EX10 系列模块数据通信协议

Ver23-8-13

目录

1 引言

简介

本文档设计了控制端（主机或上位机）和 EX10 系列模块（读写器）之间的串行通信基于请求/回复的通信机制，并规定了主机与读写器之间的通信数据协议格式。控制端和模块的设计都须遵从本协议。EX10 系列模块是指采用了 EX10 系列（E310，E510，E710，E910）射频芯片所生产的 RFID 模块。

适用范围

本文档适用于 EX10 系列所有模块型号包括 E310 系列模块，E510 系列模块，E710 系列模块。

本文档面向的读者：读写器开发人员、API 接口开发人员、系统集成开发人员、读写器技术支持人员 。

常用术语

字/块，表示 2 字节，即 16 位;

数字后面带(2)，表示为 2 进制，如 10000001(2)，0x 开头为 16 进制，如 0xFA

指令/命令，遵从协议定义的操作码

一帧指令，表示一条完整的指令数据。

文档格式说明

蓝色字体表示重要名词

蓝色带下划线字体表示该处存在超链接，通过 ctrl+鼠标单击可跳转至目标处。

红色字体表示需要额外注意。

带*号的地方详细说明在后面的“注意事项”章节中。

参考文件

EPC™ Radio-Frequency Identity Protocols Class-1 Generation-2 UHF RFID

Protocol for Communications at 860 MHz–960 MHz Version 1.2.0

2 概述

2.1 读写器运行机制

一个裸机的读写器需要通过烧录 Bootloader 层（后面简称 Boot 层，启动层）固件程序后，再升级 App Firmware 层（后面简称 APP 层，应用层）固件程序才能正常使用 RFID 相关功能。

通常读写器一旦上电之后就自动进入 Boot 层状态，此时读写器仅仅可以执行 Boot 层相关的指令，通常有两种途径让读写器进入到 APP 层状态；

<1>上位机下发启动 APP 层的切换指令，

<2>通过预先设置上电默认配置，上电自动切换至 APP 层。

读写器将加载 APP 层固件程序之后切换到 APP 层状态，此时可以执行 APP 层的指令，进入准备工作状态。在执行操作当中，也有两种途径切回到 Boot 层状态：

<1>上位机下发切回 Boot 层指令，

<2>读写器工作中发生上电复位，读写器复位到 Boot 层而未配置自动跳转 APP 层，例如供电不稳定可能会导致软复位。如图 1：

读写器运行状态切换图

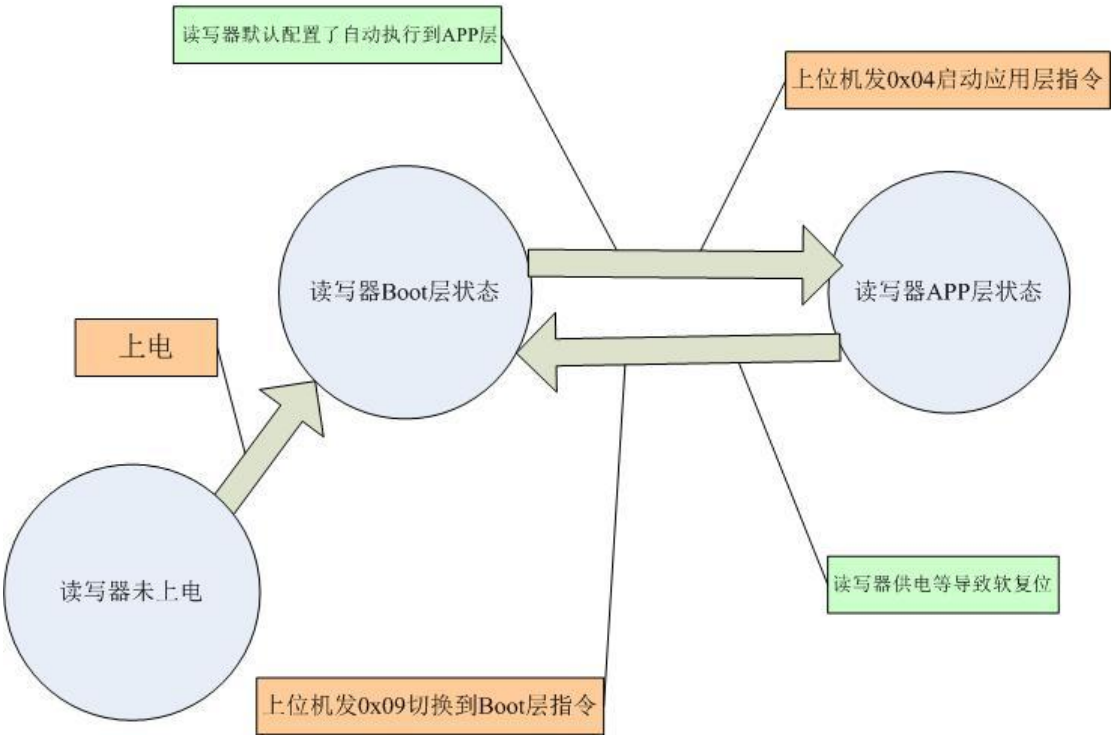


图 1

1 读写器 Boot 层只能执行支持 Boot 层的指令，APP 层只能执行支持 APP 层的指令。如使用了不支持的指令会返回 0x0101 错误，即无效的指令错误。具体指令可以参考该指令的指令属性。

2 读写器从 APP 层使用了非永久保存配置的指令，即普通设置指令。切换 Boot 层后再切回 APP 层那么之前的设置将失效，读写器 APP 层将使用默认值。 而读写器上电默认值配置是可以通过永久保存配置指令修改。

3 如修改过读写器的上电默认值项“上电运行至 APP”，那么读写器启动 Boot 层后会自动执行启动 APP 层指令，切换到 APP 层。即使发了启动 Firmware 指令 0x09，读写器也是瞬间切回 Boot 层后再跳转至 APP 层。因此配置了上电默认值项“上电运行至 APP”后，如要切换 Boot 层，在发切回 Boot 层的 0x09 指令前先发一条准备升级的指令 0xAB。

2.2 读写器认证区域

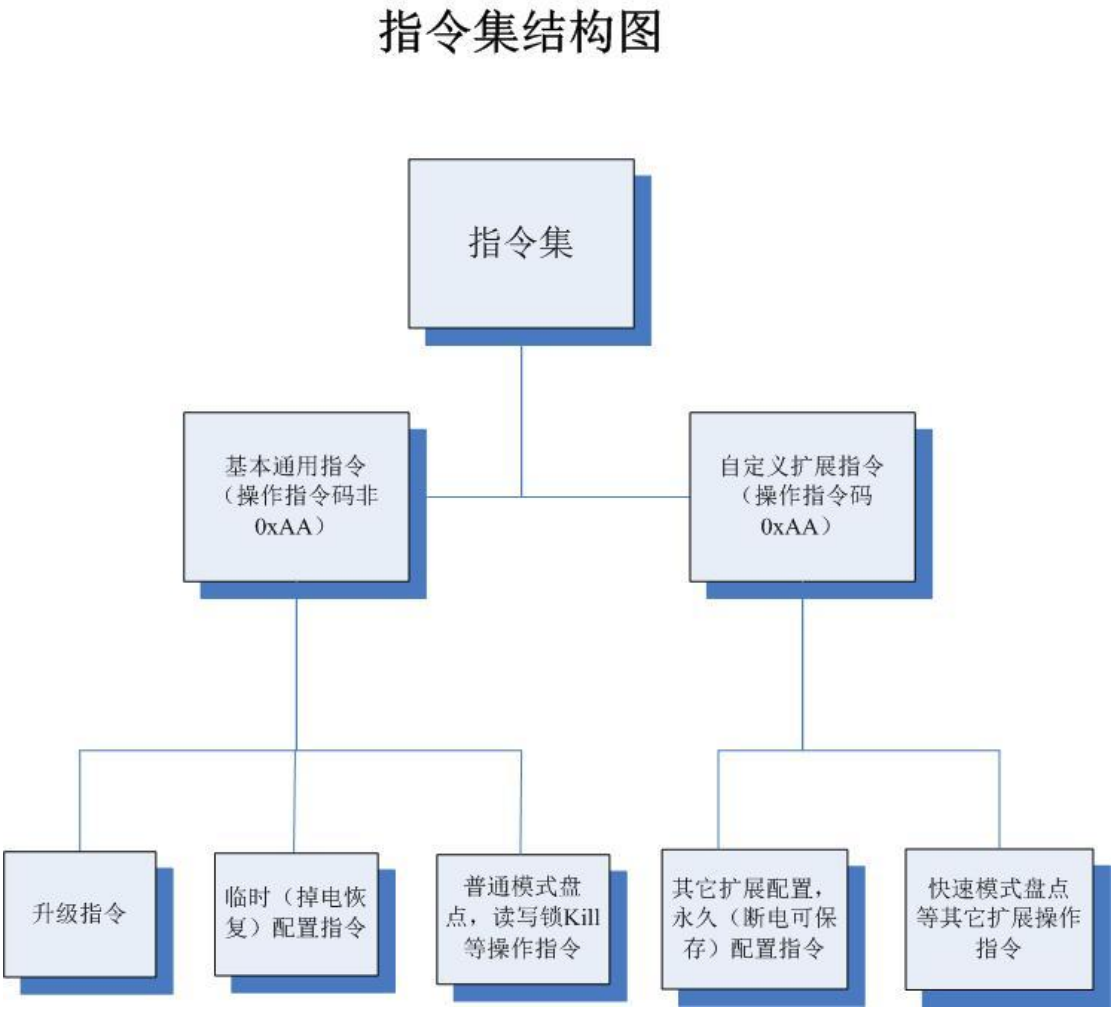
读写器认证区域是指读写器相关超高频参数符合某个国家的规定。如认证区域为中国大陆则符合中国大陆的超高频标准。EX10 系列模块认证区域类型大致分为中国大陆，CE 和 FCC。认证区域不同，模块功能上是有区别。

	中国认证区域	其他国家认证区域
符合国家标准	中国(默认)	指定的认证国家
默认工作频段	北美	指定的认证国家
可配置的工作频段	中国，北美，欧洲	指定的认证国家
是否可使用普通定频功能	是	否
是否可使用载波测试定频功能	是	是
是否可使用 EX 系列专用快速模式盘点指令(0xAA58)	是	CE 版，INDIA，RUSSIA，PHILIPPINES，JAPAN(所有），ISRAEL 版支持；其他类似 FCC 标准的国家都不支持
是否支持宜链点亮标签功能	是	否

说明：群读宜链标签要按照宜链标签规则读取对应存取区，群读温度标签与普通的嵌入读的区别在于盘点到标签后进行读取标签内存前会先让载波持续发送 40 毫秒后再进行读取，该功能仅中国版模块使用，外国认证版本模块不能。

2.2 指令集结构分类

指令码数量较多，从指令的功能和格式设计上看指令集的基本结构如下所示：图 2



文档后续将按七类功能指令分别介绍：Bootloader 指令，标签盘存指令，标签访问指令，设置指令，获取指令，永久保存配置指令，其它功能指令。

指令集概述

指令集名称	描述
Bootloader 指令	读写器 Bootloader 阶段时可以执行的任何指令都称为 Bootloader 指令。
标签盘存指令	与盘存操作相关的指令，盘存操作是指指定一个或多个天线轮询读一个或多个

指令集名称	描述
	标签的 EPC ID
标签访问指令	与标签访问操作相关的指令，是指指定单天线对单标签的内存操作
设置指令	设置相关的指令
获取指令	获取相关的指令
永久保存配置指令	属于扩展指令，应用于永久保存配置参数
其它功能指令	特殊功能指令

2.3 指令执行基本流程

通常来说，读写器从上电后到执行应用功能。必要步骤为

1 启动固件(未配置自动运行 APP)

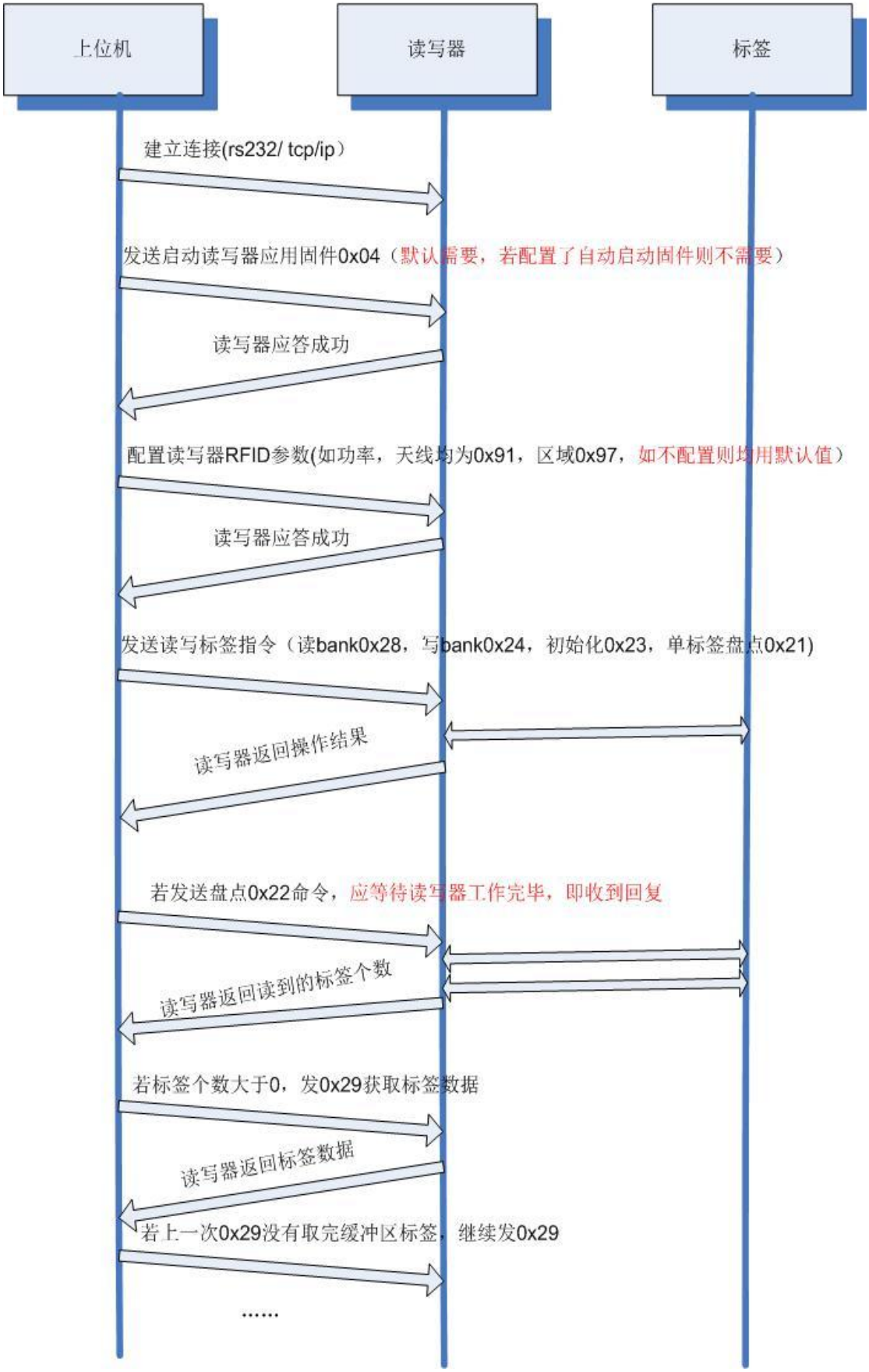
2 配置工作天线口(非单天线口) 。执行这两步之后，就可以进行基本的读写操作。

配置参数或者操作，若存在逻辑先后顺序，则需要按步骤处理。例如：设置频点，第一步先要确保要设置的频点在当前的工作区域范围内，否则就要先修改当前工作区域。又如进改密码。

