

0x00：Session 使用 S0；

0x01：Session 使用 S1；

0x02：Session 使用 S2；

0x03：Session 使用 S3。

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(可选参数)：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(可选参数)：两个字节，掩码的起始位地址（单位：Bits）。范围 0~16383。

MaskLen(可选参数)：一个字节，掩码的位长度（单位：Bits）。

MaskData(可选参数): 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。

ReadMem: 1 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。

ReadAdr: 两个字节，高字节在前。指定要读取的字起始地址。0x0000 表示从第一个字(第一个 16 位存储区)开始读，0x0001 表示从第 2 个字开始读，依次类推。

ReadLen: 1 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。ReadLen 不能超过 120，即最多读取 120 个字。若 ReadLen 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(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。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。

Target (可选参数)：1 个字节，查询 EPC 标签时使用的 Target 值。

0x00: Target 值使用 A。

0x01: Target 值使用 B。

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。

Ant (可选参数)：1 个字节，本次要进行查询的天线号。

0x80 – 天线 1;

0x81 – 天线 2;

0x82 – 天线 3;

0x83 – 天线 4。

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。

ScanTime (可选参数)：1 个字节。本次命令查询时间。读写器将会把查询命令最大响应时间设置为 ScanTime*100ms。

注:

①当 **MaskMem**、**MaskAdr**、**MaskLen**、**MaskData** 为空时表示无掩膜条件。

②**Target**、**Ant**、**ScanTime** 为可选参数，命令中必须同时带有这三个参数或同时不带这三个参数。当命令中没有带这三个参数时，设备使用预先设定的 **Target**、**Ant**、**ScanTime** 参数查询标签；当命令中带有这三个参数时，设备使用这三个指定的参数值查询标签。

(1) 当应答状态 Status 为 0x26 时，应答如下：

Len	Adr	reCmd	Status	Data[]			CRC-16
				Ant	ReadRate	TotalCount	

0xXX	0xXX	0x19	0xXX	0xXX	2Bytes	4Bytes	LSB	MSB
------	------	------	------	------	--------	--------	-----	-----

参数解析：

Status 是应答的状态，其代表的意义如下表所述：

Status	说明
0x26	查询结束后，返回本次查询的统计数据。

参数解析：

Ant: 表示有哪些天线查询到该标签。如 0x04，二进制为 0000 0100，表示天线 3 查询到该标签；如 0x08，二进制为 0000 1000，表示天线 4 查询到该标签。

ReadRate: 此次执行命令的标签识别速度(成功读取标签的次数/秒)。不区分是否多次读取同一张标签。

TotalCount: 此次执行命令的总读取标签次数，不区分是否多次读取同一张标签。

(2) 当应答状态 Status 为除 0x26 以外的状态时，应答如下：

Len	Adr	reCmd	Status	Data[]			CRC-16
				Ant	Num	Data Packet	
0xXX	0xXX	0x19	0xXX	0xXX	0xXX	Packet-1, Packet-2, Packet-3...	LSB MSB

参数解析：

Status 是应答的状态，其代表的意义如下表所述：

Status	说明
0x01	命令执行结束，同时返回查询到的电子标签数据
0x02	查询时间结束，命令执行强制退出，同时返回已查询到的标签数据
0x03	如果读到的标签数量无法在一条消息内传送完，将分多次发送。如果 Status 为 0x03，则表示这条数据结束后，还有数据。
0x04	还有电子标签未读取，电子标签数量太多，读写器的存储区已满，返回此状态值，同时返回已查询到得电子标签数据。
0xF8	天线连接检测错误，当前天线连接可能已经断开。

Ant: 表示有哪些天线查询到该标签。如 0x04，二进制为 0000 0100，表示天线 3 查询到该标签；如 0x08，二进制为 0000 1000，表示天线 4 查询到该标签。

Num: 本次应答中包含的电子标签信息的数据包的个数。

Data Packet: 读到的电子标签的数据，Packet-1 是第 1 个数据包数据，Packet-2 是第 2 个数据包数据，依此类推。每个 Packet 数据包格式如下：

Packet			
PacketParam	Len	Data	RSSI

0xXX	0xXX	变长	0xXX
------	------	----	------

数据包参数解析：

PacketParam: 数据包参数，1个字节。

Bit7: 数据包类型标志。

0 – 本数据包所带信息为标签 EPC 号；

1 – 本数据包所带信息为读取到的数据（读到数据的标签为上一包 EPC 号的标签）。

Bit6~Bit0: 数据包序号。数据包序号范围从 0~127。每执行一次混合查询，数据包序号都会重新从 0 开始，每上传一个数据包，数据包序号会自动加 1，当数据包序号超过 127，会重新从 0 开始。

Len: 1 个字节，本数据包所带数据 Data 的长度。

Data: 电子标签的 EPC 号或读取到的指定区域数据。数据以高字(EPC C1 G2 中数据以字为单位)在前，每一个字的高字节在前。

RSSI: 一个字节，读写器读取到该标签时的信号强度。

注：数据包根据读写器读到 EPC/数据的顺序上传，对于同一个标签，读写器先上传一个 EPC 号包，再上传一个读到数据的包，这两个包的序列号是连续的。

如果一个标签在上传 EPC 号后，因各种原因无法读取到指定的数据，则不会上传读到数据的包，读写器会继续查询下一个标签，然后直接上传下一个标签的 EPC 号包。

8.2.22 指定 EPC 号查询

该命令用于查询指定 EPC 号内容的标签。本命令只返回符合指定匹配条件的标签 EPC 号，不符合匹配条件的标签 EPC 号将不会返回。

命令如下：

Len	Adr	Cmd	Data[]	CRC-16	
0xXX	0xXX	0x1a	——	LSB	MSB

Data 参数如下：

Data[]			
MatchType	MatchLen	MatchOffset	EPCData
0xXX	2 Bytes	2 Bytes	变长

参数解析：

MatchType: 匹配 EPC 号类型。

0 – 查询 EPC 号与指定匹配数据完全相同的标签。

1 – 查询 EPC 号与指定匹配数据不同的标签。

其它值保留，如果为其它值将返回参数错误信息。

MatchLen: 两个字节, 高字节在前。要匹配的 EPC 数据的长度(单位: Bits)。参数范围 1 ~ 496 bits。

MatchOffset: 两个字节, 高字节在前。要匹配 EPC 号的起始位地址(单位: Bits)。参数范围 0 ~ 495 bits。

EPCData: 要指定匹配的标签 EPC 号数据。EPCData 数据字节长度是 MatchLen/8。如果 MatchLen 不是 8 的整数倍, 则 EPCData 数据字节长度为[MatchLen/8]取整再加 1。不够的在低位补 0。

注: **MatchLen** 与 **MatchOffset** 之和不能超过 496 bits, 否则返回参数错误消息。

应答:

Len	Adr	reCmd	Status	Data[]			CRC-16	
				Ant	Num	EPC ID		
0xXX	0xXX	0x1a	0xXX	0xXX	0xXX	EPC-1	LSB	MSB

参数解析:

Status 是应答的状态, 其代表的意义如下表所述:

Status	说明
0x01	命令执行结束, 同时返回查询到的电子标签数据
0x02	查询时间结束, 命令执行强制退出, 同时返回已查询到的标签数据
0x03	如果读到的标签数量无法在一条消息内传送完, 将分多次发送。如果 Status 为 0x03, 则表示这条数据结束后, 还有数据。
0xF8	天线连接检测错误, 当前天线连接可能已经断开。

Ant: 表示有哪些天线查询到该标签。如 0x04, 二进制为 0000 0100, 表示天线 3 查询到该标签; 如 0x08, 二进制为 0000 1000, 表示天线 4 查询到该标签。

Num: 本次应答中包含的电子标签的 EPC 的个数。

EPC ID: 读到的电子标签的 EPC 数据, EPC-1 是第一张标签的 **EPC 长度**+第一张标签的 EPC 号+第一张标签的 **RSSI 值**。电子标签 EPC 号高字(EPC C1 G2 中数据以字为单位)在前, 每一个字的高字节在前。 **EPC 长度**以一个字节表示。 **RSSI 值**长度以一个字节表示。