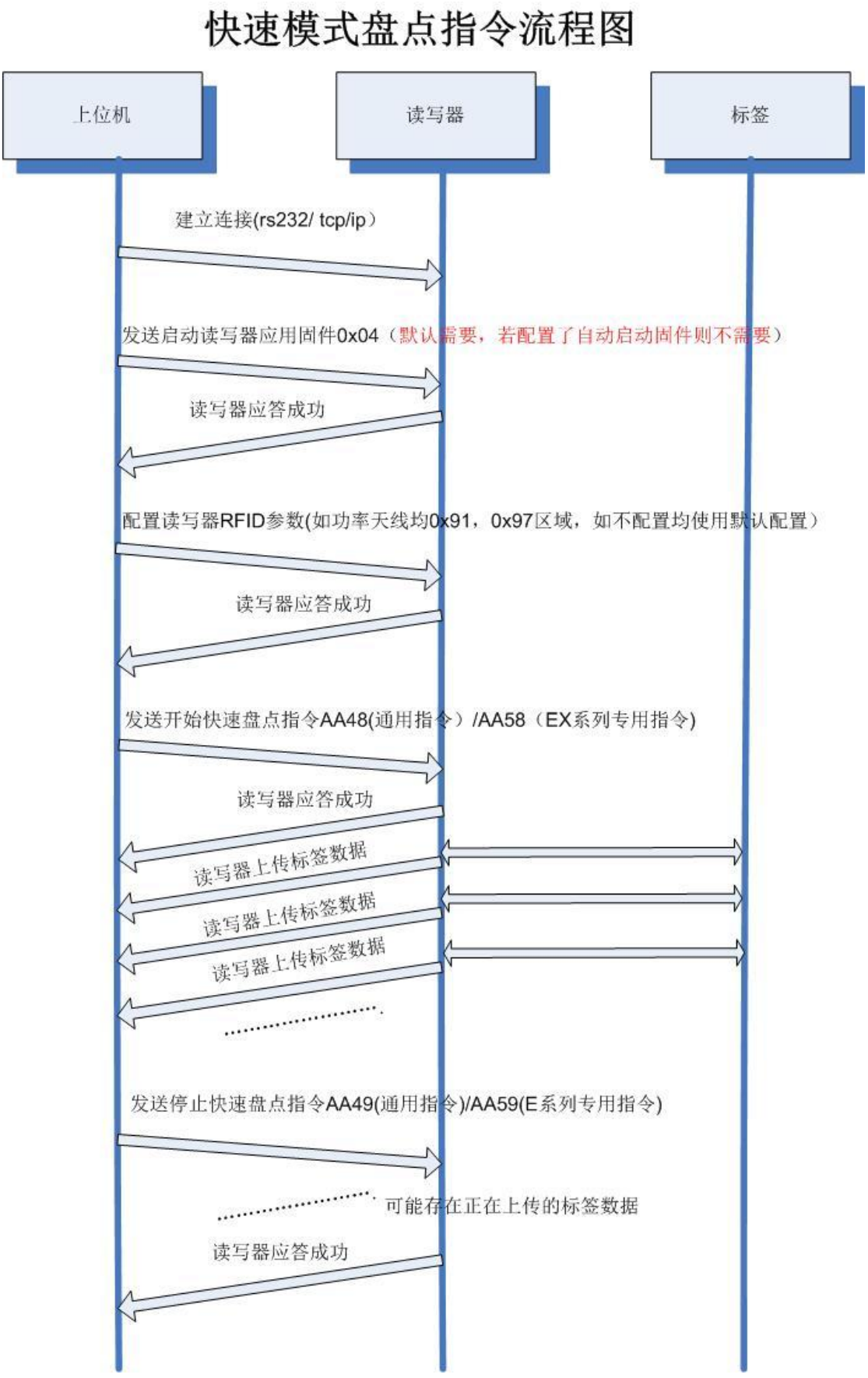
行锁，kill 操作。因为锁，kill 操作都必须在密码非 0 情况下进行，故若密码为 0 则需先

如图 3 所示，为普通模式盘点，读，写，锁，kill 等操作的流程：

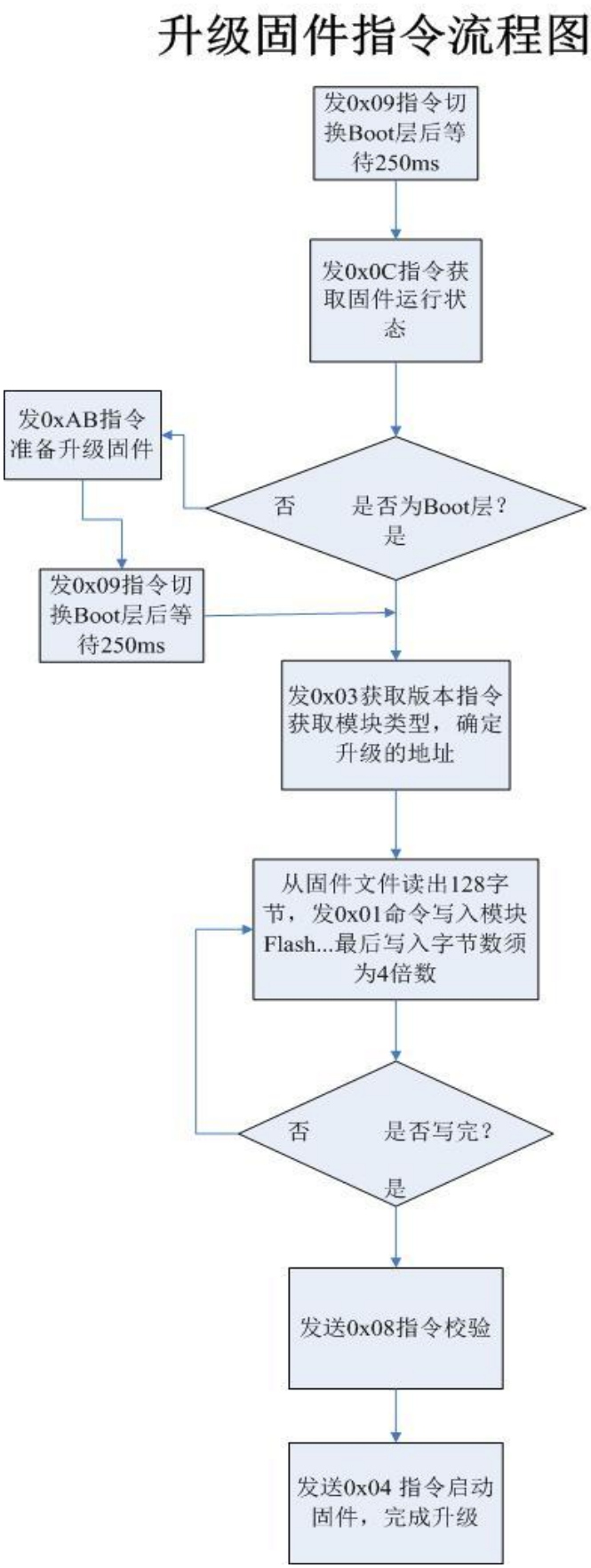
普通模式盘点以及操作指令流程图



如图 4 所示，为快速模式盘存的指令流程。



如图 5 所示，为升级固件的指令流程。



3 指令协议与数据格式

读写器采用被动工作模式，所有任务都由上位机下发命令开始，执行结束后返回操作结果，指令通信需要遵从以下规定。

(1) 主机与模块遵从一发一收的原则，每当主机向读写器发送消息时，在没有收到回复之前不应发送下一个指令。

(2)一帧通信数据（发送的指令或接收的指令）的总字节数不得超过 255。

(3)指令中的多字节整数采用 MSB 字节顺序，即大端模式：高位字节存放在低地址中（高字节在前），低位字节存放在高地址中。一字节最高位在前，最低位为 BIT0。

(4)上位机发送任何指令后，上位机等待模块回复的超时时间设置为 5 秒+指定指令执行时间。也即是有的指令中包括执行的时间的比如 0x22 盘存指令，则等待模块回复的超时时间为 5 秒+该指令中指定盘存的时间。这 5 秒时间是为了在模块突发异常的情况下给予的自恢复时间。回波检测指令建议超时时间 30 秒。

3.1 通用指令通信协议格式

Host-to-Reader 通信框架

主机到读写器通信按照下表进行打包。读写器一次只能接受一个指令，并且指令是串行执行的，因此主机在发出另一个指令之前应等待读写器到主机的响应。

Header	Data Length	Command Code	Data	CRC-16
1 字节，必须是 0xFF	1 字节，数据字段（Data）的字节数	1 字节	数据字段，高字节在前	2 字节循环冗余码，高字节在前

Reader-to-Host 通信框架

下表定义了从读写器到主机的响应数据包的格式。

Header	Data Length	Command Code	Status Code	Data	CRC-16
1 字节，必须是 0xFF	1 字节，数据字段 (Data) 的字节数	1 字节	2 个字节，状态码，0 表示操作成功，非零值表示操作失败	数据字段，高字节在前	2 字节循环冗余码，高字节在前

Host-to-Reader 通信指令，以下也称为请求指令或发送指令；Reader-to-Host 通信指令，以下也称为回复指令或接收指令；发送指令由 5 个部分排序组成，每个部分以下称为字段。发送指令由 Header 字段，Data Length 字段，Command Code 字段，Data 字段以及 CRC-16 字段组成，接收指令则由 6 个字段排序组成，即在 Command Code，Data 字段中间多了一个 Status Code 字段。

字段名称	说明
Header	1 字节，必须是 0xFF
Data Length	1 字节，注意此处长度为 Data 字段长度并非整个指令长度
Command Code	1 字节，指令码；若为通用指令则功能不同指令代码不同；若为扩展指令则此处固定为 0xAA，在 Data 字段内包含 2 个字节的子指令码
Status Code	2 个字节，状态码，0 表示操作成功，非零值表示操作失败，可参考状态码
Data	N 字节，数据字段，高字节在前；Data Length 值为 0 时没有 Data 字段，Data 字段由 Command Code 决定
CRC-16	2 字节，循环冗余码，高字节在前；见附录 1 CRC-16 C 语言示例

指令/命令组成结构：

一帧指令由多个字段组成。一个字段可能由多个域组成，一个域可能由多个子域或多个字段组成。现只有 Data 字段可能由多个域组成。

3.2 扩展指令通信协议格式

当 Command Code 为 0xAA 时候，该指令无实际含义。一般认为是扩展指令。而具体操作指令由 Subcommand Code 决定，而且发送指令的 Data 字段包含以下域：

扩展指令发送指令的 Data 字段。

当发送指令为扩展指令 0xAA 时的 Data 字段数据包含以下域：

域	字节长度	描述
Subcommand Marker	10	始终是”Moduletech”，此字段是由 ASCII 码表示的字符串。*
Subcommand Code	2	扩展子指令码，具有实际的操作含义。不同的扩展子指令码具有不同的功能。
Subcommand Data	N	不同扩展子指令具有不同的子指令数据。
SubCRC	1	首先将从子指令码（Subcommand Code）开始到子指令数据末尾（Subcommand Data）的所有字节累加，然后取结果的低 8 位。见附录 7 SubCRC C 语言示例
Terminator	1	始终是 0xBB

注意事项：

- Moduletech 16 进制字节数组为【4D 6F 64 75 6C 65 74 65 63 68】

扩展指令回复指令的 Data 字段格式

当接收指令为扩展指令时的 Data 字段数据包含以下域：

域	字节长度	描述
Subcommand Marker	10	同发送中的 Subcommand Marker
Subcommand Code	2	同发送中的 Subcommand Code
Subcommand Data	N	同发送中的 Subcommand Data

3.3 指令构建与解析

通用指令通信协议格式决定了帧头以及字段的序列，而扩展指令通信协议格式基于通用指令通信协议格式，是一种特殊形式。指令帧变化关键是由操作码字段和 DATA 字段决定，构建发送指令帧主要是构建操作码以及 DATA 字段。构建 DATA 字段可以参考文档该操作码其发送指令 DATA 字段格式部分。

而解析接收指令可认为是构建的逆顺序，由操作码字段判断为通用指令通信协议格式还是扩展指令通信协议格式。先将指令帧按字段分解。解析接收指令帧最主要为解析操作码以及其 DATA 字段部分，解析 DATA 字段可以参考文档该操作码其接收指令 DATA 字段格式部分。

后面将按操作码分类依次介绍操作码以及其发送指令 DATA 字段和接收指令 DATA 字段。发送指令构建和接收判断回复指令流程可以参考附录 6。

4 Bootloader 指令

Bootloader 在读写器上电时自动启动，允许访问板载闪存以及其他指令。下表中描述的指令是可在 Bootloader 阶段执行的所有指令。

Bootloader 指令概述

指令	Command Code	描述
写 Flash	0x01	写入板载闪存内容，用于更新读写器的固件。
读 Flash	0x02	读取板载闪存的内容。
获取版本	0x03	用于获取读写器的版本信息。
启动 Firmware	0x04	让读写器运行到 APP Firmware 层。
设置波特率	0x06	更改读写器器串口的波特率。
校验 Firmware	0x08	用于在升级 Firmware 后检查烧录是否正确，不应用于其他目的。
启动 Bootloader	0x09	让读写器回到 Bootloader 层。
获取读写器运行阶段	0x0C	获取当前读写器的运行阶段。
获取序列号	0x10	获取读写器序列号

4.1 写 Flash(0x01)

指令描述

写数据到板载闪存，用于更新读写器的固件

指令属性

Command Code	Bootloader 指令	App Firmware 指令	Data 字段
0x01	是	否	发送指令有，接收指令无

发送指令 Data 字段格式

写 Flash(0x01) 发送指令时带有 Data 字段，此时 Data 字段包含了以下的域，如表：

域	字节长度	描述
FINFLAG	1	0 表示仍有数据需要写入 Flash。 0xFF 表示这将是最后一次写入 Flash，即 Firmware 的最后一块数据。
WRITEADDR	4	烧录的初始地址是 0x08008000，每次成功写入后，下一个写地址将为 WRITEADDR + WRITELEN * 4。
WRITELEN	1	定义 WRITEDATA 的长度。WRITEDATA 的字节长度为 WRITELEN * 4。WRITELEN 的值固定为 32；只有当最后一次写入 Flash 的数据长度小于 128 字节时，才等于实际写入的字节数除以 4。
WRITEDATA	N	要写入 Flash 的数据，字节数是 4 的倍数。