8.2.23 QT 查询

本命令用于获取公开镜像的 Monza4QT 标签的私有 EPC 号。

查询命令的作用是检查有效范围内是否有符合协议的电子标签存在。想要对未知 EPC 的

新标签进行别的操作，应先通过查询命令来得到标签的 EPC 号。

在运行查询命令之前，用户可以根据需要先设定好该命令的最大运行时间(查询时间)。读写器在查询时间规定的范围内必须给上位机一个结果，如果读写器尚未读完有效范围内的所有标签，而查询时间已到，则读写器不再查询其它标签，而是直接把已经查询到得标签返回给上位机，并提示上位机还有标签未读完。然后等待下一个命令。

查询时间的缺省值是 1s，用户可以通过运行读写器自定义命令设定查询时间命令来修改。允许的范围是：3*100ms~255*100ms(实际的响应时间可能会比设定的值大 0~75ms)。

查询时间如果设定的过短，可能会出现在规定时间内查询不到电子标签的情况。

命令：

Len	Adr	Cmd	Data[]	CRC-16	
0x0XX	0xXX	0x1b	——	LSB	MSB

Data 参数如下：

Data[]				
QValue	Session	Target	Ant	Scantime
0xXX	0xXX	0xXX	0xXX	0xXX

参数解析：

QValue：1 个字节。

bit7：统计数据包标志。

0 – 询问结束后，不发送统计数据包；

1 – 询问结束后，发送统计数据包。

bit6~bit0：询问 EPC 标签时使用的初始 Q 值，Q 值的设置应为场内的标签数量约等于 2^Q 。Q 值的范围为 0~15，若命令中出现了其它值，将返回参数出错的消息。

Session：1 个字节，询问 EPC 标签时使用的 Session 值。

0x00：Session 使用 S0；

0x01：Session 使用 S1；

0x02：Session 使用 S2；

0x03：Session 使用 S3。

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。

Target (可选参数)：1 个字节，询问 EPC 标签时使用的 Target 值。

0x00：Target 值使用 A。

0x01：Target 值使用 B。

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。

Ant (可选参数)：1 个字节，本次要进行询问的天线号。

0x80 – 天线 1；

0x81 – 天线 2;
0x82 – 天线 3;
0x83 – 天线 4。

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。

ScanTime (可选参数): 1 个字节。本次命令查询时间。读写器将会把查询命令最大响应时间设置为 ScanTime*100ms。

注:

①**Target**、**Ant**、**ScanTime** 为可选参数，命令中必须同时带有这三个参数或同时不带这三个参数。当命令中没有带这三个参数时，设备使用预先设定的 **Target**、**Ant**、**ScanTime** 参数查询标签；当命令中带有这三个参数时，设备使用这三个指定的参数值查询标签。

(1) 当应答状态 Status 为 0x26 时，应答如下:

Len	Adr	reCmd	Status	Data[]			CRC-16	
				Ant	ReadRate	TotalCount		
0xXX	0xXX	0x1b	0xXX	0xXX	2Bytes	4Bytes	LSB	MSB

参数解析:

Status 是应答的状态，其代表的意义如下表所述:

Status	说明
0x26	查询结束后，返回本次查询的统计数据。

Ant: 表示有哪些天线查询到该标签。如 0x04，二进制为 0000 0100，表示天线 3 查询到该标签；如 0x08，二进制为 0000 1000，表示天线 4 查询到该标签。

ReadRate: 此次执行命令的标签识别速度(成功读取标签的次数/秒)。不区分是否多次读取同一张标签。

TotalCount: 此次执行命令的总读取标签次数，不区分是否多次读取同一张标签。

(2) 当应答状态 Status 为除 0x26 以外的状态时，应答如下:

Len	Adr	reCmd	Status	Data[]			CRC-16	
				Ant	Num	EPC ID		
0xXX	0xXX	0x1b	0xXX	0xXX	0xXX	EPC-1, EPC-2, EPC-3...	LSB	MSB

参数解析:

Status 是应答的状态，其代表的意义如下表所述:

Status	说明
0x01	命令执行结束，同时返回查询到的电子标签数据

0x02	查询时间结束, 命令执行强制退出, 同时返回已查询到的标签数据
0x03	如果读到的标签数量无法在一条消息内传送完, 将分多次发送。如果 Status 为 0x03, 则表示这条数据结束后, 还有数据。
0x04	还有电子标签未读取, 电子标签数量太多, 读写器的存储区已满, 返回此状态值, 同时返回已查询到得电子标签数据。

Ant: 表示有哪些天线查询到该标签。如 0x04, 二进制为 0000 0100, 表示天线 3 查询到该标签; 如 0x08, 二进制为 0000 1000, 表示天线 4 查询到该标签。

Num: 本条命令中包含的电子标签的 EPC 的个数。

EPC ID: 读到的电子标签的 EPC 数据, EPC-1 是第一张标签的 **EPC 长度**+第一张标签的 EPC 号+第一张标签的 **RSSI 值**, 依此类推。每个电子标签 EPC 号数据高字(EPC C1 G2 中数据以字为单位)在前, 每一个字的高字节在前。**EPC 长度**以一个字节表示。**RSSI 值**长度以一个字节表示。

8.3 18000-6B 命令

8.3.1 寻查命令(单张)

本命令只能查询单张电子标签。如果多张标签同时处于天线有效范围内, 可能无法查询到电子标签。

命令:

Len	Adr	Cmd	CRC-16	
0x04	0xXX	0x50	LSB	MSB

应答:

Len	Adr	reCmd	Status	Data[]		CRC-16	
				Ant	ID		
0x10	0xXX	0x50	0x00	0Xxx	10 Byte	LSB	MSB

参数解析:

Ant: 表示有哪些天线查询到该标签。如 0x04, 二进制为 0000 0100, 表示天线 3 查询到该标签; 如 0x08, 二进制为 0000 1000, 表示天线 4 查询到该标签。

ID: 10 个字节。第 1 个字节是 UID 长度, 为 0x08。第 2~9 个字节为标签的 UID 号, 低字节在前。第 10 个字节是 **RSSI 值**。

8.3.2 按条件寻查标签

本命令按照给定的条件查询电子标签。

命令：

Len	Adr	Cmd	Data[]				CRC-16	
			Condition	Address	Mask	Word_data		
0x0f	0xXX	0x51	0xXX	0xXX	0xXX	8 Bytes	LSB	MSB

参数解析：

Condition: 选择标签的要求。0x00: 等于条件; 0x01: 不等于条件; 0x02: 大于条件; 0x03: 小于条件。

Address: 比较的起始字节地址。

Mask: 掩码。用来指定要比较的数据。

Word_data: 比较的条件，用来比较的数据。

Mask 的每一位对应 Word_data 的一个字节。Mask 的最高位(Bit7)对应 Word_data 的最左边的一个字节。Mask 的最低位 (Bit0)对应 Word_data 的最右边一字节。Word_data 是用来与标签中的数据进行比较的。Word_data 的最左边一字节与电子标签的 Address 地址上的数据进行比较，最右边一字节与 Address+7 地址上的数据进行比较。其它依此类推。Mask 相应位为 1，表示要把该位在 Word_data 中对应的字节与标签中对应的字节进行比较；为 0 则不比较。

应答：

Len	Adr	reCmd	Status	Ant	Num	Data[]	CRC-16	
0xXX	0xXX	0x51	0xXX	0xXX	0xXX	UID1, UID2...	LSB	

参数解析：

Status 是应答的状态，其代表的意义如下表所述：

Status	说明
0x15	命令执行结束，同时返回查询到的电子标签数据
0x16	查询时间结束，命令执行强制退出，同时返回已查询到的标签数据
0x17	如果读到的标签数量无法在一条消息内传送完，将分多次发送。如果 Status 为 0x17，则表示这条数据结束后，还有数据。
0x18	还有电子标签未读取，电子标签数量太多，读写器的存储区已满，返回此状态值，同时返回已查询到得电子标签数据。
0xF8	天线连接检测错误，当前天线连接可能已经断开。

参数解析：

Ant: 表示有哪些天线查询到该标签。如 0x04, 二进制为 0000 0100, 表示天线 3 查询到该标签；如 0x08, 二进制为 0000 1000, 表示天线 4 查询到该标签。

Num: 本次应答中包含的 UID 个数。

Data[]: 电子标签的 UID。每个 UID 是 10 个字节，第 1 个字节是 UID 长度，为 0x08。第 2~9 个字节为标签的 UID 号，低字节在前。第 10 个字节是 **RSSI 值**。当无 UID 时(即 Num 为 0 时) Data[] 为空。

8.3.3 读数据

该命令用来从电子标签的某个指定地址开始读若干个字节。

命令：

Len	Adr	Cmd	Data[]			CRC-16	
			Address	ID	Num		
0x0e	0xXX	0x52	0xXX	8 Bytes	0xXX	LSB	MSB

参数解析：

Address: 读数据的起始字节地址。地址范围为 0 ~ 223。如果地址超出 223，将返回参数错误信息。

Num: 要读的数据个数，以字节为单位。Num 的范围是 1 ~ 32。如果 Address+Num 大于 224、或是 Num 超过 32、或 Num 为 0，读写器将返回参数错误信息。

ID: 要读数据的电子标签的 ID。8 个字节，低字节在前。

应答：

Len	Adr	reCmd	Status	Data[]	CRC-16	
0xXX	0xXX	0x52	0x00	Data	LSB	MSB

参数解析：

Data: 读到的数据，低字节在前。

8.3.4 写数据

该命令向指定的电子标签写入若干个字节。

命令：

Len	Adr	Cmd	Data[]			CRC-16	
			Address	ID	Wdata		
0xXX	0xXX	0x53	0xXX	8 Bytes	变长	LSB	MSB

参数解析：

Address: 写入数据的起始地址。地址范围：8 ~ 223。地址如果超出范围，将返回参数错误信息。

ID: 要读数据的电子标签的 ID。8 个字节，低字节在前。

Wdata: 要写入的数据。Wdata 的长度限定在 32 个字节以内。Wdata 的高字节写在电子标签的低地址。如果命令中 Wdata 的长度为 0(即 Wdata 部分不存在)或超过 32，将返回参数错误信息。如果 Address 加 Wdata 的长度大于 224，也将返回参数错误信息。

应答：

Len	Adr	reCmd	Status	Data[]	CRC-16

0x05	0xXX	0x53	0x00	---	LSB	MSB
------	------	------	------	-----	-----	-----

8.3.5 锁定检测

该命令用来检测指定的字节是否锁定。

命令：

Len	Adr	Cmd	Data[]		CRC-16	
			Address	ID		
0x0d	0xXX	0x54	0xXX	8 Bytes	LSB	MSB

参数解析：

Address：要检测是否被锁定的字节的地址。范围：0 ~ 223。超过这个范围将返回参数错误信息。

ID：要读数据的电子标签的 ID。8 个字节，低字节在前。

应答：

Len	Adr	reCmd	Status	Data[]	CRC-16	
0x06	0xXX	0x54	0x00	LockState	LSB	MSB

参数解析：

LockState：

0x00：该字节未被锁定

0x01：该字节已经被锁定

8.3.6 锁定

该命令锁定指定的字节。

命令：

Len	Adr	Cmd	Data[]		CRC-16	
			Address	ID		
0x0d	0xXX	0x55	0xXX	8 Bytes	LSB	MSB

参数解析：

Address：要锁定的字节地址。范围：8 ~ 223。超过这个范围将返回参数错误信息。

ID：要读数据的电子标签的 ID。8 个字节，低字节在前。

应答：

Len	Adr	reCmd	Status	Data[]	CRC-16	
0x05	0xXX	0x55	0x00	---	LSB	MSB

8.4 读写模块自定义命令

8.4.1 读取读写器信息

上位机发送该命令给读写器，将获得读写器的信息，这其中包括读写器地址(Adr)、读写器软件版本(Version)、读写器类型代码、读写器协议支持信息、读写器的频率范围、读写器的功率、查询时间、天线检测参数等信息。

命令：

Len	Adr	Cmd	Data[]	CRC-16	
0x04	0xXX	0x21	——	LSB	MSB

应答：

Len	Adr	reCmd	Status	Data[]	CRC-16	
0x0f	0xXX	0x21	0x00	Version, Type, Tr_Type, dmaxfre, dminfre, Power, Scntm, Ant, Reserved, Reserved, CheckAnt	LSB	MSB

参数解析：

参数	长度(Byte)	说明
Version	2	版本号，高字节代表主版本号，低字节代表子版本号。
Type	1	读写器类型代号。0x20 代表 UHFReaderD840。
Tr_Type	1	读写器支持的协议信息，Bit1 为 1 表示支持 18000-6c 协议，Bit0 为 1 表示 18000-6B 协议，其它位保留。
dmaxfre	1	Bit7-Bit6 用于频段设置用；Bit5-Bit0 表示当前读写器工作的最大频点。
dminfre	1	Bit7-Bit6 用于频段设置用；Bit5-Bit0 表示当前读写器工作的最小频点。
Power	1	读写器的输出功率。范围是 0 到 30。
Scntm	1	查询时间。读写器收到查询命令后，在查询时间内，会给出上位机应答。
Ant	1	天线配置信息。
Reserved	1	保留。
Reserved	1	保留。
CheckAnt	1	天线检测参数。0-关闭读卡天线检测；1-打开读卡天线检测

频段设置如下表：

MaxFre(Bit7)	MaxFre(Bit6)	MinFre(Bit7)	MinFre(Bit6)	FreqBand
0	0	0	0	保留
0	0	0	1	Chinese band2
0	0	1	0	US band

0	0	1	1	Korean band
0	1	0	0	EU band
0	1	0	1	保留
0	1	1	0	Ukraine band
0	1	1	1	Peru band
1	0	0	0	Chinese band1
1	0	0	1	EU3 band
1	0	1	0	Taiwan band
1	1	0	0	US band3
...
1	1	1	1	保留

8.4.2 设置读写器工作频率

这个命令用来选择频段及各频段中的上限频点，下限频点。上限频点必须大于或等于下限频点。

命令：

Len	Adr	Cmd	Data[]		CRC-16	
			MaxFre	MinFre		
0x06	0xXX	0x22	0xXX	0xXX	LSB	MSB

参数解析：

MaxFre: 一个字节, Bit7-Bit6 用于频段设置用; Bit5-Bit0 表示读写器工作的最大频点。

MinFre: 一个字节, Bit7-Bit6 用于频段设置用; Bit5-Bit0 表示读写器工作的最小频点。最小频点必须小于等于最大频点。

频段设置如下表：

MaxFre(Bit7)	MaxFre(Bit6)	MinFre(Bit7)	MinFre(Bit6)	FreqBand
0	0	0	0	保留
0	0	0	1	Chinese band2
0	0	1	0	US band
0	0	1	1	Korean band
0	1	0	0	EU band
0	1	0	1	保留
0	1	1	0	Ukraine band
0	1	1	1	Peru band
1	0	0	0	Chinese band1
1	0	0	1	EU3 band
1	0	1	0	Taiwan band
1	1	0	0	US band3
...
1	1	1	1	保留

应答：

Len	Adr	reCmd	Status	Data[]	CRC-16
-----	-----	-------	--------	--------	--------

0x05	0xXX	0x22	0x00	—	LSB	MSB
------	------	------	------	---	-----	-----

设置的时候, 如果下限频点大于上限频点, 则会返回参数出错信息。

各频段计算公式:

Chinese band2:	$F_s = 920.125 + N * 0.25$ (MHz) 其中 $N \in [0, 19]$ 。
US band:	$F_s = 902.75 + N * 0.5$ (MHz) 其中 $N \in [0, 49]$ 。
Korean band:	$F_s = 917.1 + N * 0.2$ (MHz) 其中 $N \in [0, 31]$ 。
EU band:	$F_s = 865.1 + N * 0.2$ (MHz) 其中 $N \in [0, 14]$ 。
Ukraine band:	$F_s = 868.0 + N * 0.1$ (MHz) 其中 $N \in [0, 6]$ 。
Peru band:	$F_s = 916.2 + N * 0.9$ (MHz) 其中 $N \in [0, 11]$ 。
Chinese band1:	$F_s = 840.125 + N * 0.25$ (MHz) 其中 $N \in [0, 19]$ 。
EU3 band:	$F_s = 865.7 + N * 0.6$ (MHz) 其中 $N \in [0, 3]$ 。
US band3:	$F_s = 902 + N * 0.5$ (MHz) 其中 $N \in [0, 52]$ 。
Taiwan band:	$F_s = 922.25 + N * 0.5$ (MHz) 其中 $N \in [0, 11]$ 。

8.4.3 设置读写模块地址

命令:

Len	Adr	Cmd	Data[]	CRC-16	
			address		
0x05	0xXX	0x24	0xXX	LSB	MSB

参数解析:

address: 要设置的新的读写模块地址。本条命令使用原来的地址应答。这个地址不能为0xFF。如果设置为0xFF, 则读写模块将返回参数出错信息。

应答:

Len	Adr	reCmd	Status	Data[]	CRC-16	
0x05	0xXX	0x24	0x00	—	LSB	MSB

8.4.4 设置读写模块查询时间

命令:

Len	Adr	Cmd	Data[]	CRC-16	
0x05	0xXX	0x25	Scantime 0xXX	LSB	MSB

参数解析:

Scantime: 查询时间。读写器将会把查询命令最大响应时间改为用户给定的值(0*100ms~255*100ms), 以后将使用此项新的查询命令最大响应时间。出厂时缺省值是0x14(对应的时间为20*100ms)。用户修改范围是0x00~0xff(对应时间是0*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时, 读写器查询命

令的最大响应时间无上限，查询命令直到查询完所有标签才会退出。

应答：

Len	Adr	reCmd	Status	Data[]	CRC-16	
0x05	0xXX	0x25	0x00	—	LSB	MSB

8.4.5 设置串口波特率

此命令用来更改读写模块的串口波特率。

命令：

Len	Adr	Cmd	Data[]	CRC-16	
0x05	0xXX	0x28	baudrate	LSB	MSB
			0xXX		

参数解析：

baudrate: 新的波特率，波特率默认为 57600。Baudrate 的范值是 0/1/2/5/6。其它值保留。其对应的波特率为：

baudrate	实际波特率
0	9600bps
1	19200 bps
2	38400 bps
5	57600 bps
6	115200 bps

应答：

Len	Adr	reCmd	Status	Data[]	CRC-16	
0x05	0xXX	0x28	0x00	—	LSB	MSB

需要特别注意的是，本次传送应答数据所用的波特率还是原来的波特率。从下一次发命令开始，使用新的波特率。

8.4.6 调整功率

该命令设置读写模块功率。范围是 0~30，取值 30 时约为 1W 的输出功率。

命令：

Len	Adr	Cmd	Data[]	CRC-16	
0x05	0xXX	0x2F	Pwr	LSB	MSB
			0xXX		

Pwr: 功率参数，1 个字节。

Bit0~Bit6: 要设定的功率参数，范围是 0~30，取值 30 时约为 1W 的输出功率。

Bit7: 表示本次配置是否掉电保存。Bit7=0 掉电保存；Bit7=1 掉电不保存。

应答：

Len	Adr	reCmd	Status	Data[]	CRC-16	
0x05	0xXX	0x2F	0x00	—	LSB	MSB

8.4.7 声光控制命令

该命令用来控制 LED 灯和蜂鸣器（与 GPO1 引脚复用）按一定规律闪烁和鸣叫。

命令：

Len	Adr	Cmd	Data[]			CRC-16	
			ActiveT	SilentT	Times		
0x07	0xXX	0x33	0xXX	0xXX	0xXX	LSB	MSB

参数解析：

ActiveT： LED 灯亮和蜂鸣器鸣叫 (GPO1 引脚低电平) 时间(ActiveT*50ms)，默认值为零。
0<=ActiveT<=255。

SilentT： LED 灯和蜂鸣器静默 (GPO1 引脚高电平) 时间(SilentT *50ms)，默认值为零。0<=SilentT <=255。

Times： LED 灯亮和蜂鸣器鸣叫次数(0<=Times<=255) 默认值为零。

应答：

Len	Adr	reCmd	Status	Data[]	CRC-16	
0x05	0xXX	0x33	0x00	——	LSB	MSB

8.4.8 配置天线

该命令用于设置读写器天线配置。

命令：

Len	Adr	Cmd	Data[]		CRC-16	
			Ant			
0x05	0xXX	0x3f	0xXX	LSB	MSB	

Ant： 天线配置信息。天线至少要配置一个。

Bit0： 天线 1 配置位。Bit0=0 天线 1 关闭； Bit0=1 天线 1 打开。

Bit1： 天线 2 配置位。Bit1=0 天线 2 关闭； Bit1=1 天线 2 打开。

Bit2： 天线 3 配置位。Bit2=0 天线 3 关闭； Bit2=1 天线 3 打开。

Bit3： 天线 4 配置位。Bit3=0 天线 4 关闭； Bit3=1 天线 4 打开。

Bit4~Bit6： 保留， 默认值为 0。

Bit7： 表示本次配置是否掉电保存。Bit7=0 掉电保存； Bit7=1 掉电不保存。

应答：

Len	Adr	reCmd	Status	Data[]	CRC-16	
0x05	0xXX	0x3f	0x00	——	LSB	MSB

8.4.9 蜂鸣器设置

该命令用于设置蜂鸣器（与 GPO1 引脚复用）开关。

命令：

Len	Adr	Cmd	Data[]	CRC-16	
			BeepEn		
0x05	0xXX	0x40	0Xxx	LSB	MSB

BeepEn: Bit0=0 时蜂鸣器关。

Bit0=1 时蜂鸣器开，当读写器对标签操作成功有提示音（GPO1 引脚输出低脉冲）。

Bit1~Bit7 位保留，默认值 0。

应答：

Len	Adr	reCmd	Status	Data[]	CRC-16	
0x05	0xXX	0x40	0x00	——	LSB	MSB

8.4.10 GPIO 控制命令

该命令用于控制通用 GPIO 口输出， 默认输出为高电平。

命令：

Len	Adr	Cmd	Data[]	CRC-16	
			OutputPin		
0x05	0xXX	0x46	0xXX	LSB	MSB

OutputPin: GPIO 口(Out1-Out2 引脚)输出状态。Bit0-Bit1 分别控制 Out1-Out2 引脚，Bit2-Bit7 保留。

应答：

Len	Adr	reCmd	Status	Data[]	CRC-16	
0x05	0xXX	0x46	0x00	——	LSB	MSB

8.4.11 读取 GPIO 状态

该命令用于获取 GPIO 口输出状态。

命令：

Len	Adr	Cmd	Data[]	CRC-16	
0x04	0xXX	0x47	---	LSB	MSB

应答：

Len	Adr	reCmd	Status	Data[]	CRC-16	
				OutputPin		
0x06	0xXX	0x47	0x00	0xXX	LSB	MSB

OutputPin: GPIO 口输出状态。Bit0 代表 IN1 引脚状态, Bit4-Bit5 分别代表 Out1-Out2 状态, 其他位保留。

8.4.12 读写器唯一序列号获取

该命令用于读取读写器唯一序列号信息。

命令：

Len	Adr	Cmd	Data[]		CRC-16	
0x04	0xXX	0x4c	---		LSB	MSB

应答：

Len	Adr	reCmd	Status	Data[]	CRC-16	
				SeriaNo		
0x09	0xXX	0x4c	0x00	4bytes	LSB	MSB