注意事项：

●此指令会改写 FLASH 块内容，只作为升级 APP 应用程序段专用。

指令实例：

实例 1： 第一次写入

发送指令：

FF	86	01	00	08 00 80 00
Header	Data Length	Command Code	FINFLAG	WRITEADDR
20	98 8D 01 20 A1 E3 00 00 E5 A3 01 00 31 35 01 00 53 58 01 00 B1 FC 00 00 55 D2 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 A9 B2 01 00 31 06 01 00 00 00 00 00 09 A6 01 00 D1 C8 01 00 39 35 01 00 49 35 01 00 59 35 01 00 69 35 01 00 79 35 01 00 89 35 01 00 99 35 01 00 A9 35 01 00 B9 35 01 00 C9 35 01 00 D9 35 01 00 E9 35 01 00 F9 35 01 00 09 36 01 00 19 36 01 00 29 36 01 00			33 2A
WRITELEN	WRITEDATA			CRC

接收指令：

FF	00	01	00 00	94 E1
Header	Data Length	Command Code	Status Code	CRC

实例 2： 最后一次写入

发送指令：

FF	86	01	FF	08 03 04 00
Header	Data Length	Command Code	FINFLAG	WRITEADDR
02	12 01 52 05 23 C4 09 00			96 91
WRITELEN	WRITEDATA			CRC

接收指令：

FF	00	01	00 00	94 E1
Header	Data Length	Command Code	Status Code	CRC

4.2 读 Flash(0x02)

指令描述

读取板载闪存的内容。

指令属性

Command Code	Bootloader 指令	App Firmware 指令	Data 字段
0x02	是	否	发送指令有，接收指令有

发送指令 Data 字段格式

读 Flash(0x02) 发送指令时带有 Data 字段，此时 Data 字段包含了以下的域，如表：

域	字节长度	描述
READADDR	4	要读取的地址，读最低地址为 0x08008000
READLEN	1	0-32，读取的字节数为 READLEN * 4

接收指令 Data 字段格式

读 Flash(0x02) 接收指令时带有 Data 字段，此时 Data 字段包含了以下的域，如表：

域	字节长度	描述
READDATA	N	读取的数据，长度为 READLEN * 4 个字节。

注意事项：

●此指令用作烧录 APP Firmware 的辅助指令，不应用于其他目的。

4.3 获取版本(0x03)

指令描述

该指令用于获取读写器的版本信息。

指令属性

Command Code	Bootloader 指令	App Firmware 指令	Data 字段
0x03	是	是	发送指令无，接收指令有

接收指令 Data 字段格式

获取版本(0x03) 接收指令时带有 Data 字段，此时 Data 字段包含了以下的域，如表：

域	字节长度	描述
BootLoader Version	4	Bootloader 版本

域	字节长度	描述
Hardware Version	4	硬件版本
Firmware Date	4	Firmware 编译日期
Firmware Version	4	Firmware 版本
Supported Protocol	4	支持的标签协议，总是为 0x00000010（Gen2 协议）

Hardware Version 域说明

字节（从高位字节开始）	Hardware Version
第 1 字节	表示芯片的类型，E710=0x31、E510=0x32、E310=0x33、E910=0x34
第 2 字节	低 4 位表示天线口数量，ANTPORT_1=0，ANTPORT_2=1，ANTPORT_4=2，ANTPORT_8=3，ANTPORT_16=4，ANTPORT_32=5；高 4 位表示该种天线口的不同模块类型。
第 3 字节	表示该模块使用的认证区域 CHINA=0x00；FCC=0x01；JAPAN=0x02；JAPAN2=0x18；JAPAN3=0x19；CE（LOW）=0x03；KOREA=0x04；CE（HIGH）=0x05；HK=0x06；TAIWAN=0x07；MALAYSIA=0x08；SOUTH_AFRICA=0x09；BRAZIL=0x0a；THAILAND=0x0b；SINGAPORE=0x0c；AUSTRALIA=0x0d；INDIA=0x0e；URUGUAY=0x0f；VIETNAM=0x10ISRAEL=0x11；PHILIPPINES=0x12；INDONESIA=0x13；NEW_ZEALAND=0x14；PERU=0x15；RUSSIA=0x16；CE（LOW AND HIGH）=0x17（暂不支持）；
第 4 字节	用于表示版本更新的序号

指令实例：

发送指令：

FF	00	03	1D 0C
Header	Data Length	Command Code	CRC

接收指令：

FF	14	03	00 00	22 02 18 00
Header	Data Length	Command Code	Status Code	BootLoader Version

31 00 00 00	20 22 07 08	22 07 08 00	00 00 00 10	FD 54
Hardware Version	Firmware Date	Firmware Version	Supported Protocol	CRC

4.4 启动 Firmware(0x04)

指令描述

指令读写器运行到 APP Firmware 层。当读写器处于 Bootloader 层并收到此指令时，它将执行到 APP Firmware 层。如果读写器正处于 APP Firmware 层中，则返回操作成功。

指令属性

Command Code	Bootloader 指令	App Firmware 指令	Data 字段
0x04	是	是	发送指令无，接收指令有

接收指令 Data 字段格式

启动 Firmware(0x04) 接收指令时带有 Data 字段，格式请参考 获取版本(0x03) 接收指令 Data 字段格式

指令实例：

发送指令：

FF	00	04	1D 0B
Header	Data Length	Command Code	CRC

接收指令：

FF	14	04	00 00	22 02 18 00
Header	Data Length	Command Code	Status Code	BootLoader Version
31 00 00 00	20 22 07 08	22 07 08 00	00 00 00 10	FD 54
Hardware Version	Firmware Date	Firmware Version	Supported Protocol	CRC

4.4 设置波特率(0x06)

目前无效。需要修改波特率可参考修改上电默认值配置上电默认波特率。

4.5 校验 Firmware(0x08)

指令描述

此指令用于在烧录 App Firmware 后校验是否正确，不应用于其他目的。

指令属性

Command Code	Bootloader 指令	App Firmware 指令	Data 字段
0x08	是	否	发送指令有，接收指令无

发送指令 Data 字段格式

校验 Firmware(0x08) 发送指令时带有 Data 字段，此时 Data 字段包含了以下的域，如表：

域	字节长度	描述
CHECKADDR	4	校验的起址，必须是 0x08008000
CHECKDATALEN	4	该值是 0x01 指令写入 Flash 的字节数除以 4。
CHECKCRC	4	计算方法：以 4 个字节为单位，将 0x01 指令写入 Flash 的所有字节（即所有 WRITEDATA）从开始到结束分为 N 个 4 字节数字。N 个数字的最高字节被累加到 DATA1。 N 个数字的第二高字节被累加到 DATA2。 N 个数字的第二低字节被累加到 DATA3。 N 个数字的最低字节被累加到 DATA4。 DATA1，DATA2，DATA3 和 DATA4 也是 32 位数字。 DATA1 的最低 8 位是 CHECKCRC 的最高字节。DATA2 的最低 8 位是 CHECKCRC 的第二高字节。DATA3 的最低 8 位是 CHECKCRC 的第二低字节。 DATA4 的最低 8 位是 CHECKCRC 的最低字节。

指令实例：

发送指令：

FF	0C	08	08 00 80 00	00 00 A1 02	05 08 0C 08	1D 0C
Header	Data Length	Command Code	CHECKADDR	CHECKDATA LEN	CHECKCRC	CRC

接收指令：

FF	00	08	00 00	05C8
Header	Data Length	Command Code	Status Code	CRC

4.6 启动 Bootloader(0x09)

指令描述

如果读写器在 APP Firmware 层收到此指令，它将返回到 Bootloader 层。如果读写器当前正处于 Bootloader 层，它将返回操作成功而不进行任何处理。当发送此指令后收到成功响应时，再发送另一个指令之前应该等待 250ms，因为从 APP Firmware 层返回到 Bootloader 层需要一些时间。

指令属性

Command Code	Bootloader 指令	App Firmware 指令	Data 字段
0x09	是	是	发送指令无，接收指令无

指令实例：

发送指令：

FF	00	09	1D 06
Header	Data Length	Command Code	CRC

接收指令:

FF	00	09	00 00	15 E9
Header	Data Length	Command Code	Status code	CRC

注意事项:

●发了 0x09 指令后，需要等待固件处理时间。

●如配置了上电默认值“自动启动应用层”，应先发准备升级指令 0xAB 后再发 0x09 指令。

4.7 获取读写器运行阶段(0x0C)

指令描述

获取读写器当前的运行阶段（是 Bootloader 层还是 App Firmware 层）。

指令属性

Command Code	Bootloader 指令	App Firmware 指令	Data 字段
0x0c	是	是	发送指令无，接收指令有

接收指令 Data 字段格式

获取版本(0x0C) 接收指令时带有 Data 字段，此时 Data 字段包含了以下的域，如表:

域	字节长度	描述
Program	1	0x11 表示 Bootloader 层; 0x12 表示 APP Firmware 层。

指令实例：

发送指令：

FF	00	0C	1D 03
Header	Data Length	Command Code	CRC

接收指令：

FF	01	0C	00 00	12	63 43
Header	Data Length	Command Code	Status Code	Program	CRC

4.8 获取序列号(0x10)

指令描述

获取读写器序列号。

指令属性

Command Code	Bootloader 指令	App Firmware 指令	Data 字段
0x10	是	是	发送指令有，接收指令有

发送指令 Data 字段格式

获取序列号(0x10) 发送指令时带有 Data 字段，此时 Data 字段包含了以下的域，如表：

域	字节长度	描述
Option	1	保留参数，该值目前无意义
Data Flags	1	保留参数，该值目前无意义

接收指令 Data 字段格式

获取序列号(0x10) 接收指令时带有 Data 字段，此时 Data 字段包含了以下的域，如表：

域	字节长度	描述
Year	4	本产品的制造年份，例如 02 00 02 03，即 0x02,0x00,0x02,0x03 表示年份为 2023
Serial Number	8	此批次中的序列号，09 09 09 09 09 09 09 09，表示该模块的序列号为 99999999

指令实例：

发送指令：

FF	02	10	00	00	F0 93
Header	Data Length	Command Code	Option	Data Flags	CRC

接收指令：

FF	0C	10	00 00	02 00 02 03	00 00 00 00 01 02 45 09	B5 A4
Header	Data Length	Command Code	Status Code	Year	Serial Number	CRC

5 标签盘存指令

在 APP 层比较常用的指令为标签盘存指令，盘存标签基本操作是采集标签的 EPCID。为适应不同应用场景，读写器具有不同的盘存方式。

现 EX10 系列读写器实现了四种标签盘存模式，即单标签盘存，同步盘存（普通盘存），异步盘存（快速盘存）和 EX10 系列异步盘存（快速盘存）。

- 单标签盘存仅盘存首先响应读写器的第一个标签。适用于单天线单标签实时场景。
- 同步盘存指令必须指定盘存的执行时间。指令发送到读写器后，读写器执行该时间段的盘存，然后返回盘存到的标签数量，然后通过获取标签缓冲区（0x29）指令获取读写器内存中的标签信息。适用于标签数量不多，限时读取。
- 异步盘存包含一组指令，主机可以通过开始异步盘存指令启动盘存，读写器将立即回复主机启动盘存是否成功，然后读写器将保持连续盘存状态，一旦盘存到标签后会立即上传到主机。适用于实时性强场景。
- EX10 系列异步盘存包含一组指令，主机可以通过开始 EX10 异步盘存指令启动盘存，读写器将立即回复主机启动盘存是否成功，然后读写器将保持连续盘存状态，一旦盘存到标签后会立即上传到主机。此指令现仅 EX10 系列模块支持。适用于大量标签应用场景。

此外，需要引入标签盘存指令和标签访问指令中经常使用的一些参数和域。

标签盘存指令概述

指令	Command Code	描述
单标签盘存	0x21	盘存单个标签，读第一个标签将停止工作并返回
同步盘存	0x22	盘存多标签，并将盘存到的标签存储在读写器的内存中。与获取标签缓冲区 0x29 指令配合使用
获取标签缓冲区	0x29	获取同步盘存到的标签信息。

指令	Command Code	描述
异步盘存	0xAA（0xAA48，0xAA49）	异步盘存包含一组指令：开始异步盘存（子指令码：0xAA48），停止异步盘存（子指令码：0xAA49），主动动上传的 Reader-to-Host 指令。
EX 异步盘存	0xAA（0xAA58，0xAA59）	EX 异步盘存包含一组指令:开始 EX 异步盘存(子指令码：0xAA58）,停止 EX 异步盘存（子指令码：0xAA59），主动动上传的 Reader-to-Host 指令。现仅 EX10 系列读写器支持

5.1 常用的域说明

盘存和标签访问操作指令中的 Data 字段常用的域：

5.1.1 Option

Option 域为可选控制标志字段，用于启用或禁用相关的功能，同时可能影响后续相关域组成。Option 字段通常为一个字节，由两个部分（控制位）组成。包含用于标签 Tag Singulation 域选择功能的 Select-Option-Bits，Option 域的其他位可用于其他目的的 Non-Sel-Option Bits。

Select-Option Bits

Tag Singulatio 域选择功能使用一个字节（通常为 Option）的第 0,1,2,3 和 5 位。这些位称为 Select-Option Bits。 Select-Option Bits 取值将影响 Data 字段中的 Tag Singulation 域和访问密码（AccessPassword）域（若 Data 字段定义此域，并且非固定域）。

Non-Sel-Option Bits

在大多数标签操作指令中有一个字节的 Option 域，Option 域中位置不是

Select-Option Bits 的位称为 Non-Sel-Option Bits，Non-Sel-Option Bits 根据操作码不同有不同的含义定义,例如单标签盘存 0x21 的 Non-Sel-Option Bits 记为 Non-Sel-Option Bits-0x21 。同步盘存 0x22 的 Non-Sel-Option Bits 记为 Non-Sel-Option Bits-0x22.两者定义不同。

域	字节长度	子域	控制位	描述
Option	1	Select-Option Bits	第 0,1,2,3 和 5 位 BIT	用于控制过滤 bank 以及 Tag Singulation 域和访问密码（若 Data 字段定义此域，并且非固定域）
		Non-Sel-Option Bits	除 Select-Option Bits 位外其余位 BIT（4，6，7）	Non-Sel-Option Bits 用于控制其它功能，功能根据指令不同而不同

5.1.2 Tag Singulation

所有标签盘存和标签访问指令都支持 Tag Singulation 域。如果使用标签选择过滤，则只有符合标签过滤规则的标签被才能被盘存到；对于标签访问操作，例如读取，写入，锁定等，则只有某一个符合标签过滤规则的标签被操作。

Tag Singulation 域

Tag Singulation 域包含的子域如下：

域	字节长度	描述
Select Address	0/4	Bank 内的偏移量（以位 BIT 为单位），注意：编址从零开始。由 Select-Option Bits 的

域	字节长度	描述
		BIT0/BIT1/BIT2 决定是否存在
Select Data Length	1/2	要比较的数据长度（选择数据），以位 BIT 为单位。通常为 1 字节。注意：若 Select-Option Bits 的 BIT5 为 1 即值 0x20 时，该域长度为 2 字节。
Select Data	N	要与 bank 中指定的标签数据进行比较的数据。 注意 N=Select Data Length/8，然后向上取整

举例

The following EPC IDs (first 3 bits) are in the field:

0xAAAA (101)

0xCCCC (110)

0x4444 (010)

0x3000 (001)

Select Option = 0x04 (EPC MemBank)

Select Data Length = 0x01 (only match 1 bit)

Select Data = 0x80 (10000000, select data lenght is 1 bit,so others bits no effect)

Select Data Address = 0x00000022 (third bit in the EPC ID, EPCID address is start from 0x20 bits)