参数解析：

SeriaNo：读写器唯一序列号。4 个字节数据。

8.4.13 标签自定义功能设置

该命令用于设置读写器启动某些类型标签的自定义工作机制，以实现标签特定功能。

命令：

Len	Adr	Cmd	Data[]	CRC-16	
			InlayType		
0x05	0xXX	0x3a	0xXX	LSB	MSB

InlayType：标签类型，取值范围 0~254。

默认值为 0，表示不指定标签类型。

取值 1 为启动 Monza4QT 标签的 Peek 功能（标签状态临时从 public 转换到

private)，它将影响标签的读数据、写数据、块写数据、写保护字和写 EPC 号等操作。

应答：

Len	Adr	reCmd	Status	Data[]	CRC-16	
0x06	0xXX	0x3a	0x00	InlayType	LSB	MSB

InlayType：标签类型，取值范围 0~254。

8.4.14 设置天线检测

该命令用于设置读写标签的过程中是否进行天线检测。

命令如下：

Len	Adr	Cmd	Data[]	CRC-16		
			CheckAnt			
0x05	0xXX	0x66	0xXX	LSB	MSB	

参数解析：

CheckAnt：1 个字节，天线检测开关。

0x00：关闭读写标签过程中的天线检测。

0x01：开启读写标签过程中的天线检测。

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。

应答：

Len	Adr	reCmd	Status	Data[]	CRC-16	
0x05	0xXX	0x66	0x00	——	LSB	MSB

8.4.15 设置通信接口

该命令用于设置 UHFReaderD840 与上位机的通信接口，接口参数掉电不丢失。通信接口只能使用其中一个，连接读写器时需要根据设备当前的通信接口设置使用相应的接口连接。

命令如下：

Len	Adr	Cmd	Data[]	CRC-16		
			CommType			
0x05	0xXX	0x6A	0xXX	LSB	MSB	

参数解析：

CommType：1 个字节。通信接口类型。

0x00：通信接口为 USB 口。

0x01：通信接口为 UART 口。

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。

注意：①当设置为 USB 口时，UART 口不可用；当设置为 UART 口时，USB 口不可用。②更改通信接口后读写器需要重新上电，新的接口才生效。

应答：

Len	Adr	reCmd	Status	Data[]	CRC-16	
0x05	0xXX	0x6A	0x00	——	LSB	MSB

0x05	0xXX	0x6A	0x00	—	LSB	MSB
------	------	------	------	---	-----	-----

8.4.16 天线检测回损设置/读取命令

该命令用于设置或读取内部进行天线检测时的回损阈值。回损阈值默认为-6dB，该参数掉电不丢失。

命令：

Len	Adr	Cmd	Data[]	CRC-16	
			ReturnLoss		
0x05	0xXX	0x6e	0xXX	LSB	MSB

参数解析：

ReturnLoss：天线检测回损设置/读取参数。

Bit7：读取/设置天线检测回损标志。

0 – 读取天线检测回损阈值；

1 – 设置天线检测回损阈值。

Bit6~Bit0：天线检测回损阈值。

如果 Bit7=0，Bit6~Bit0 将被忽略；

如果 Bit7=1，Bit6~Bit0 为要设置的天线检测回损阈值。参数范围 0~20，分别表示回损阈值为 0dB ~ -20dB。

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。

应答：

Len	Adr	reCmd	Status	Data[]	CRC-16	
				ReturnLoss		
0x06	0xXX	0x6e	0x00	0xXX	LSB	MSB

参数解析：

ReturnLoss：读写器当前天线检测回损阈值。

Bit7：保留，默认值为 0。

Bit6~Bit0：读写器当前天线检测回损阈值。参数范围 0~20。

8.4.17 设置缓存的 EPC/TID 长度

该命令用于设置带缓存查询时存储的 EPC/TID 最大长度。如果当前缓存中有标签数据时，设置长度后缓存中的数据将被清空。

命令：

Len	Adr	Cmd	Data[]	CRC-16	
			SaveLen		
0x05	0xXX	0x70	0xXX	LSB	MSB

SaveLen：1 个字节，规定缓存 EPC/TID 的最大长度。取值 0 时为 128bit 长度，即 16 个字节，对应的最大缓存标签数量为 528 张。取值 1 时为 496bit 长度，即 62 个字节，对应的最大缓存标签数量为 160 张。

应答：

Len	Adr	reCmd	Status	Data[]	CRC-16	
0x05	0xXX	0x70	0x00	——	LSB	MSB

8.4.18 获取缓存的 EPC/TID 长度

该命令用于获取带缓存查询时存储的 EPC/TID 最大长度。

命令：

Len	Adr	Cmd	Data[]	CRC-16	
0x04	0xXX	0x71	——	LSB	MSB

应答：

Len	Adr	reCmd	Status	Data[]	CRC-16	
0x06	0xXX	0x71	0x00	SaveLen	LSB	MSB

SaveLen: 1 个字节, 规定缓存 EPC/TID 的最大长度。取值 0 时为 128bit 长度, 即 16 个字节。取值 1 时为 496bit 长度, 即 62 个字节。

8.4.19 缓存数据获取

该命令用于获取读写器存储区中所有标签信息。响应完成后, 缓存中的数据并不丢失, 可以多次提取。若运行 8.2.1 “查询标签” 命令, 缓存中的数据将被清空。

命令：

Len	Adr	Cmd	Data[]	CRC-16	
0x04	0xXX	0x72	——	LSB	MSB

应答：

Len	Adr	reCmd	Status	Data[]		CRC-16	
				Num	EPC Data		
0xXX	0xXX	0x72	0xXX	0xXX	EPC-1, EPC-2, ... EPC-n	LSB	MSB

Status 是应答的状态, 其代表的意义如下表所述:

Status	说明
0x01	此次应答结束, 数据全部返回。
0x03	如果缓存的标签数据无法在一条消息内传送完, 将分多次发送。如果 Status 为 0x03, 则表示这条数据结束后, 还有数据。

参数解析:

Num: 1 个字节, 本响应帧中包含的电子标签的 EPC/TID 的个数。

EPC Data: 缓存中电子标签的 EPC/TID 数据。

EPC-n				
Ant	Len	EPC/TID	RSSI	Count
0xXX	0xXX	nBytes	0xXX	0xXX

Ant: 1 个字节, 表示有哪些天线查询到该标签。如 5, 二进制为 0101, 表示天线 1 和 3 查询到该标签。

Len: 1 个字节, 标签的 EPC/TID 字节长度。

EPC/TID: 标签的 EPC 号或 TID 数据, 长度和 Len 规定的相同。每个电子标签 EPC 号或 TID 数据高字(EPC C1 G2 中数据以字为单位)在前, 每一个字的高字节在前。

RSSI: 1 个字节, 第一次读到该标签时的信号强度。

Count: 1 个字节, 该标签成功读取的次数, 取值 0xFF 时表示次数大于等于 255 次。

8.4.20 清缓存

该命令用于清空读写器存储区中所有标签信息。

命令:

Len	Adr	Cmd	Data[]	CRC-16	
0x04	0xXX	0x73	——	LSB	MSB

应答:

Len	Adr	reCmd	Status	Data[]	CRC-16	
0x05	0xXX	0x73	0x00	——	LSB	MSB

8.4.21 查询缓存区标签数量

该命令用于获取缓存区中的标签数量。

命令:

Len	Adr	Cmd	Data[]	CRC-16	
0x04	0xXX	0x74	——	LSB	MSB

应答:

Len	Adr	reCmd	Status	Data[]	CRC-16	
				Count		
0x07	0xXX	0x74	0x00	2bytes	LSB	MSB

Count: 2 个字节, 缓存区中的标签数量, 高字节在前。

8.4.22 设置实时查询参数

该命令用于设置读写器进入自动实时查询模式后所使用的查询参数。

命令:

Len	Adr	Cmd	Data[]	CRC-16	
0xXX	0xXX	0x75	——	LSB	MSB

Data 参数如下：

Data[]					
TagProtocol	ReadPauseTime	FliterTime	QValue	Session	
0xXX	0xXX	0xXX	0xXX	0xXX	

Data[]					
MaskMem	MaskAdr	MaskLen	MaskData	AdrTID	LenTID
0xXX	2Bytes	0xXX	变长	0xXX	0xXX