In this case the third bit of the EPC ID is matched against the first bit of the Select

Data value, 1. This would result in the following IDs being returned:

0xAAAA

0x3000

Select-Option Bits 控制位值定义：

以下“所有域”指的是 Tag Singulation 域所有子域和访问密码域（若 Data 字段定义此域，并且非固定域）

控制位	值	描述
第 0，1，2	0x00	禁用选择过滤功能，响应读写器的第一个标签将是被操作的标签，且 Tag Singulation 域所有子域不出现在指令中，且无访问密码域
	0x01	过滤选择 EPC 的值。需要除了 Select Address 域以外的所有 Tag Singulation 域所有子域(Select Data Length+Select Data)，访问密码域 （与操作码有关，若发送 Data 字段定义了此域，并且非固定域。）
	0x02	过滤选择 TID bank 的内容，需要所有域。
	0x03	过滤选择用 USER bank 的内容，需要所有域。
第 0，1，2	0x04	过滤选择 EPC bank 的内容，需要所有域。
	0x05	如果需要操作已经被锁定的存储区域但不进行过滤选择，请使用此选项。使用此选项时，无 Tag Singulation 域，有访问密码域（同上）。
	0x07	表示采用多标签匹配过滤盘存标签。使用此选项时，无 Tag Singulation 域，有访问密码域（同上）。0x21 指令不支持此项。
第 3 位	0x08	设置反转标志，这将导致返回不匹配过滤选择规则的标签。
第 5 位	0x20	过滤选择数据长度为 2 个字节，允许选择数据大于 255 位。

注意事项：

●使用多标签匹配过滤必须是成功配置过多标签匹配过滤数据（0xAA4C）才能正确执行 ，否则返回错误

Select-Option Bits 控制位值 影响以下的指令域，如下表所示：

值	Select Address	Select Data Length	Select Data	AccessPassword （若 Data 字段定义此域）
0x00	无	无	无	无
0x01	无	有	有	有
0x02	有	有	有	有
0x03	有	有	有	有
0x04	有	有	有	有
0x05	无	无	无	有
0x07	无	无	无	有
0x20		长度为 2 字节		

Non-Sel-Option Bits 控制位值定义：

控制位	值	描述
第 4 位	0x10	由操作码决定，操作码不同有不同的定义
第 6 位	0x40	由操作码决定，操作码不同有不同的定义
第 7 位	0x80	由操作码决定，操作码不同有不同的定义

5.1.3 Metadata Flags

使用 BIT 位标识某项元数据是否存在，元数据标志定义的每个位的内容如下。

Metadata Flags 值	描述
0x0000	无元数据返回，仅返回标签 EPC（包括标签 PC，CRC）
0x0001	BIT0 为 1 返回标签的 Read Count，在盘存时间内被盘存到的次数
0x0002	BIT1 为 1 返回标签的 RSSI，反应标签信号强度
0x0004	BIT2 为 1 返回标签的 Antenna ID，被盘存到时所用的天线 ID 号
0x0008	BIT3 为 1 返回标签的 Frequency，盘存到时所用的频率值
0x0010	BIT4 为 1 返回标签的 Timestamp，首次被盘存到时的时间值
0x0020	BIT5 为 1 返回标签的相位值
0x0040	BIT6 为 1 返回标签的 Protocol ID，模块使用的标签协议值
0x0080	BIT7 为 1 返回标签的 Tag Data Length 域

说明：若要返回多项元数据只需将其 Metadata Flags 各 BIT 值 做或运算

5.1.4 Metadata

若发送指令中包含了 Metadata Flags 域，那么接收指令中将返回相应的 Metadata 项。

项	字节长度	描述	
Read Count	1	标签被盘存的次数，如果 Metadata Flags 的 BIT0 为 0 则不存在此字段。	
RSSI	1	信号强度，以 dBm 为单位，有符号单字节。 如果 Metadata Flags 的 BIT1 为 0 则不存在此字段。该值采用补码方式，计算值 rssi 除最高符号位外，其它位取反+1，例如 0xE6 表示-26dBm(256-26=230=0xE6)。	
Antenna ID	1	盘存到此标签的天线编号。如果 Metadata Flags 的 BIT2 为 0 则不存在此字段。	
Frequency	3	盘存到此标签的频率，单位为 kHz。如果 Metadata Flags 的 BIT3 为 0 则不存在此字段。	
Timestamp	4	从发出盘存指令到获取此标签所经历的时间，单位为毫秒。如果 Metadata Flags 的 BIT4 为 0 则不存在此字段。	
PHASE	2	指令为单标签盘存(0x21)， 指令为读标签存储区(0x28)， 如果 Metadata Flags 的 BIT5 为 0 则不存在此字段。	高字节为起始相位值，低字节为结束相位值。相位数据转换为度的方式为： (相位值/256)*360 （度）
		指令为同步盘存指令(0x22)， 指令为异步盘存指令， 如果 Metadata Flags 的 BIT5 为 0 则不存在此字段。	起始相位跟结束相位分别都为 2 个字节。此项为结束相位值，低 12 位有效。相位数据转换为度的方式为： (相位值/4096)*360 （度）
Protocol ID	1	协议编号(0x05 表示 GEN2)，如果 Metadata Flags 的 BIT6 为 0 则不存在此字段。	

项	字节长度	描述
Tag Data Length	2	Bank 数据的位长度，如果 Metadata Flags 的 BIT7 为 0 则不存在此字段。且在单标签盘存 0x21 指令中 Tag Data Lengt 的值总为 0x0000，其它盘存指令中如启用了盘存嵌入指令，且 Tag Data Length 不为 0 时，表示成功读出数据，值表示后续 TagData 域的位长度。
Tag Data	N	标签内存数据，长度为 Tag Data Length/8。Tag Data Length 不为 0 时才存在此字段。此域为盘点返回的附加数据。

5.1.5 Tag EPC and Meta Data

在盘存操作当中，常常返回标签 EPC ID 和其它的属性项，如 EPC bank 包含的 PC 和 Tag CRC，如 Meta Data 的天线号和 RSSI 信号强度等。

Tag EPC and Meta Data 域

域	字节长度	描述
Metadata	N	Metadata 域长度由 Metadata Flags 决定
EPC Length	2	若操作码为 0x29 指令，该域为 EPC 的位长度（BIT），包括 PC，EPCID 和 TagCRC。例如 16+64+16=0x0060
	1	若操作码为 0xAA 指令，该域为 PC+EPC+TagCRC（EPCCRC）的字节长度（byte）；例如 2+8+2=0x0C
PC Word	2	EPC bank 中的 PC 字段。PC 的高 5 位代表 EPC 的块长度（1 块=2 bytes）。
EPC ID	N	Tag EPC，若启用了 FASTID 功能而且成功返回 TID，那么 EPC ID 可以细分为 EPCID0+TagCRC0+TID，详细见 FASTID 功能

域	字节长度	描述
TagCRC/ PHASE2	2	当操作码为 0x29，0xAA 时；由 Metadata Flags 决定该域为 Tag CRC 或 PHASE2,当使能了返回相位值时，这里返回的是起始相位值 PHASE2，低 12 位有效。相位计算为度的方式为：(相位值/4096)*360 （度））
		当操作码为 0x21 该域为 Tag CRC。参考附录 5 TagCRC 算法

5.1.6 Timeout

同步盘存和所有标签操作指令都具有此域，该域指定指令执行的最长时间（以毫秒为单位）。如果指令在此超时时间之前完成操作，则读写器会提前回复主机，否则会在超时时间结束后回复主机，Timeout 域为 2 字节，最大超时为 65535（0xFFFF）。

5.2 单标签盘存(0x21)

指令描述

此指令用于在指定时间内盘存单个标签。也即是在指定时间内盘存到一个标签后就返回。

该指令遵从通用指令通信协议格式。

指令属性

Command Code	Bootloader 指令	App Firmware 指令	Data 字段
0x21	否	是	发送指令有，接收指令有

发送指令 Data 字段格式

单标签盘存(0x21) 发送指令时带有 Data 字段，此时 Data 字段包含了以下的域，如表：

域	字节长度	描述
Timeout	2	请参考 Timeout 域描述
Option	1	Option 域包含 Select-Option Bits 控制位和 Nol-Select-Option Bits-0x21 控制位
Metadata Flags	0/2	由 Option 域的 Nol-Select-Option Bits-0x21 控制位(BIT4)决定，设置为 1 时(值为 0x10，00010000(2))，此域才存在,长度为 2。否则此域不存在。该域告诉读写器要返回的元数据。
Tag Singulation	N	Tag Singulation 的具体内容，此域仅在启用 Tag Singulation 时存在，否则此域不存在。

接收指令 Data 字段格式

单标签盘存(0x21) 接收指令时带有 Data 字段

有两种不同的数据字段格式，具体取决于发送指令 Option 域的 BIT4 是否为 1，为 1 包含 Metadata Flags 域。第一种是只获取 EPC，发送指令中没有 Metadata Flags 域。 另一种是获取 EPC 和元数据，在发送指令中必须有 Metadata Flags 域。

获取 EPC

发送指令中 Option 域的 BIT4 为 0，没有 Metadata Flags 域时，接收指令时带有 Data 字段，此时 Data 字段包含了以下的域，如表：

域	字节长度	描述
Option	1	与发送指令的 Option 字段相同。
EPC	M	标签的 EPC
TagCRC	2	EPC bank 中 TagCRC

获取 EPC 和元数据

发送指令中中 Option 域的 BIT4 为 1，有 Metadata Flags 域时，接收指令时带有 Data 字段，此时 Data 字段包含了以下的域，如表：

字段	字节长度	描述
Option	1	与发送指令的 Option 字段相同。
Metadata Flags	2	与发送指令中的 Metadata Flags 字段相同。
Metadata	N	Metadata 域长度由 Metadata Flags 决定
EPC ID	N	标签 EPC
Tag CRC	2	标签 CRC

●须先指定单个操作天线。

指令实例：

实例 1：返回 1 秒（1000ms）内读到的 EPC：

发送指令：

FF	03	21	03 E8	00	A5E8
Header	Data Length	Command Code	Timeout	Option	CRC

接收指令：

FF	0F	21	00 00	00	C0C011112222 3333AAAA0009	641F	A542
Header	Data Length	Command Code	Status Code	Option	EPC	Tag CRC	CRC

实例 2： 获取 EPC 号的同时获取天线 ID 号与模块系统时间信息

timeout=488ms

Metadata Flags = 0x0004 |(或运算) 0x0010 = 0x0014

不启用选择匹配过滤，返回第一个盘存到的标签：

发送指令：

FF	05	21	01 E8	10	0014	2F 6D
Header	Data Length	Command Code	Timeout	Option	Metadata Flags	CRC

接收指令：

FF	16	21	00 00	10	00 14
Header	Data Length	Command Code	Status Code	Option	Metadata Flags
01	00 BB 5F 04	01 23 45 67 89 AB CD EF 01 23 45 67		E6 C8	83 D0
Ant ID	Timestamp	Tag EPC		Tag CRC	CRC

实例 3： **获取 EPC 并返回 Antenna ID 和 Timestamp**

Metadata Flags = 0x0004 | 0x0010 = 0x0014，使能标签过滤，过滤的 EPC 为 0x111122223333444455556666

发送指令：

FF	12	21	01 E8	11	0014

Header	Data Length	Command Code	Timeout	Option	Metadata Flags
60		11 11 22 22 33 33 44 44 55 55 66 66			9F CE
Select Data Length		Select Data(EPC)			CRC

接收指令：

FF	16	21	00 00	11	0014
Header	Data Length	Command Code	Status Code	Option	Metadata Flags
02	0F C8 C0 B7	11 11 22 22 33 33 44 44 55 55 66 66		18 35	AF D0
Ant ID	Timestamp	Tag EPC		Tag CRC	CRC

5.3 同步盘存(0x22)

指令描述

此指令和 0x21 指令之间的区别在于该指令在设置的时间内盘存天线场区中的所有标签，并返回标签的数量，直到设置的时间到期。发送指令后，如果盘存到任何标签，需要稍后发送 0x29（获取标签缓冲区）指令以获取标签信息。目前标签缓冲区最多可存储 1200 个标签。因此在发送指令后，在设置的盘存时间中最多可以保存 1200 个标签，当标签缓冲区中累积 1200 个标记时，将停止盘存并返回结果。如果上次发了 0x22 指令后，没有发送 0x29 指令获取缓冲标签，下次 0x22 指令执行前将自动清除所有缓冲标签。该指令遵从通用指令通信协议格式。

指令属性

Command Code	Bootloader 指令	App Firmware 指令	Data 字段
0x22	否	是	发送指令有，接收指令有

发送指令 Data 字段格式

同步盘存(0x22) 发送指令时带有 Data 字段，此时 Data 字段包含了以下的域，如表：

域	字节长度	描述
Option	1	Option 域包含 Select-Option Bits 控制位和 Nol-Select-Option Bits-0x22 控制位。Nol-Select-Option Bits-0x22 中 BIT7 位置 1

域	字节长度	描述
		（对应值 0x80），表示启用 FASTID 功能。注意若 Select-Option Bits=0x07 时，即启用使用多标签匹配过滤时，FASTID 功能无效。另外，若启用了附加数据功能时，FASTID 功能也无效。
Search Flags	2	该值低字节只有 BIT2 位跟 BIT4 位有效（BIT 位从 0 开始）。 BIT2=1 时使用盘存嵌入指令，存在 Embedded Command Content 否则不启用，不存在 Embedded Command Content 域。 BIT4=1 时 使用 IMPINJ 的 TAGFOCUS 功能，0 时不使用。* 当 BIT2=1 时，且高字节值为 0xA5，表示是群读宜链温度标签功能。
Timeout	2	请参考 Timeout 域描述
Access Password	0/4	访问密码. 如果标签已锁定且嵌入读标签数据指令则需要密码，请发送正确的访问密码。如果标签未锁定或访问操作不需要密码，则密码为 0x00000000。注意：如果 Option 中的 Select-Option Bits = 0，则指令中不包含 4 字节访问密码。
Tag Singulation	N	过滤功能。请参考 Tag Singulation。由 Option 中的 Select-Option Bits 决定。如果没有启用过滤功能，则此域不存在。
Embedded Command Content	N	附加数据功能。同步盘存指令可以嵌入另一个标签访问操作指令。目前仅支持嵌入 0x28 指令。当 Search Flags 的 BIT2 为 0 时，不应该有此字段。

Embedded Command Content 域

域	字节长度	描述
Embedded Command Count	1	嵌入指令的数量；必须是 1。
Embedded Command Length	1	嵌入指令的数据字段长度，以字节为单位。现最大支持 64 字节。
Embedded Command Opcode	1	嵌入的指令代码，目前仅支持 0x28 指令。
Embedded Values	N	嵌入指令的数据字段，目前仅为 0x28 指令的发送 Data 字段 *

接收指令 Data 格式

同步盘存(0x22) 接收指令时带有 Data 字段，此时 Data 字段包含了以下的域，如表：

域	字节长度	描述
Option	1	发送指令相同。
Search Flags	2	与发送指令相同。如果盘存标签的数量大于 255，则 Search Flags 的 BIT 4 将设置为 1。
Tags Found	1/4	盘存到的标签数量，如果标签数量大于 255(Search Flags 的 BIT 4)，则此字段为 4 个字节。
Embedded Command Result	N	由 Search Flags 的 BIT2 控制，如果未使用嵌入指令，则不存在此字段。

Embedded Command Result

字段	字节长度	描述
Embedded Command Count	1	嵌入指令的数量必须为 1。
Embedded Command Opcode	1	与发送指令相同。
Operations Succeeded	2	嵌入指令操作成功的次数。由于在盘存期间可以多次操作相同的标签，因此这里成功操作的数量仅可用作参考。
Operations Failed	2	嵌入指令操作失败的次数。由于在盘存期间可以多次操作相同的标签，因此这里的操作失败次数只能用作参考。
Embedded Command Data Returned	N	嵌入指令成功运行返回的数据（如果 0x28 指令操作成功，它将返回读到第一个标签的标签数据。如果不成功，则没有此字段）

注意事项：

●TAGFOCUS 功能，只有在设置为 S1，静态 TARGET A 时才有效；

●若读写器为多天线口并连接多个天线，那么在发送同步盘存(0x22)前，需要先发送配置天线指令（0x91）。若配置了多天线，目前的天线轮询规则是：例如启用了天线 1,3 和 4，那么盘存将从 1 开始，如果没有读到新增标签则跳转到 3，然后跳转到 4，然后跳回到 1....。

●当盘存嵌入 0x28 指令成功执行时，0x29 指令可用于获取存储的标签信息。当盘存嵌入 0x28 指令时，读取标签存存储区的长度最多为 32 个字节。嵌入的 0x28 指令的格式可参考读标签数据章节。 盘存嵌入 0x28 指令的操作流程是每次盘存后对标签执行 0x28 指令，无论指令 0x28 的操作是否成功，都将保存标签的 EPC，并在退出时返回。

●Embedded Values（0x28 的发 Data 字段），中的的(Emb Cmd) Timeout 与(Emb Cmd)Option 的值是不起作用的，都为 0。整个指令的执行时间为 Timeout 指定的时间。

指令实例：

例子 1：启用匹配过滤，匹配区域为 EPC

发送指令：

FF	0F	22	04	00 00	03 E8	00 00 00 00	00 00 00 78	08	66	DE C0
Header	Data Length	Command Code	Option	Search Flags	Time out	Access Password	Select Address	Select data length	Select data	CRC

接收指令：

FF	04	22	00 00	04	00 00	02	B7 6E
Header	Data Length	Command Code	Status Code	Option	Search Flags	Tag Found	CRC

如果盘存到的标签数量超过 255，则 Tag Found 的长度为 4 个字节，Search Flags 的 BIT4

设置为 1.如果盘存了 257 个标签，则返回指令的格式如下。

FF	07	22	00 00	04	00 10	00 00 01 01	5A0E
Header	Data Length	Command Code	Status Code	Option	Search Flags	Tag Found	CRC

例子 2：

不使用过滤匹配功能，启用 FASTID 功能

发送指令：

FF	05	22	80	00 00	00 C8	332D
Header	Data Length	Command Code	Option	Search Flags	Timeout	CRC

接收指令：

FF	04	22	00 00	80	00 00	00	6030
Header	Data Length	Command Code	Status Code	Option	Search Flags	Tag Found	CRC

例子 3：

不使用过滤匹配，嵌入 0x28 指令，读取 USER bank 从块地址 0 开始的 32 个数据块。

发送指令：

FF	11	22	00	00 04	03 E8	01	09	28
Header	Data Length	Command Code	Option	Search Flags	Time out	Embedded Command Count	Embedded Command Length	Embedded Command Opcode

00 00	00	03	00 00 00 00	20	
Embedded Command Timeout	Embedded Command Option	Read MemBank	Read Address	Read Word Count	CRC

注意：嵌入指令的 Embedded Command Timeout 和 Embedded Command Option 的值不起作用，均为 0，整个指令的执行时间是 Timeout 指定的时间。

例子 4:

使用标签匹配过滤，匹配区域是从 TID bank 的地址 0x00 开始的 8 位，匹配值是 0xE2，并且盘存嵌入 0x28 指令，读取从 RESERVED bank 的地址 0x02 开始的 2 个块（即是读取访问密码）

发送指令：

FF	1B	22	02	00 04	03 E8	22 22 11 11	00 00 00 00	08
Header	Data Length	Command Code	Option	Search Flags	Time out	Access Password	Select Data Address	Select Data Length

E2	01	09	28	00 00	00	00	00 00 00 02	02	82 CF
Select Data	Embedded Command Count	Embedded Command Length	Embedded Command Opcode	Embedded Command Timeout	Embedded Command Option	Read MemBank	Read Address	Read Word Count	CRC

接收指令：

FF	0E	22	00 00	02	00 04	1C	01
Header	Data Length	Command Code	Status Code	Option	Search Flags	Tag Found	Embedded Command Count

28	00 01	00 2F	22 22 11 11	C6F2
Embedded Command Opcode	Operations Succeeded	Operations Failed	Data Read	CRC

5.4 获取标签缓冲区(0x29)

指令描述

此指令用于获取由同步盘存指令（0x22）盘存到的标签信息。可以获取的信息包括标签的 EPC 及其相关的元数据。从缓冲区里获取的标签数据后，将从缓冲区中删除这些缓冲的标签。该指令遵从通用指令通信协议格式。

指令属性

Command Code	Bootloader 指令	App Firmware 指令	Data 字段
0x29	否	是	发送指令有，接收指令有

发送指令 Data 字段格式

获取标签缓冲区(0x29) 发送指令时带有 Data 字段，此时 Data 字段包含了以下的域，如表：

域	字节长度	描述
Metadata Flags	2	请参考 Metadata Flags。
Read Option	1	0x00 表示获取尚未获取的标签的信息。 0x01 表示获取前一个 0x29 指令获得的标签信息。

接收指令 Data 字段格式

获取标签缓冲区(0x29) 接收指令时带有 Data 字段，此时 Data 字段包含了以下的域，如表：

域	字节长度	描述
Metadata Flags	2	请参考 Metadata Flags。
Read Option	1	同上述发送指令的 Read Option。
Tag Count	1	返回信息中包含的标签数量。
Tag EPC and Meta Data	N	每个标签的信息被打包为 Tag EPC and Meta Data 的数据块。 这些数据块的数量是 Tag Count。

5.4.1 FASTID 功能

Gen2 协议中 PC 字节高 5 位代表 EPC 的字长度，而 PC 和 EPC 可以计算出 Tag CRC。计算 Tag CRC 算法见附录 TagCRC C 语言示例。

采用 FASTID 盘存功能，此时如果是有 FASTID 功能的标签返回的标签数据 EPC 域包含了 EPC0+TagCRC0+TID 内容，没有 FASTID 功能的标签返回的标签数据还是原来的 EPC 内容。支持 FASTID 功能的标签的 TID 长度固定为 6 个字也即是 12 个字节。

返回有 FASTID 数据的格式为：PC+（EPC0+TagCRC0+TID）+TagCRC

没有返回 FASTID 数据的格式为：PC+EPC+TagCRC

一旦启用了 FASTID 功能时，上位机要进行判断确认模块返回的标签数据里面是否包含 TID。

若返回的数据 通过 PC 值高 5 位，计算 EPC 字长度（计算方法为 PC 高字节>>3)为 EPCWORDLEN。

如果 EPCWORDLEN 小于 7，那么标签的 EPCID 域不包含 TagCRC0 和 TID 内容。如果 EPCWORDLEN 大于等于 7（TagCRC 固定 1 字+TID 固定 6 字），那么该标签可能是带有 TID 的标签数据。假设 EPC 域包含了 EPC0+TagCRC0+TID，然后根据以下步骤计算判断：

1 取 EPC 域前 EPCWORDLEN-7 个字长度作为 EPC0

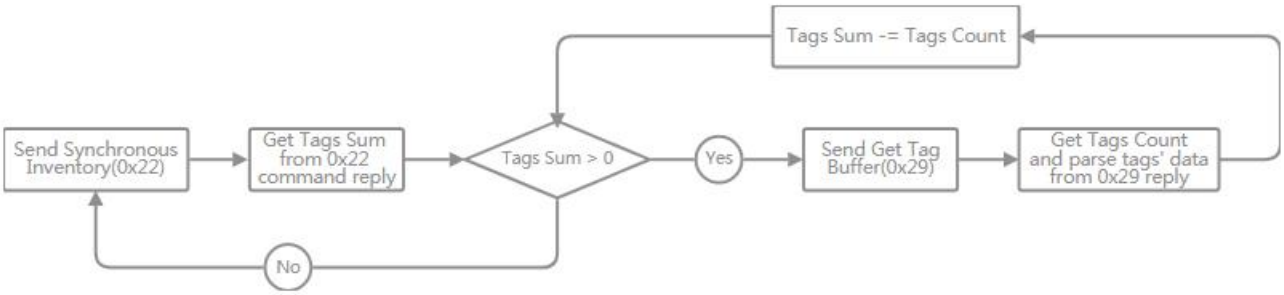
2 由 EPCWORDLEN-7 的值左移 3 位，作为 PC0 的高字节值。取 PC 的低字节值为 PC0 的低字节值。

3 根据 PC0 和 EPC0 计算出 tag CRC 值（参考附录 5 tagCRC），与 TagCRC0 比较。相等则表示该标签数据是包含 TID 的标签数据。否则标签的 EPCID 域不包含 TagCRC0 和 TID 内容。

注意：计算 tag CRC 的算法只适合 impinj 定义为此格式的 FASTID 功能的标签。若存在其它格式的 FASTID 功能的标签，则无法判断是否存在 TID，需要另外的计算规则。

注意事项：

●使用同步盘存，指令发送过程如下。



指令实例：

例子 1：获取标签，并返回读取次数，天线 ID 和时间戳。Metadata Flags= 0x0001 | 0x0004 | 0x0010 = 0x0015

发送指令：

FF	03	29	00 15	00	E1 22
Header	Data Length	Command Code	Metadata Flags	Option	CRC

接收指令：

FF	34	29	00 00	00 15	00	02	22	01
Header	Data Length	Command Code	Status Code	Metadata Flags	Option	Tag Count	Read Count	Ant ID

02 50 CE F6	00 80	31 C1	11 11 22 22 33 33 44 44 55 55 66 66	FB 15	0E
Timestamp	EPC Length	PC Word	EPC ID	Tag CRC	Read Count

01	04 1D 3D 3C	00 80	30 00	05 00 00 00 00 00 00 00 00 00 23 54	4A C8	92 A3
Ant ID	Timestamp	EPC Length	PC Word	EPC ID	Tag CRC	CRC

例子 2：获取标签，并返回除 Protocol ID 外的所有标签元数据，Metadata Flags = 0x00BF.

发送指令：

FF	03	29	00 BF	00	4B 22
Header	Data Length	Command Code	Metadata Flags	Option	CRC

接收指令：

FF	4A	29	00 00	00 BF	00	02	07	E3	01	0E 22 2A
Header	Data Length	Command Code	Status Code	Metadata Flags	Option	Tag Count	Read Count	RSSI	Ant ID	Frequency

00 00 8D 8F	00 00	00 00	00 60	20 00	11 11 22 22 33 33 44 44	C2 41	07	D0
Timestamp	PHASE	Tag Data Length	EPC Length	PC Word	EPC ID	Tag CRC	Read Count	RSSI

01	0E 22 2A	00 00 8D 87	00 00	00 00	00 D0	58 00	11 11 22 22 33 33 44 44 55 55 66 66 77 77 88 88 99 99 00 00 AA AA	96 86	FD 4C

Ant ID	Frequency	Timestamp	PHASE	Tag Data Length	EPC Length	PC Word	EPC ID	Tag CRC	CRC

例子 3： 指令 0x22 嵌入指令 0x28，读取 TID bank 中地址 0 开始的 2 个字，并获取除 Protocol ID 外的所有标签元数据。元数据标志= 0x00BF

发送指令：

FF	03	29	00 BF	00	4B 22
Header	Data Length	Command Code	Metadata Flags	Option	CRC

接收指令：

FF	6E	29	00 00	00 BF	00	03	08	D7	01	0D F7 32
Header	Data Length	Command Code	Status Code	Metadata Flags	Option	Tag Count	Read Count	RSSI	Ant ID	Frequency

00 00 71 9B	00 00	00 20	E2 00 34 12	00 80	30 00	E2 00 81 81 81 16 02 40 08 20 C7 4C	7E 4C	08	D5	01
Timestamp	PHASE	Tag Data Length	Tag Data	EPC Length	PC Word	EPC ID	Tag CRC	Read Count	RSSI	Ant ID

0D F7 32	00 00 71 B5	00 00	00 20	E2 00 60 04	00 D0	58 00	11 11 22 22 33 33 44 44 55 55 66 66 77 77 88 88 99 99 00 00 AA AA	96 86
Frequency	Timestamp	PHASE	Tag Data Length	Tag Data	EPC Length	PC Word	EPC ID	Tag CRC

07	D4	01	0D F7 32	00 00 71 8D	00 00	00 20	E2 00 60 04	00 20	00 00	E2 F0	96 E7
Read Count	RSSI	Ant ID	Frequency	Timestamp	PHASE	Tag Data Length	Tag Data	EPC Length	PC Word	Tag CRC	CRC

5.5 异步盘存

异步盘存包括一组指令，所有这些指令的指令代码是 0xAA。 不同的指令功能被封装在数据字段中。 因此异步盘存的不同指令使用不同的子指令代码。异步盘存通常又成为快速盘存模式/高速盘存模式。

异步盘存属于扩展指令，遵从扩展指令通信协议格式。指令码固定为 0xAA。扩展指令的子指令称为 SubCommand Code，固定 2 个字节。SubCommand Code 对应的数据域为 Subcommand Data 域，以下简称 SubData 域。

5.5.1 异步盘存(0xAA48)

指令描述

此盘存模式使用异步模式，启动异步盘存的指令将在盘存启动后立即返回，读写器处于连续异步状态，一旦标签被读取，就会主动上传到主机。通过这种方式，读写器的盘存性能是最佳的，对于有较高盘存性能要求的应用应使用此异步盘存。基于 R2000 芯片和 E 系列芯片的 UHF 模块都支持该指令。异步盘存进行中，正常的结束指令是停止异步盘存命令，返回正常状态码，发送其它指令或模块异常都将结束盘存并返回包含错误状态码的停止异步盘存命令的回复。该指令遵从扩展指令通信协议格式。

指令属性

SubCommand Code	Bootloader 指令	App Firmware 指令	Subcommand Data
0xAA48	否	是	发送指令有，接收指令无