参数解析：

TagProtocol: 1 个字节，自动实时查询的标签类型。若命令中出现了其它值，将返回参数出错的消息。

0 – EPC C1G2 (ISO18000-6C) 标签。

1 – ISO18000-6B 标签。

当 标 签 类 型 设 置 为 6B 时，
QValue、Session、MaskMem、MaskAdr、MaskLen、MaskData、AdrTID、LenTID 参数将被忽略。

ReadPauseTime: 1 个字节，读写器自动实时查询标签的间隔时间。

0x00 – 10ms;

0x01 – 20ms;

0x02 – 30ms;

0x03 – 50ms;

0x04 – 100ms。

若命令中出现了其它值，将返回参数出错的消息。

FliterTime: 1 个字节，标签过滤时间。以 1s 为单位，参数范围 0~255s。本参数表示，在自动实时查询模式下，读写器在过滤时间内如果多次读到同一个标签，只会上传一次。如果该参数为 0，则表示不启用标签过滤功能。

QValue: 1 个字节。

bit7: 保留，置 0。

bit6: 策略选择标志。

0 – 通用策略；

1 – 特殊策略。

bit5~bit0: 查询 EPC 标签时使用的初始 Q 值。Q 值的设置应为场内的标签数量约等于 2^Q 。Q 值的范围为 0~15，若命令中出现了其它值，将返回参数出错的消息。

Session: 1 个字节, 询问 EPC 标签时使用的 Session 值。

0x00: Session 使用 S0;

0x01: Session 使用 S1;

0x02: Session 使用 S2;

0x03: Session 使用 S3。

0xff: 读写器自动配置 Session (仅对 EPC 询问有效)。

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, 掩码区。0x01: EPC 存储区; 0x02: TID 存储区; 0x03: 用户存储区。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。

MaskAdr: 两个字节, 掩码的起始位地址 (单位: Bits)。范围 0~16383。

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。

AdrTID: 询问 TID 区的起始字地址。命令中有此参数和 LenTID 时表示询问的是 TID 而不是 EPC 号。

LenTID: 询问 TID 区的数据字数。LenTID 取值为 0~15, 若为其它参数将返回参数错误信息。命令中有此参数和 AdrTID 时表示询问的是 TID 而不是 EPC 号。

注:

①当 MaskMem、MaskAdr、MaskLen、MaskData 为空时表示无掩膜条件。

②自动查询模式下, 读写器会按照预先设置的天线、查询时间参数来进行查询。

应答:

Len	Adr	reCmd	Status	Data[]	CRC-16	
0x05	0xXX	0x75	0x00	---	LSB	MSB

8.4.23 设置工作模式

上位机发送该命令改变读写器的工作模式。

命令:

Len	Adr	Cmd	Data[]	CRC-16	
			ReadMode		
0x05	0xXX	0x76	0xXX	LSB	MSB

参数解析:

ReadMode: 读写器当前工作模式。

0 – 应答模式。

1 – 自动实时查询模式。

2 – 带触发的自动实时查询模式(触发模式)。此模式下,当 GPI1 口的电平为低电平时,读写器才进行自动查询, GPI1 口电平为高电平时,读写器处于待机模式。

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。

应答:

Len	Adr	reCmd	Status	Data[]	CRC-16	
0x05	0xXX	0x76	0x00	—	LSB	MSB

注: 本命令设置的工作模式掉电不丢失,即重新上电时会继续运行上次所设置的工作模式

自动实时查询模式下端口输出格式说明:

当读写器被设置为自动实时查询模式后,将按照预先设定的参数自动读取标签。

当读写器读到一个标签并符合过滤条件时,将主动向上位发送以下格式的数据:

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

Status 是应答的状态,其代表的意义如下表所述:

Status	说明
0x00	读到符合条件的标签,同时返回查询到的电子标签数据
0x28	心跳包时间间隔内没有读到符合条件的标签,上传心跳包数据

(1) 当应答状态为 0x00 时, Data 参数如下:

Data[]			
Ant	Len	EPC/TID	RSSI
0xXX	0xXX	nBytes	0xXX

参数解析:

Ant: 1 个字节, 表示有哪些天线查询到该标签。如 5, 二进制为 0101, 表示天线 1 和 3 查询到该标签。

Len: 1 个字节, 标签的 EPC/TID 字节长度。

EPC/TID: 标签的 EPC 号或 TID 数据, 长度和 Len 规定的相同。每个电子标签 EPC 号或 TID 数据高字(EPC C1 G2 中数据以字为单位)在前, 每一个字的高字节在前。

RSSI: 1 个字节, 第一次读到该标签时的信号强度。

(2) 当应答状态为 0x28 时, Data 参数如下:

Data[]		
PacketNo	AntStatus	TotalCount
4Bytes	4Bytes	4Bytes

参数解析：

PacketNo：心跳包序号。4个字节，高字节在前。

读写器每向上发送一次心跳包，心跳包序号自动加1。如果心跳包序号超出4字节范围，序号将回0并重新开始累加。

AntStatus：当前4个天线的状态，按字节先后顺序分别为天线1～天线4的状态字节。天线状态字节定义如下：

0x00 – 对应天线未被设置为有效查询天线；

0x01 – 对应天线正常连接；

0x02 – 对应天线已经断开。

其他值保留。

TotalCount：本次进入自动实时查询模式后读取标签的总次数，不区分是否多次读取同一张标签。长度为4个字节，高字节在前。

如果读取标签的总次数超出4字节范围，计数将回0并重新开始计数。

注：读写器在自动实时查询模式下，将只响应上位机发来的 8.4.1（读取读写器信息）、8.4.22（设置工作模式）和 8.4.23（读取工作模式参数）等三条命令。

8.4.24 读取工作模式参数

该命令用于读取工作模式参数。

命令：

Len	Adr	Cmd	Data[]	CRC-16	
0x04	0xXX	0x77	——	LSB	MSB

应答：

Len	Adr	reCmd	Status	Data[]	CRC-16	
0xXX	0xXX	0x77	0x00	ReadMode, TagProtocol, ReadPauseTime, FliterTime, QValue, Session, MaskMem, MaskAdr, MaskLen, MaskData, AdrTID, LenTID	LSB	MSB

参数解析：

ReadMode：1个字节，读写器当前工作模式。

TagProtocol: 1 个字节, 自动查询模式的标签类型。

ReadPauseTime: 1 个字节, 读写器自动查询标签的间隔时间。

FliterTime: 1 个字节, 自动查询模式的标签过滤时间。

QValue: 1 个字节。

bit7: 保留。

bit6: 策略选择标志。

0 – 通用策略;

1 – 特殊策略。

bit5~bit0: 自动查询 EPC 标签时使用的初始 Q 值。

Session: 1 个字节, 自动查询 EPC 标签时使用的 Session 值。

MaskMem、**MaskAdr**、**MaskLen**、**MaskData**: 自动查询模式下读写器查询 EPC C1G2 标签掩码条件参数。其中 **MaskMem** 为一个字节; **MaskAdr** 为两个字节, 高字节在前; **MaskLen** 为一个字节; **MaskData** 固定为 32 个字节, 超过 **MaskLen** 指示的内容为零。

AdrTID: 自动查询 TID 区的起始字地址。

LenTID: 自动查询 TID 区的数据字数。

8.4.25 读取/设置实时查询心跳包时间

该命令用于设置读写器进入自动实时查询模式后, 主动向上发送心跳包的时间间隔。心跳包时间间隔默认值为 0, 即不发送心跳包。

命令:

Len	Adr	Cmd	Data[]	CRC-16	
			HeartBeatTime	LSB	MSB
0x05	0xXX	0x78	0xXX		

参数解析:

HeartBeatTime: 心跳包时间间隔参数。

Bit7: 读取/设置心跳包时间间隔标志。

0 – 读取心跳包时间间隔;

1 – 设置心跳包时间间隔。

Bit6~Bit0: 心跳包时间间隔。

如果 Bit7=0, Bit6~Bit0 将被忽略;

如果 Bit7=1, Bit6~Bit0 为自动实时查询模式下, 读写器上传心跳包的时间间隔。以 30 秒为单位, 参数范围 0 秒~ 127×30 秒。

如果心跳包时间间隔设置为 0, 则在自动实时查询模式下, 读写器将不上传心跳包。

应答：

Len	Adr	reCmd	Status	Data[]	CRC-16	
				HeartBeatTime		
0x06	0xXX	0x78	0x00	0xXX	LSB	MSB

参数解析：

HeartBeatTime：当前读写器心跳包时间间隔。

Bit7：保留，默认值为0。

Bit6~Bit0：当前读写器上传心跳包的时间间隔。以30秒为单位，参数范围0秒~ 127×30 秒。

注：读写器只有在一段连续的时间内（超过心跳包时间间隔）没有读到任何标签数据，才会上传心跳包。

8.4.26 设置写功率

该命令用于单独设置读写器在执行写操作相关命令时的功率，写功率参数默认值为0x00，该参数掉电不丢失。

命令：

Len	Adr	Cmd	Data[]	CRC-16	
			WritePower		
0x05	0xXX	0x79	0xXX	LSB	MSB

参数解析：

WritePower：写功率参数。

Bit7：是否启用写功率设置。

0 – 不启用写功率设置。执行写操作相关命令时的功率与读功率一样；

1 – 启用写功率设置。执行写操作相关命令时的功率为Bit6~Bit0设定的功率值。

Bit6~Bit0：要设定的写操作功率。功率值范围是0~30，取值30时约为1W的输出功率。

应答：

Len	Adr	reCmd	Status	Data[]	CRC-16	
0x05	0xXX	0x79	0x00	—	LSB	MSB

注：写功率设置在执行以下命令时生效：

EPC C1G2(ISO18000-6C)命令：写数据，写EPC号，指定掩码扩展写数据，块擦除，块写；
ISO18000-6B命令：写数据。

8.4.27 读取写功率

该命令用于读取读写器在执行写操作相关命令时的功率设置参数。

命令：

Len	Adr	Cmd	Data[]	CRC-16	
0x04	0xXX	0x7A	——	LSB	MSB

应答：

Len	Adr	reCmd	Status	Data[]	CRC-16
				WritePower	
0x06	0xXX	0x7A	0x00	0xXX	LSB MSB

参数解析：

WritePower: 写功率参数。

Bit7: 是否启用写功率设置。

0 – 不启用写功率设置。执行写操作相关命令时的功率与读功率一样；

1 – 启用写功率设置。执行写操作相关命令时的功率为 Bit6~Bit0 设定的功率值。

Bit6~Bit0: 写操作功率。功率值范围是 0~30，取值 30 时约为 1W 的输出功率。

8.4.28 读取/设置写重试次数

该命令用于设置读写器在执行标签写数据及相关命令时，如果执行失败的自动重试次数。写重试次数默认值为 3，该参数掉电不丢失。

命令：

Len	Adr	Cmd	Data[]	CRC-16	
			RetryTimes	CRC-16	
0x05	0xXX	0x7B	0xXX	LSB	MSB

参数解析：

RetryTimes: 写重试次数参数。

Bit7: 读取/设置写重试次数标志。

0 – 读取写重试次数；

1 – 设置写重试次数。

Bit6~Bit3: 保留。

Bit2~Bit0: 写重试次数。

如果 Bit7=0，Bit2~Bit0 将被忽略；

如果 Bit7=1，Bit2~Bit0 为读写器在执行标签写数据及相关命令时，如果执行失败的自动重试次数。参数范围 0~7。

应答：

Len	Adr	reCmd	Status	Data[]	CRC-16
				RetryTimes	
0x06	0xXX	0x7B	0x00	0xXX	LSB MSB

参数解析：

RetryTimes: 写重试次数。

Bit7~Bit3: 保留, 默认值为 0。

Bit2~Bit0: 写重试次数。读写器在执行标签写数据及相关命令时, 如果执行失败的自动重试次数。参数范围 0~7。

注: 写重试次数在执行以下命令时生效:

EPC C1G2(ISO18000-6C)命令: 写数据, 写 EPC 号, 指定掩码扩展写数据, 块擦除, 块写;

ISO18000-6B 命令: 写数据。

8.4.29 标签自定义功能用户密码设置

本命令用于设置用户自定义访问密码, 访问密码在设置启动 Monza4QT 标签的 Peek 功能后有效。该密码将存储进读写器, 下次上电仍有效。

命令:

Len	Adr	Cmd	Data[]	CRC-16	
			UserPwd		
0x08	0xXX	0x7D	4Bytes	LSB	MSB

UserPwd: 四个字节, 高字节在前。用户自定义访问密码。

应答:

Len	Adr	reCmd	Status	Data[]	CRC-16	
0x05	0xXX	0x7D	0x00	—	LSB	MSB

8.4.30 标签自定义功能用户密码读取

本命令用于获取用户自定义访问密码。

Len	Adr	Cmd	Data[]	CRC-16	
0x04	0xXX	0x7E	—	LSB	MSB

应答:

Len	Adr	reCmd	Status	Data[]	CRC-16	
				UserPwd		
0x09	0xXX	0x7E	0x00	4Bytes	LSB	MSB

UserPwd: 四个字节, 高字节在前。用户自定义访问密码。

8.4.31 读写器 profile 设置/读取命令

该命令用于设置或读取读写器的内部 profile 参数配置。profile 默认值为 1, 该参数掉电不丢失。

命令:

Len	Adr	Cmd	Data[]	CRC-16	
			profile		
0x05	0xXX	0x7F	0xXX	LSB	MSB

参数解析：

profile: profile 设置/读取参数。

Bit7: 读取/设置 profile 标志。

0 – 读取 profile 编号；

1 – 设置 profile 编号。

Bit6~Bit0: profile 编号。

如果 Bit7=0, Bit6~Bit0 将被忽略；

如果 Bit7=1, Bit6~Bit0 为要设置的 profile 编号。参数范围 0~3。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。

应答：

Len	Adr	reCmd	Status	Data[]	CRC-16	
				profile		
0x06	0xXX	0x7F	0x00	0xXX	LSB	MSB

参数解析：

profile: 读写器当前 profile 设置编号。

Bit7: 保留，默认值为 0。

Bit6~Bit0: 读写器 profile 编号。参数范围 0~3。

注：profile0~3 的配置如下：

Profile 0: Tari 25uS, FM0 40KHz;

Profile1: Tari 25uS, Miller 4 250KHz (推荐配置, 系统默认) ;

Profile2: Tari 25uS, Miller 4 300KHz;

Profile3: Tari 6.25uS, FM0 400KHz。

8.4.32 同步 EM4325 时间戳

本命令用于读写器向射频场内的所有 EM4325 电子标签广播发送时间戳。

命令如下：

Len	Adr	Cmd	Data[]	CRC-16	
			UTC Time		
0x08	0xXX	0x85	4Bytes	LSB	MSB

参数解析：

UTC Time: 四个字节, 要广播发送的 UTC 时间, 表示从 1970-01-01 00:00:00 开始到当前时

间的秒数。高字节在前。UTC Time 的最高字节不能为 0，否则同步不成功。

应答：

Len	Adr	reCmd	Status	Data[]	CRC-16	
0x05	0xXX	0x85	0x00	—	LSB	MSB

注意：

- (1) EM4325 标签必须处于 BAP 模式下，才会接收同步时间戳命令并生效。
- (2) 要同步的 UTC 时间最高字节不能为 0，否则同步无效。
- (3) 当 EM4325 标签内部有任何一个警报位被置位时，UTC 时间同步无效。必须先使用“复位 EM4325 警报”命令清除标签的警报标志，或修改 EM4325 寄存器设置暂停相关报警功能。
- (4) 由于 EM4325 标签对同步时间戳命令不作回复，因此读写器发送同步 UTC 命令成功后即返回成功回复，至于标签 UTC 时间同步是否成功需要使用其他命令读取验证。
- (5) EM4325 标签内部的 UTC 时间寄存器设置成功后，每过一秒会自动增加 1，直至四字节 UTC 寄存器到达 0xFFFFFFFF 溢出回零后，或标签内部用户区中的系统配置寄存器被修改后，停止运行。