发送指令 SubData 域格式

异步盘存(0xAA48) 发送指令时带有 SubData 域，此时 SubData 域包含了以下的域，如表：

域	字节长度	描述
Metadata Flags	2	参考 Metadata Flags 域
Option	1	含义与 0x22 指令相同。
Search Flags	2	低字节含义与 0x22 指令相同。但高字节不同，不支持群读温度标签功能。高字节控制位如下： 最高位(BIT7):表示读写器是否在异步库存模式下每隔一段时间向主机发送心跳包，1 表示是，0 表示否。 当此功能被开启时，读写器每隔 15 秒向主机端发送一帧心跳包。如果异步库存停止，读写器将不会再发送心跳包。心跳包格式参考心跳数据包。 次高位(BIT6):表示当启用了单天线在一段时间后无法读取到新的标签时是否停止盘存，并将停止异步盘存命令的回复（数据格式参考 0xAA49 接收指令）发送给主机（此功能仅当一次启用一个天线进行盘存时使用）。1 表示是，0 表示否。使用异步盘存模式时，此功能通常用于将读写器的单个天线端口扩展为多个外部天线端口。若模块出现了异常，则模块停止盘存并返回带有错误状态的停止异步盘存命令的回复。 BIT5：当使能了多个天线口工作的时候，置 1 的话则所有天线每轮询完一遍后模块将会发送一个告知上位机当前所有天线已经轮询完一遍的通知帧，为 0 则不使能。通知帧格式参考轮询周期数据包
Access Password	0/4	含义与 0x22 指令相同。
Tag Singulation	N	含义与 0x22 指令相同。
Embedded Command Content	N	含义与 0x22 指令相同。

注意事项：

●目前的天线轮询规则是：如果启用了多天线工作，将按天线号升序排序。那么盘存将从最低的天线号开始盘存，当该天线在一段时间内（此时间为模块内部处理的判断时间）没有读到新增标签则跳转到下一个天线，另外如该天线驻留时间超过规定时间（默认为 4 秒，修改参考 0x95 指令）会强制切换到下一个天线，依次轮询完毕所有天线后又重新从最低序号天线开始，如此循环。

指令实例：

例子 1：

不使用 Tag Singulation 和 Embedded Command Content 的情况下开始异步盘存。 Metadata Flags 是 0x00BF，这意味着要求读写器返回除 Protocol ID 之外的所有元数据。

发送指令：

FF	13	AA	4D 6F 64 75 6C 65 74 65 63 68	AA 48
Header	Data Length	Command Code	Subcommand Marker (Moduletech)	Subcommand Code

00 BF	00	80 03	34	BB	29 0F
Metadata Flags	Option	Search Flags	SubCRC	Terminator	CRC

接收指令：

FF	0C	AA	00 00	4D 6F 64 75 6C 65 74 65 63 68	AA 48	0F 23
Header	Data Length	Command Code	Status Code	Subcommand Marker (Moduletech)	Subcommand Code	CRC

例子 2：开始异步盘存，并使用 Tag Singulation/Select. Metadata Flags 为 0x00BF。

发送指令：

FF	1D	AA	4D 6F 64 75 6C 65 74 65 63 68	AA 48	00 BF	04
Header	Data Length	Command Code	Subcommand Marker (Moduletech)	Subcommand Code	Metadata Flags	Option

80 03	00 00 00 00	00 00 00 20	08	E2	42	BB	AB 26
Search Flags	Access Password	Select Address	Select Data Length	Select Data	SubCRC	Terminator	CRC

实例 3： 开始异步盘存，并使用 Tag Singulation/Select 和 Embedded Command Content. 并且 Metadata Flags 为 0x00BF。

发送指令：

FF	2A	AA	4D 6F 64 75 6C 65 74 65 63 68	AA 48	00 BF	02	80 07
Header	Data Length	Command Code	Subcommand Marker (Moduletech)	Subcommand Code	Metadata Flags	Option	Search Flags

00 00 00 00	00 00 00 20	0C	E2 00	01	09
Access Password	Select Address	Select Data Length	Select Data	Embedded Command Count	Embedded Command Length

28	00 00	00	02	00 00 00 00	02	7E	BB	D0 91
Embedded Command Opcode	Embedded Command Time out	Embedded Command Optionn	Read Membank	Read Address	Read Word Count	SubCRC	Terminator	CRC

5.5.2 异步盘存主动上传数据包

当读写器处于异步盘存的过程中，读写器可以主动向主机发送数据帧，在没有请求的情况下发送的这些指令帧称为数据包。

5.5.2.1 标签信息数据包

启动了异步盘存操作，若盘点到标签，读写器将立刻主动上传标签信息数据包，标签信息数据包格式遵从通用指令通信协议格式。

接收指令 Data 字段格式

标签信息数据包 接收指令时带有 Data 字段，此时 Data 字段包含了以下的域，如表：

域	字节长度	描述
Metadata Flags	2	请参考 Metadata Flags。
Tag EPC and Meta Data	N	请参考 Tag EPC and Meta Data。

注意事项：

●标签信息数据包 以下值固定：

Command Code ： 0xAA

Status Code：0x0000

指令实例：

实例 1：标签信息数据包 1

接收指令：

FF	1B	AA	00 00	003F	01BD020DF73200000 01300000C20001111 20190211019422AF	E259
Header	Data Length	Command Code	Status Code	Metadata Flags	Tag EPC and Meta Data	CRC

解析 Tag EPC and Meta Data：由 Metadata Flags=003F 可以得出包含的元数据（0x0001|0x0002|0x0004|0x0008|0x0010|0x0020）

01	BD	02	0DF732	00000013	0000
Read Count	RSSI	Antenna ID	Frequency	Timestamp	Phase
0C	2000	1111201902110194			22AF
EPCLENGTH	PC	EPC			EPCCRC

实例 2：标签信息数据包 2

接收指令：

FF	21	AA	00 00	00BF	01 D3 01 0D CC 3A 00 00 00 1A 00 17 00 00 10 30 00 E2 00 00 1D 40 01 01 58 10 40 82 73 36 C1	42 A1
Header	Data Length	Command Code	Status Code	Metadata Flags	Tag EPC and Meta Data	CRC

接着解析 Tag EPC and Meta 由 Metadata Flags=00BF 分析得出

（0x0001|0x0002|0x0004|0x0008|0x0010|0x0020|0x0080）

01	D3	01	0D CC 3A	0000001A	0017	0000
Read Count	RSSI	Antenna ID	Frequency	Timestamp	Phase	Tag Data Length
10	3000	E200001D4001015810408273			36C1	
EPCLENGTH	PC	EPC			EPCCRC	

5.5.2.2 心跳数据包

当读写器在开始异步盘存命令中启用心跳功能时，读写器将定期（大约每隔 15 秒左右）发送心跳数据包。心跳数据包的格式遵从通用指令通信协议格式。

接收指令 Data 字段格式

心跳数据包 接收指令时带有 Data 字段，此时 Data 字段包含了以下的域，如表：

域	字节长度	描述

域	字节长度	描述
Heartbeat Marker	4	始终为“XTSJ”，此字段是由 ASCII 码表示的字符串。
Search Flags	2	含义与 0x22 指令相同。

注意事项：

●心跳数据包 以下值固定：

Command Code：0xAA

指令实例：心跳包

接收指令：

FF	06	AA	00 00	58 54 53 4A	80 03	17 24
Header	Data Length	Command Code	Status Code	XTSJ	Search Flags	CRC

5.5.2.3 轮询周期数据包

当使能了多个天线口工作的时候，并且启用了轮询周期（指所有天线都依次盘点了一遍）通知，那么每个周期会发一个通知帧，称为轮询周期数据包。轮询周期数据包的格式遵从通用指令通信协议格式。

接收指令 Data 字段格式

轮询周期数据包 接收指令时带有 Data 字段，此时 Data 字段包含了以下的域，如表：

域	字节长度	描述
Metadata Flags	2	请参考 Metadata Flags。

域	字节长度	描述
Tag EPC and Meta Data	N	请参考 Tag EPC and Meta Data。 注意，标签数据帧中的以下域将固定值或重新定义，如下： EPC Length：固定 1 字节，值固定为 0x05 PC Word：2 字节，固定 0x0000 EPCID：1 字节，此处实际含义为 ANTWORKCNT， 表示为第几轮天线轮询完通知帧，当 ANTWORKCNT=0xFF 后，下一次通知帧将会变为 0，然后再重新计数。 EPCCRC:2 字节，，固定 0x0000

指令实例：返回第一轮天线轮询完通知帧

接收指令：

FF	09	AA	00 00	00 04	
Header	Data Length	Command Code	Status Code	Metadata Flags	
02	05	00 00	01	00 00	F5 75
Header	EPC Length	PC Word	EPCID (ANTWORKCNT)	EPCCRC	CRC

5.5.3 停止异步盘存(0xAA49)

指令描述

如启动了异步盘存操作，则可以使用此指令停止异步盘存。

该指令遵从扩展指令通信协议格式。

指令属性

SubCommand Code	Bootloader 指令	App Firmware 指令	Subcommand Data
0xAA49	否	是	发送指令无，接收指令无

注意事项：

●如果模块在已经成功启动“异步盘存指令”后，收到其他有效的指令（包括启动异步盘存指令），则模块退出异步盘存，并返回该有效指令的指令不成功应答，返回错误代码 0xAA49，其它代码为模块其它异常情况；例如：开启异步盘存后发送，

FF 00 03 1D 0C 则模块返回 FF 00 03 AA 49 1E EA

●如果模块当前没启动异步盘存收到异步盘存命令停止指令，则返回执行成功；

指令实例：

发送指令：

FF	0E	AA	4D 6F 64 75 6C 65 74 65 63 68	AA 49	F3	BB	03 91
Header	Data Length	Command Code	Subcommand Marker (Moduletech)	Subcommand Code	SubCRC	Terminator	CRC

接收指令：

FF	0C	AA	00 00	4D 6F 64 75 6C 65 74 65 63 68	AA 49	0F 22
Header	Data Length	Command Code	Status Code	Subcommand Marker (Moduletech)	Subcommand Code	CRC

5.5.4 EX 异步盘存(0xAA58)

指令描述

此盘存模式使用异步模式，启动异步盘存的指令将在盘存启动后立即返回，读写器处于连续异步状态，一旦标签被读取，就会主动上传到主机。这种方式可用于大量标签环境。基于 E 系列芯片的 UHF 模块都支持该指令。异步盘存进行中，正常的结束指令是停止 EX 异步盘存命令，返回正常状态码，发送其它指令或模块异常都将结束盘存并返回包含错误状态码的 EX 停止异步盘存命令的回复。该指令遵从扩展指令通信协议格式。

指令属性

SubCommand Code	Bootloader 指令	App Firmware 指令	Subcommand Data
0xAA58	否	是	发送指令有，接收指令无

发送指令 SubData 域格式

异步盘存(0xAA58) 发送指令时带有 SubData 域，此时 SubData 域包含了以下的域，如表：

域	字节长度	描述
ExConfigData	20	目前只有首字节可设置，当为 0 时为密集标签模式，主要在于读多读全大量标签或者用于复杂环境的情况下，为 1 时表示在标签数量不是很多且非常好读的情况下使用，可以相对减小读全时间，其他字节为 0 即可。
Metadata Flags	2	参考 Metadata Flags 域
Option	1	参考 0x22 指令，注意:0xAA58 指令不支持匹配过滤。

域	字节长度	描述
Search Flags	2	低字节含义参考 0x22 指令，注意不支持嵌入数据功能。 高字节控制位参考 0xAA48 指令，注意不支持 BIT6 位单天线盘存无新增标签自动停止功能。
Access Password	0/4	含义与 0x22 指令相同。
Tag Singulation	N	含义与 0x22 指令相同。
Embedded Command Content	N	含义与 0x22 指令相同。

注意事项：

●盘存轮询规则参考异步盘存(0xAA48)注意事项中的轮询规则

●该命令适用于读大量标签的环境下，比如手持机盘点大量标签场景，智能柜档案柜大量标签场景，或者是有比较难读的场景，比如柜子里面的物品比较复杂难读的场景，标签堆叠难读场景等。

●该命令不需要指定 SESSION，TARGET，Q，RFMODE，命令内部自行处理，外面的设置不起作用。

●只有中国版，CE 版，INDIA，RUSSIA，PHILIPPINES，JAPAN，JAPAN2，JAPAN3，ISRAEL 版模块支持该命令，其他类似 FCC 标准的国家都不支持。

发送指令：

FF	13	AA	4D 6F 64 75 6C 65 74 65 63 68	AA 58
Header	Data Length	Command Code	Subcommand Marker (Moduletech)	Subcommand Code

00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	00 16	00	80 03	9B	BB	0A BF
ExConfigData	Metadata Flags	Option	Search Flags	SubCRC	Terminator	CRC

接收指令：

FF	0C	AA	00 00	4D 6F 64 75 6C 65 74 65 63 68	AA 58	0F 33
Header	Data Length	Command Code	Status Code	Subcommand Marker (Moduletech)	Subcommand Code	CRC

5.5.5 停止 EX 异步盘存(0xAA59)

指令描述

如启动了 EX 异步盘存操作，则可以使用此指令停止 EX 异步盘存。该指令遵从扩展指令通信协议格式。

指令属性

SubCommand Code	Bootloader 指令	App Firmware 指令	Subcommand Data
0xAA59	否	是	发送指令无，接收指令无

注意事项：

●如果模块在已经成功启动 EX 异步盘存指令后收到其他有效的指令（包括启动 EX 异步盘存指令），则模块退出 EX 异步盘存，并返回该有效指令的指令不成功应答，返回错误代码 0xAA59，其它代码为模块其它异常情况；

例如：开启异步盘存后发送 FF 00 03 1D 0C，则模块返回 FF 00 03 AA 59 1E EA。

●如果模块当前没启动 EX 异步盘存收到 EX 异步盘存命令停止指令，则返回执行成功；

指令实例：

发送指令：

FF	0E	AA	4D 6F 64 75 6C 65 74 65 63 68	AA 59	03	BB	E1 A0
Header	Data Length	Command Code	Subcommand Marker (Moduletech)	Subcommand Code	SubCRC	Terminator	CRC

接收指令：

FF	0C	AA	00 00	4D 6F 64 75 6C 65 74 65 63 68	AA 59	0F 32
Header	Data Length	Command Code	Status Code	Subcommand Marker (Moduletech)	Subcommand Code	CRC

5.6 清空缓存命令(0x2A)

原是在发送同步盘存命令（0x22）前使用，已无效现不需要。

6 标签访问指令

标签访问操作包括读取、写入、锁定和销毁等标签操作，需要对 Gen2 协议标签内存有一定的了解。Gen2 协议内存参考附录 4 Gen2 内存结构。标签访问指令遵从通用指令通信协议格式。

标签访问指令概述

指令	Command Code	描述
写标签 EPC	0x23	更新标签 EPC 码（会自动修改 PC 块内容），将影响盘存操作读出的 EPC ID 数据内容或长度。
写标签数据	0x24	将数据写入标签存储区中的指定地址，注意修改 EPCID 内容块是不会改变盘存时读出的 EPCID 的长度，只修改对应的数据块。
锁标签	0x25	锁定或解锁指定的标签内存区域
销毁标签	0x26	销毁标签
读标签数据	0x28	读取标签存储区域的内容。

注意事项：

●标签内存操作都必须先指定单个操作天线

●写标签内存需要的能量大于读标签内存的需要能量

6.1 写标签 EPC(0x23)

指令描述

用于更新标签 EPC 码，它与 0x24 命令的区别在于该命令根据用户写入的数据长度自动改变 PC 中指示 EPC 长度的位的值。该命令将 EPC ID 写入 EPC 区域中以 0x20（BITS）开始的地址。

指令属性

Command Code	Bootloader 指令	App Firmware 指令	Data 字段
0x23	否	是	发送指令有，未嵌入读指令时接收指令无，嵌入读指令时接收指令有。

发送指令 Data 字段格式

写标签 EPC(0x23) 发送指令时带有 Data 字段，此时 Data 字段包含了以下的域，如表：

域	字节长度	描述
Timeout	2	请参考 Timeout 域描述
WriteReadFlag	0/1	启用写入后读取存储区的功能，启用时需有此域并且固定值为 0x8C，不启用时将没有此域
Option	1	Option 域包含 Select-Option Bits 控制位和 Nol-Select-Option Bits-0x23 控制位，Nol-Select-Option Bits-0x23 须为 0
RFU	0/1	由 Option 域决定，当 WriteReadFlag 不存在且 Option=0x00 时，此域才存在,长度为 1，固定为 0x00。否则此域不存在。
Access Password	0/4	访问密码，如果 EPC bank 未锁定，则访问密码为 0x00000000，如果 EPC bank 已锁定，则密码必须正确。注意：当 Select-Option Bits

域	字节长度	描述
		= 0x00 时，命令中不包含访问密码。
Tag Singulation	N	过滤功能。请参考 Tag Singulation。由 Option 中的 Select-Option Bits 决定。如果没有启用过滤功能，则此域不存在。
Tag EPC ID	N	需要被写入的 EPC 码，最多 496 位（取决于标签）
ReadBank	1	指定要读取的标签区域，有 WriteReadFlag 域才有此域
Read Address	4	读取的起始地址，有 WriteReadFlag 域才有此域
Read Length	1	读取的数据字长度 ，有 WriteReadFlag 域才有此域

接收指令 Data 格式

0x23 指令带有嵌入读功能时的接收指令时带有 Data 字段，此时 Data 字段包含了以下的域：

域	字节长度	描述
WriteReadFlag	1	表示启用写入后读出存储区的功能，并且固定值为 0x8C。
Option	1	同发指令 Option
Read DATA	N	读取到的数据（长度为发送命令中指定的长度）

注意事项：

●当使用该命令时如果选择的盘存算法为 Dynamic Q 则模块内部将使用 Q=2 去盘存要更改 EPC 的标签，如果选择的是 Static Q 算法则按设置的 Q 值去盘存。

●须先指定单个操作天线。

指令实例：

例子 1：不启用选择匹配过滤。

发送指令：

FF	0C	23	03 E8	00	00	11 11 22 22 33 33 44 44	63 2C
Header	Data Length	Command Code	Timeout	Option	RFU	Tag EPC ID	CRC

接收指令：

FF	00	23	00 00	90 C1
Header	Data Length	Command Code	Status Code	CRC

例子 2：启用标签匹配过滤器，匹配过滤区域为 EPC bank，匹配地址为 0x00000020，匹配数据长度为 0x08 位，匹配数据为 0x11，匹配规则为选择不符合数据特征的标签，即地址 0x00000020 开始的数据不是 0x11 的标签被选择。

发送指令：

FF	19	23	03 E8	0C	00 00 00 00
Header	Data Length	Command Code	Timeout	Option	Access Password

00 00 00 20	08	11	11 11 22 22 33 33 44 44 55 55 66 66	57 3E
Select Address	Select Data Length	Select Data	Tag EPC ID	CRC

假若没有符合条件的标签，

接收指令：

FF	00	23	04 00	94 C1
Header	Data Length	Command Code	Status Code	CRC

例子 3：启用标签匹配过滤器，匹配滤波器区域为 EPC 区域，匹配地址为 0x00000020，匹配数据长度为 0x08 位，匹配数据为 0x11，即地址 0x00000020 开始的数据是 0x11 的标签被选择。

发送指令：

FF	19	23	03 E8	04	00 00 00 00
Header	Data Length	Command Code	Timeout	Option	Access Password

00 00 00 20	08	11	11 11 22 22 33 33 44 44 55 55 66 66	98 48
Select Address	Select Data Length	Select Data	Tag EPC ID	CRC

接收指令：

FF	00	23	00 00	90 C1
Header	Data Length	Command Code	Status Code	CRC

例子 4：写 EPC 数据：11 22 33 44 55 66 77 88 99 AA BB CC 11 22 33 44 55 66 77 88 99 AA BB CC 11 22 33 44 55 66 77 88 99 AA BB CC 11 22 33 44 55 66

并读出 CRC+PC+EPC，即读取 EPC 区起始地址 0，字长度 0x17 的内容

发送指令：

FF	34	23	03 E8	8C	00	11 22 33 44 55 66 77 88 99 AA BB CC 11 22 33 44 55 66 77 88 99 AA BB CC 11 22 33 44 55 66 77 88 99 AA BB CC 11 22 33 44 55 66
Header	Data Length	Command Code	Timeout	WriteReadFlag	Option	Tag EPC ID

01	00 00 00 00	17	E4 A5
ReadBank	Read Address	Read Length	CRC

接收指令：

FF	30	23	00 00	8C	00
Header	Data Length	Command Code	Status Code	WriteReadFlag	Option

54 B8 AC 00 11 22 33 44 55 66 77 88 99 AA BB CC 11 22 33 44 55 66 77 88 99 AA BB CC 11 22 33 44 55 66 77 88 99 AA BB CC 11 22 33 44 55 66	A6 B3
Read DATA	CRC

例子 5：Select Option=0x01，匹配过滤 EPC 区，Access Password=0x00000000，过滤位长度 0x20，过滤数据 0x11223344，

写 EPC 数据: 11 22 33 44 55 66 77 88 99 AA BB CC 11 22 33 44 55 66 77 88 99 AA BB CC 11 22 33 44 55 66 77 88 99 AA BB CC 11 22 33 44 55 66

并读出 TID 区，起始地址 0，字长度 0x06 的内容

发送指令：

FF	3D	23	03 E8	8C	01	00 00 00 00	20
Header	Data Length	Command Code	Timeout	WriteReadFlag	Option	Access Password	Select Data Length
11 22 33 44	11 22 33 44 55 66 77 88 99 AA BB CC 11 22 33 44 55 66 77 88 99 AA BB CC 11 22 33 44 55 66 77 88 99 AA BB CC 11 22 33 44 55 66				02	00 00 00 00	06	59 21
Select Data	Tag EPC ID				Read Bank	Read Address	Read Length	CRC

接收指令：

FF	0E	23	00 00	8C	01
Header	Data Length	Command Code	Status Code	WriteReadFlag	Option
E2 80 11 0C 20 00 77 0B 04 BE 09 71					3D 26
Read DATA					CRC

6.2 写标签(0x24)

指令描述

此命令用于将数据写入标签 bank 的指定地址中，首个响应读写器的标签会被实际操作。

指令属性

Command Code	Bootloader 指令	App Firmware 指令	Data 字段
0x24	否	是	发送指令有，未嵌入读指令时接收指令无，嵌入读指令时接收指令有。

发送指令 Data 字段格式

写标签数据(0x24) 发送指令时带有 Data 字段，此时 Data 字段包含了以下的域，如表：

域	字节长度	描述
Timeout	2	请参考 Timeout 域描述
WriteReadFlag	0/1	启用写入后读取存储区的功能，启用时需有此域并且固定值为 0x84，不启用时将没有此域
Option	1	Option 域包含 Select-Option Bits 控制位和 Nol-Select-Option Bits-0x24 控制位,Nol-Select-Option Bits-0x24 为 0 值。
Write Address	4	写入起始地址，字地址。从 0 开始。
Write MemBank	1	0x00 = Reserved bank，0x01 = EPC bank，0x02= TID bank，0x03 = USER bank
Access	0/4	访问密码。如果写入存储区未锁定，则访问密码为 0x00000000。

域	字节长度	描述
Password		如果内存区域已锁定，则密码必须正确。注意：当 Select-Option Bits = 0x00 时，命令中不包含访问密码。
Tag Singulation	N	过滤功能。请参考 Tag Singulation。由 Option 中的 Select-Option Bits 决定。如果没有启用过滤功能，则此域不存在。
Write Data	N	被写入的数据，写入数据字节长度必须是 2 的倍数，一次最多只能写入 32 个字，即 64 字节。
ReadBank	1	指定要读取的标签区域，有 WriteReadFlag 域才有此域
Read Address	4	读取的起始地址，有 WriteReadFlag 域才有此域
Read Length	1	读取的数据字长度 ，有 WriteReadFlag 域才有此域

接收指令 Data 格式

0x24 指令带有嵌入读功能时的接收指令时带有 Data 字段，此时 Data 字段包含了以下的域：

域	字节长度	描述
WriteReadFlag	1	表示启用写入后读出取存储区的功能，并且固定值为 0x84。
Option	1	同发指令 Option
Read DATA	N	读取到的数据（长度为发送命令中指定的长度）

注意事项：

●当使用该命令时如果选择的盘存算法为 Dynamic Q 则模块内部将使用 Q=2 去盘存要写入的标签，如果选择的是 Static Q 算法则按设置的 Q 值去盘存。

●须先指定单个操作天线。

指令实例：

例子 1：不使用标签匹配过滤，将 0xAAAABBBBCCCCDDDD 写入 USER bank 的起始地址 1。

Write Address=0x00000001；

Write MemBank=0x03

Write Data=0xAAAABBBBCCCCDDDD

发送指令：

FF	10	24	03 E8	00	00 00 00 01
Header	Data Length	Command Code	Timeout	Option	Write Address
03		AA AA BB BB CC CC DD DD		C7 B3	
Write MemBank		Write Data		CRC	

写失败，存储区锁定则：

接收指令：

FF	00	24	04 24	E4 02
Header	Data Length	Command Code	Status Code	CRC

例子 2：不使用标签匹配过滤，将 0xAAAABBBBCCCCDDDD 写入 USER bank 的起始地址 1。

Write Address=0x00000001

Write MemBank=0x03

Write Data=0xAAAABBBBCCCCDDDD

发送指令：

FF	10	24	03 E8	00	00 00 00 01	03
Header	Data Length	Command Code	Timeout	Option	Write Address	Write MemBank

AA AA BB BB CC CC DD DD	C7 B3
Write Data	CRC

写成功：

接收指令：

FF	00	24	00 00	E0 26
Header	Data Length	Command Code	Status Code	CRC

例子 3：使用标签匹配过滤

Write MemBank=0x00

Write Address=0x00000000

Write Data=0xAAAABBBBCCCCDDDD

Access Password=0xCCCCDDDD

Select MemBank=EPC bank

Select Address(bits)=0x00000020

Select Data Length(bits)=0x0C

Select Data=0x1110

发送指令：

FF	1B	24	03 E8	04	00 00 00 00	00
Header	Data Length	Command Code	Timeout	Option	Write Address	Write MemBank

CC CC DD DD	00 00 00 20	0C	11 10	AA AA BB BB CC CC DD DD	26 AA
Access Password	Select Address	Select Data Length	Select Data	Write Data	CRC

例子 4：使用标签匹配过滤

Write MemBank=0x03(USER bank)

Write Address=0x00000002
Write Data=0x1111222200000000
Access Password=0x00000000
Select MemBank=0x01 (EPC bank)
Select Data Length (bits) =0x60
Select Data=0x0123456789ABCDEF01234567

发送指令：

FF	21	24	03 E8	01	00 00 00 02	03	00 00 00 00
Header	Data Length	Command Code	Timeout	Option	Write Address	Write MemBank	Access Password

60	01 23 45 67 89 AB CD EF 01 23 45 67	11 11 22 22 00 00 00 00	27 03
Select Data Length	Select Data	Write Data	CRC

例子 5：

假设标签 Epc： 0xFFFF FFFF
Select Option=0x01，匹配过滤 EPC 区，Access Password=0x00000000，过滤位长度 0x20，过滤数据 0xFFFF FFFF，
写入 USER 区（0x03），起始地址 0x00000000，数据： 0xBBBB BBBB
读取 Tid 区数据（0x02），起始地址 0x00000002，数据长度 0x02

发送指令：

FF	1C	24	03 E8	84	01	00 00 00 00	03
Header	Data Length	Command Code	Timeout	WriteReadFlag	Option	Write Address	Write bank

00 00 00 00	20	FF FF FF FF	BBBB BBBB	02	00 00 00 02	02	41 5F
Access Password	Select Data Length	Select Data	Write Data	Read Bank	Read Address	Read Length	CRC

接收指令：

FF	06	24	00 00	84	01
Header	Data Length	Command Code	Status Code	WriteReadFlag	Option
20 00 FC 02					14 DF
Read DATA					CRC

例子 6：

假设标签 Epc： 0xFFFF FFFF，
Select Option=0x01，匹配过滤 EPC 区，Access Password=0x11112222，过滤位长度 0x20，过滤数据 0xFFFF FFFF，
写入 USER 区（0x03），起始地址 0x00000000，数据： 0xBBBB BBBB
读取 USER 区数据（0x03），起始地址 0x00000000，数据长度 0x02

发送指令：

FF	1C	24	03 E8	84	01	00 00 00 00	03
Header	Data Length	Command Code	Timeout	WriteReadFlag	Option	Write Address	Write bank

11112222	20	FF FF FF FF	BBBB BBBB	03	00 00 00 00	02	0B E6
Access Password	Select Data Length	Select Data	Write Data	Read Bank	Read Address	Read Length	CRC

接收指令：

FF	06	24	00 00	84	01
Header	Data Length	Command Code	Status Code	WriteReadFlag	Option
BB BB BB BB					81 C7
Read DATA					CRC

例子 7：Select Option=0x00,写入 USER 区（0x03），起始地址 0x00000000，数据：0xBBBB BBBB；读取 Tid 区数据（0x02），起始地址 0x00000002，数据长度 0x02

发送指令：

FF	13	24	03 E8	84	00	00 00 00 00	03
Header	Data Length	Command Code	Timeout	WriteReadFlag	Option	Write Address	Write bank
BBBB BBBB				03	00 00 00 00	02	0B E6
Write Data				Read Bank	Read Address	Read Length	CRC

接收指令：

FF	06	24	00 00	84	00
Header	Data Length	Command Code	Status Code	WriteReadFlag	Option
20 00 77 0B					A8 E6
Read DATA					CRC

6.3 锁标签(0x25)

指令描述

此命令用于锁定或解锁指定的标签存储区域，首个响应读写器的标签会被实际操作。

指令属性

Command Code	Bootloader 指令	App Firmware 指令	Data 字段
0x25	否	是	发送指令有，接收指令无

发送指令 Data 字段格式

锁标签(0x25) 发送指令时带有 Data 字段，此时 Data 字段包含了以下的域，如表：

域	字节长度	描述
Timeout	2	请参考 Timeout 域描述
Option	1	Option 域包含 Select-Option Bits 控制位。Option=0x05 不能用于此命令。
Access Password	4	标签访问密码
Mask Bits	2	见下图 6，对应的位为 1 时表示执行对应的 ACTIONBIT 位的操作。Mask Bits 是 Class-1 Generation-2 UHF RFID 规范中定义的术语。 有关详细信息，请参阅 Class-1 Generation-2 UHF RFID 规范。
Action Bits	2	ACTIONBIT 中的位只有当对应的 MASKBIT 位为 1 时才起作用。0 为解锁，1 为锁定。 Action Bits 是 Class-1 Generation-2 UHF RFID 规范中定义的术语。 有关详细信息，请参阅 Class-1 Generation-2 UHF RFID 规范。
Tag Singulation	N	过滤功能。请参考 Tag Singulation。由 Option 中的 Select-Option Bits 决定。如果没有启用过滤功能，则此域不存在。