8.4.33 获取 EM4325 温度数据

本命令用于读写器向 EM4325 标签获取温度数据。

命令如下：

Len	Adr	Cmd	Data[]	CRC-16	
0xXX	0xXX	0x86	—	LSB	MSB

Data 参数如下：

Data[]				
ENum	EPC	SendUID	NewSample	Pwd
0xXX	变长	0xXX	0xXX	4Byte
MaskMem	MaskAdr	MaskLen	MaskData	
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。高字节在前，每个字的高字节在前。这里要求给出的是完整的 EPC 号。

SendUID: 一个字节。标签是否回复 UID 标志。0x00 表示不回复 UID; 0x01 表示回复 UID, 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。

NewSample: 一个字节。标签是否获取新的温度数据标志。0x00 表示获取上一次的温度数据; 0x01 表示标签将重新测量, 获取新的温度数据, 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。

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(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。Pwd 可以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)。范围 0~16383。

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	reCmd	Status	Data[]			CRC-16	
				UID	SenserData	UTC		
0xXX	0xXX	0x86	0x00	变长	4Bytes	4Bytes	LSB	MSB

参数解析:

UID: EM4325 的标签唯一识别号。

如果命令中 SendUID 标志为 0, 则回复数据中没有 UID 字段。

如果命令中 SendUID 标志为 1, 则回复数据中有 UID 字段, 字段长度由标签决定, 根据标签回复的不同, UID 长度可能为 8 个字节、10 个字节或 12 个字节。

SenserData: EM4325 标签返回的温度数据, 长度为 4 个字节, 高字节在前。具体定义见 EM4325 数据手册的 Sensor Data 寄存器说明。

UTC: 四个字节, 标签当前的 UTC 时间戳, 表示从 1970-01-01 00:00:00 开始的秒数。高字节在前。如果标签之前没有被成功同步或设置 UTC 时间戳, 则返回的 UTC 时间戳为全零。

8.4.34 获取 EM4325 的 SPI 外部数据

本命令用于读写器通过 EM4325 标签作为 SPI 主器件，向连接在 EM4325 的 SPI 口上的从器件获取数据信息。

命令如下：

Len	Adr	Cmd	Data[]	CRC-16	
0xXX	0xXX	0x87	——	LSB	MSB

Data 参数如下：

Data[]						
SPICmdSize	ENum	EPC	SPIResSize	SPISclk	SPIInitDelay	SPIInterval
0xXX	0xXX	变长	0xXX	0xXX	0xXX	0xXX
SPICmd	Pwd	MaskMem	MaskAddr	MaskLen	MaskData	
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、MaskAddr、MaskLen、MaskData 参数项。ENum 为 0xff 时有 MaskMem、MaskAddr、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。

SPICmdSize: 一个字节，要发送的 SPI 命令字节长度。SPI 命令字节长度参数范围 1~8，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。

SPIResSize: 一个字节，SPI 从设备将回复的数据字节长度。SPI 回复数据字节长度范围 0~7，其中 0 表示不回复，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。

SPISclk: 一个字节，表示 SPI 总线时钟。

0 – 40KHz;

1 – 80KHz;

2 – 160KHz;

3 – 320KHz。

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。

SPIInitDelay: 一个字节，表示初始化 SPI 时钟的延迟时间。

0 – 1 SCLK;

1 – 50us;
2 – 500us;
3 – 5ms。

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。

SPIInterval: 一个字节，表示每个 SPI 字节数据之间的延时。
0 – 无延时；
1 – 50us；
2 – 100us；
3 – 500us。

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。

SPICmd: 要发送的 SPI 命令数据，字节长度必须与 SPICmdSize 指定的一致。

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(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。Pwd 可以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）。范围 0~16383。

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	reCmd	Status	Data[]	CRC-16	
				SPIResData		
0xXX	0xXX	0x87	0x00	变长	LSB	MSB

参数解析：

SPIResData: SPI 从器件返回给 EM4325 标签的数据，长度范围为 0~7 个字节，字节长度应与命令中 SPIResSize 指定的长度一致。

注意：发送获取 EM4325 的 SPI 外部数据命令前，必须先配置 EM4325 的 I/O 控制字 (I/O Control Word) 寄存器，使能 SPI 口并设置为 SPI 主口，同时使能 SPI 引脚上拉寄存器。

8.4.35 复位 EM4325 警报

本命令用于复位/清除 EM4325 标签内部的所有警报信号，包括 UTC 时钟和监控功能都会被清零。

命令：

Len	Adr	Cmd	Data[]	CRC-16	
0xXX	0xXX	0x88	——	LSB	MSB

Data 参数如下：

Data[]						
ENum	EPC	Pwd	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: 要复位警报的标签的 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。

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(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。Pwd 可以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）。范围 0~16383。

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	reCmd	Status	Data[]	CRC-16	
				——	LSB	MSB
0x05	0xXX	0x88	0x00	——	LSB	MSB

注意： 使用“复位 EM4325 警报”命令前，必须先配置 EM4325 的温度传感器控制字（Temp Sensor Control Word 1）寄存器，使能 EM4325 的警报复位命令功能，否则 EM4325 标签不会对本命令作出任何回复。

8.4.36 DRM 设置/读取命令

该命令用于设置或读取 DRM 开关模式。该参数掉电丢失，重新上电后 DRM 默认关闭。

命令：

Len	Adr	Cmd	Data[]		CRC-16	
			DRMMode			
0x05	0xXX	0x90	0xXX		LSB	MSB

参数解析：

DRMMode：DRM 设置/读取参数。

Bit7：读取/设置 DRM 标志。

0 – 读取当前 DRM 模式；

1 – 设置 DRM 模式。

Bit6~Bit0：DRM 模式。

如果 Bit7=0，Bit6~Bit0 将被忽略；

如果 Bit7=1，Bit6~Bit0 为要设置的 DRM 模式。

0 – 关闭 DRM。

1 – 打开 DRM。

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。

应答：

Len	Adr	reCmd	Status	Data[]		CRC-16	
				DRMMode			
0x06	0xXX	0x90	0x00	0xXX		LSB	MSB

参数解析：

DRMMode：读写器当前 DRM 模式。

Bit7：保留，默认值为 0。

Bit6~Bit0：读写器当前 DRM 模式。0 – DRM 关闭；1 – DRM 打开。

8.4.37 测量天线口的回波损耗

该命令用于测量天线口在指定频点上的回波损耗值。

命令如下：

Len	Adr	Cmd	Data[]		CRC-16	
			TestFreq	Ant		
0x09	0xXX	0x91	4Bytes	0xXX	LSB	MSB

参数解析：

TestFreq: 测试回波损耗使用的频点，以 KHz 为单位，高字节在前。频点必须为 125KHz 或 100KHz 的倍数，否则会报参数错误。

Ant: 1 个字节，本次要进行测量的天线号。

0 – 天线 1;

1 – 天线 2;

2 – 天线 3;

3 – 天线 4。

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。

应答：

Len	Adr	reCmd	Status	Data[]	CRC-16	
				ReturnLoss		
0x06	0xXX	0x91	0x00	0xXX	LSB	MSB

参数解析：

ReturnLoss: 回波损耗值的测量结果，单位是 dB。

8.4.38 测量读写器当前工作温度

该命令用于读写器当前的工作温度。

命令如下：

Len	Adr	Cmd	Data[]	CRC-16	
0x04	0xXX	0x92	—	LSB	MSB

应答：

Len	Adr	reCmd	Status	Data[]		CRC-16	
				PlusMinus	Temp		
0x07	0xXX	0x92	0x00	0xXX	0xXX	LSB	MSB

参数解析：

PlusMinus: 温度正负符号，1 个字节。0x00 – 零下；0x01 – 零上。

Temp: 温度值，1 个字节，单位为摄氏度。

注：只有部分带温度传感器的读写器支持此命令。