	First Byte								Second Byte							
Bit	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
	Unused						Kill Pwd		Access Pwd		EPC Mem		TID Mem		User Mem	
Mask	X	X	X	X	X	X	Set?	Set?	Set?	Set?	Set?	Set?	Set?	Set?	Set?	Set?
Action	X	X	X	X	X	X	R/W	Perm	R/W	Perm	W	Perm	W	Perm	W	Perm

图 6

图 6 所示，mask 和 action 域都是 2 个字节，且低 10 位有效。Mask 域低 10 位对应 action 域低 10 位是否有效。Action 域 控制位 R/W 表示读写锁操作类型，置 1 为锁定；置 0 为解锁。 控制位 W 表示写锁操作类型，置 1 为锁定；置 0 为解锁。控制位 Perm 表示锁类型，1 为永久锁，永久锁表示无法解锁也无法写入；0 为临时锁可以解锁。

注意事项：

●当使用该命令时如果选择的盘存算法为 Dynamic Q 则模块内部将使用 Q=2 去盘存要 LOCK 的标签，如果选择的是 Static Q 算法则按设置的 Q 值去盘存。

●Option=0x05 不能用于此命令。

●须先指定单个操作天线。

指令实例：

例子 1

过滤 EPC ID=0x111122223333444455556666, access password=0x11223344，使能标签过滤并锁定 EPC bank

发送指令：

FF	18	25	03 E8	01	11 22 33 44	00 20	00 20	60	11 11 22 22 33 33 44 44 55 55 66 66	9E 7A
Header	Data Length	Command Code	Timeout	Option	Access Password	Mask Bits	Action Bits	Select Data Length	Select Data	CRC

例子 2

access password=0x11223344，使能标签过滤 EPCID 首字节为 0x11 并锁定 EPC bank

发送指令：

FF	11	25	03 E8	04	11 22 33 44	00 20	00 20	00 00 00 20	08	11	94 32
Header	Data Length	Command Code	Timeout	Option	Access Password	Mask Bits	Action Bits	Select Address	Select Data Length	Select Data	CRC

例子 3

access password=0x11223344，不启用选择匹配过滤，过滤并锁定 USER bank

发送指令：

FF	0B	25	03 E8	00	11 22 33 44	00 02	00 02	0F A9
Header	Data Length	Command Code	Timeout	Option	Access Password	Mask Bits	Action Bits	CRC

6.4 销毁标签(0x26)

指令描述

此命令使标签失效，不能被识别。

指令属性

Command Code	Bootloader 指令	App Firmware 指令	Data 字段
0x26	否	是	发送指令有，接收指令无

发送指令 Data 字段格式

销毁标签(0x26) 发送指令时带有 Data 字段，此时 Data 字段包含了以下的域，如表：

域	字节长度	描述
Timeout	2	请参考 Timeout 域描述
Option	1	Option 域包含 Select-Option Bits 控制位和 Nol-Select-Option Bits-0x26 控制位,Nol-Select-Option Bits-0x26 为 0 值。Option=0x05 不能用于此命令。
Kill Password	4	标签的销毁密码
RFU	1	保留，目前必须为 0x00

域	字节长度	描述
Tag Singulation	N	过滤功能。请参考 Tag Singulation。由 Option 中的 Select-Option Bits 决定。如果没有启用过滤功能，则此域不存在。

注意事项：

●当使用该命令时如果选择的盘存算法为 Dynamic Q 则模块内部将使用 Q=2 去盘存要 KILL 的标签，如果选择的是 Static Q 算法则按设置的 Q 值去盘存。

●须先指定单个操作天线。

指令实例：

例子 1:不使能标签过滤

发送指令：

FF	08	26	03 E8	00	11 22 33 44	00	91 16
Header	Data Length	Command Code	Timeout	Option	Kill Password	RFU	CRC

例子 2:使能标签过滤，过滤 bank 为 USER

发送指令：

FF	10	26	03 E8	03	11 22 33 44	00	00 00 00 00	18	11 11 22	BF 40
Header	Data Length	Command Code	Time out	Option	Kill Password	RFU	Select Address	Select Data Length	Select Data	CRC

例子 3:使能标签过滤，过滤 bank 为 EPC

发送指令：

FF	13	26	03 E8	01	11 11 22 22	00	50	11 22 33 44 55 66 77 88 99 AA	B969
Header	Data Length	Command Code	Timeout	Option	Kill Password	RFU	Select Data Length	Select Data	CRC

6.5 读标签储存区(0x28)

指令描述

读取标签存储区域的内容。标签储存区地址分布可参考附录 4 Gen2 标签内存结构

指令属性

Command Code	Bootloader 指令	App Firmware 指令	Data 字段
0x28	否	是	发送指令有，接收指令有

发送指令 Data 字段格式

读标签存储区(0x28) 发送指令时带有 Data 字段，此时 Data 字段包含了以下的域，如表：

域	字节长度	描述
Timeout	2	请参考 Timeout 域描述

域	字节长度	描述
Option	1	Option 域包含 Select-Option Bits 控制位和 Nol-Select-Option Bits-0x28 控制位
Metadata Flags	0/2	由 Option 域的 Nol-Select-Option Bits-0x28 控制位(BIT4)决定，设置为 1 时，此域才存在,长度为 2。否则此域不存在。该域告诉读写器要返回的元数据。
Read MemBank	1	指定读取的存储区，0x00 = RESERVED bank; 0x01 = EPC bank; 0x02 = TID bank; 0x03 = USER bank
Read Address	4	读取起始地址，即从 0 开始的存储区的块地址。
Word Count	1	要读取的块数，一次最多读 96 块
Access Password	0/4	访问密码，如果内存区域未锁定，则密码为 Access Password = 0x00000000; 如果内存区域被锁定，则访问密码必须正确。注意：当 Select-Option Bits= 0x00 时，命令中不包含访问密码。
Tag Singulation	N	过滤功能。请参考 Tag Singulation。由 Option 中的 Select-Option Bits 决定。如果没有启用过滤功能，则此域不存在。

接收指令 Data 字段格式

读标签存储区(0x28) 接收指令时带有 Data 字段

有两种不同的数据字段格式，具体取决于发送指令 Option 域的 BIT4 是否为 1，为 1 包含是否包含 Metadata Flags 域。第一种是只获取存储区数据，发送指令中没有 Metadata Flags 域。 另一种是存储区数据和元数据，在发送指令中必须有 Metadata Flags 域。

获取存储区数据

发送指令中 Option 域的 BIT4 为 0，没有 Metadata Flags 域时，接收指令时带有 Data 字段，此时 Data 字段包含了以下的域，如表：

字段	字节长度	描述
Option	1	与发送指令的 Option 字段相同。
Data Read	N	读到的标签存储区数据。

发送指令中 Option 域的 BIT4 为 1，有 Metadata Flags 域时，接收指令时带有 Data 字段，此时 Data 字段包含了以下的域，如表：

字段	字节长度	描述
Option	1	与发送指令的 Option 字段相同。
Metadata Flags	2	与发送指令中的 Metadata Flags 字段相同。
Metadata	N	Metadata 域长度由 Metadata Flags 决定

注意事项：

●当使用该命令时如果选择的盘存算法为 Dynamic Q 则模块内部将使用 Q=2 去盘存要读取存储区的标签，如果选择的是 Static Q 算法则按设置的 Q 值去盘存。

●须先指定单个操作天线。

指令实例：

例子 1:禁用标签匹配过滤功能，并读取 TID 区中从地址 1 开始的 2 个块。

发送指令：

FF	09	28	03 E8	00	02	00 00 00 01	02	C1 F3
Header	Data Length	Command Code	Timeout	Option	Read MemBank	Read Address	Word Count	CRC

接收指令：

FF	05	28	00 00	00	60 04 01 35	13 04
Header	Data Length	Command Code	Status Code	Option	Data Read	CRC

例子 2

启用标签匹配过滤功能，读取 TID 区中从地址 1 开始的 3 个块，password = 0x00000000，
匹配区域为 TID 区域，起始地址为 0x10（BITS），匹配长度为 4 位，匹配数据为 0x60。

发送指令：

FF	13	28	03 E8	02	02	00 00 00 01
Header	Data Length	Command Code	Timeout	Option	Read MemBank	Read Address

03	00 00 00 00	00 00 00 10	04	60	7C 91
WordCount	Access Password	Select Address	Select Data Length	Select Data	CRC

接收指令：

FF	07	28	00 00	02	60 04 01 35 F8 69	6C 29
Header	Data Length	Command Code	Status Code	Option	Data Read	CRC

例子 3

过滤 EPC ID = 0x0123456789ABCDEF01234567，读取 USER 区域，启用标签匹配过滤。

发送指令：

FF	1A	28	03 E8	01	03	00 00 00 02
Header	Data Length	Command Code	Timeout	Option	Read MemBank	Read Address

04	00 00 00 00	60	01 23 45 67 89 AB CD EF 01 23 45 67	7A C1
Word Count	Access Password	Select Data Length	Select Data	CRC

接收指令：

FF	09	28	00 00	01	AA BB CC DD 00 00 00 00	E7 54
Header	Data Length	Command Code	Status Code	Option	Data Read	CRC

例子 4：读取标签数据同时返回标签元数据

发送指令：

FF	15	28	03 E8	14	00 14	00	00 00 00 02
Header	Data Length	Command Code	Timeout	Option	Metadata Flags	Read MemBank	Read Address

02	00 00 00 00	00 00 00 78	08	34	9C 0E
WordCount	Access Password	Select Address	Select Data Length	Select Data	CRC

接收指令：

FF	0C	28	00 00	14	00 14	02	00 00 00 15	12 34 56 78	DC42
Header	Data Length	Command Code	Status Code	Option	Metadata Flags	Antenna ID	Timestamp	Tag Data	CRC

6.6 写标签(0x2D)

指令描述

此命令当标签支持块写功能时即可使用块写命令，能够更加快速的把数据写入标签存储区。

指令属性

Command Code	Bootloader 指令	App Firmware 指令	Data 字段
0x2D	否	是	发送指令有，接收指令无。

发送指令 Data 字段格式

块写标签数据(0x2D) 发送指令时带有 Data 字段，此时 Data 字段包含了以下的域，如表：

域	字节长度	描述
Timeout	2	请参考 Timeout 域描述
Chip Type	1	0x00
Option	1	Option 域包含 Select-Option Bits 控制位和 Nol-Select-Option Bits-0x2D 控制位，且 Nol-Select-Option Bits-0x2D 控制位(BIT6)需为 1.
Sub Command write	2	固定 0x00C7，BLOCK WRITE。

域	字节长度	描述
Access Password	0/4	访问密码，如果内存区域未锁定，则密码为 Access Password = 0x00000000；如果内存区域被锁定，则访问密码必须正确。注意：由于 BIT6 须为 1，所以 Option= 0x40 时，命令中不包含访问密码。
Tag Singulation	N	过滤功能。请参考 Tag Singulation。由 Option 中的 Select-Option Bits 决定。如果没有启用过滤功能，则此域不存在。
Write Flags	1	0x00
Write MemBank	1	指定块写存储区：0x00 = Reserved bank，0x01 = EPC bank，0x02= TID bank，0x03 = USER bank
Write Address	4	写入起始地址，字地址（16BITS）从 0 开始。
WordCount	1	写入的字数（16BITS），最多一次写入 48 个字。
Data	2*WordCount	写入的数据，为 WordCount*2 个字节。

注意事项：

●当使用该命令时如果选择的盘存算法为 Dynamic Q 则模块内部将使用 Q=2 去盘存要进行块写的标签，如果选择的是 Static Q 算法则按设置的 Q 值去盘存。

●须先指定单个操作天线。

指令实例：

例子 1：启用选择匹配过滤功能：

发送指令：

FF	19	2D	03 E8	00	44	00 C7
Header	Data Length	Command Code	Timeout	Chip type	Option	Sub Command write

11 22 33 44	00 00 00 78	08	34	00	00	00 00 00 00	01	00 00	90 E3
Access password	Select Address	Select data length	Select data	Write Flag	Write MemBank	Write Address	Word count	Data	CRC

接收指令：

FF	00	2D	00 00	710F
Header	Data Length	Command Code	Status Code	CRC

例子 2：不启用选择匹配过滤功能。

发送指令：

FF	15	2D	03 E8	00	40	00 C7
Header	Data Length	Command Code	Timeout	Chip type	Option	Sub Command write

00	03	00 00 00 00	04	11 11 22 22 33 33 44 44	8D 2D
Write Flags	Write MemBank	Write Address	WordCount	Data	CRC

接收指令：

FF	00	2D	00 00	710F
Header	Data Length	Command Code	Status Code	CRC

7 设置指令

设置命令用于设置固件中的可配置值。由于这些值未存储在读写器 Flash 中，因此只要重新启动应用程序固件，这些值就会重置为默认值。设置指令遵从通用指令通信协议格式。

设置命令概述

命令	Command Code	描述
设置天线端口	0x91	配置天线端口，可配置项包括：标签访问操作使用的天线，盘存操作使用的天线，读写器发射功率等。
设置当前标签协议	0x93	设置操作的标签协议。
设置跳频配置	0x95	设置跳频表和监管跳频时间。
设置 GPIO	0x96	设置和获取 GPIO 引脚的状态
设置当前工作区域	0x97	设置读写器的当前工作区域
设置读写器配置	0x9A	设置读写器的配置选项。
设置标签协议配置	0x9B	设置标签协议特定的配置参数。

7.1 设置天线端口(0x91)

指令描述

该命令使用逻辑天线编号的概念。读写器的逻辑天线编号与读取器上标有数字的物理天线端口号不同。逻辑天线分为用于接收的天线和用于发射的天线。用于接收的天线的逻辑天线编号称为 RX Logical Antenna Number。用于发射的天线的逻辑天线编号称为 TX Logical Antenna Number。

目前我公司的所有读写器产品都采用收发一体天线模式，即读写器的某个物理天线端口工作时，该端口既发射也接收信号。

模块分别有 1、2、4、8、16、32 个天线口的模块，设置天线命令有多种格式，设置命令中的天线逻辑号与实际物理天线口的对应关系如下：

TX ANT NUM（天线逻辑号）	RX ANT NUM（天线逻辑号）	实际物理天线口
0x01	0x01	天线口 1
0x02	0x02	天线口 2
…	…	…
0x20	0x20	天线口 32

目前模块上电默认使能逻辑天线口 1 工作，也即是物理天线口 1，所有天线上电默认初始发射功率为模块的最大功率。

指令属性

Command Code	Bootloader 指令	App Firmware 指令	Data 字段
0x91	否	是	发送指令有， 接收指令无。

发送指令 Data 字段格式

设置天线端口(0x91) 发送指令时带有 Data 字段

有三种不同的数据字段格式，具体取决于发送指令是否包含 Option 域或者 Option 域值。第一种是只设置单个天线口工作，发送指令中没有 Option 域。 第二种是有 Option=0 或 2 设置单个或多个天线口工作。第三种是有 Option=3 或 4，设置天线口的发射功率与天线配置时间。

设置天线端口(0x91）设置单个或多个天线口工作发送指令时带有 Data 字段，此时 Data 字段包含了以下的域，如表：

域	字节长度	描述
Option	0/1	设置单个天线口时，Option 域可以不存在或者值为 0 或者 2，设置多个天线口时 Option 必须存在并且固定为 2 值。
TX,RX Logical Antenna Number pairs	N*2（N 最小值为 1，最大值为 32）	N 个 2 字节 TX,RX Logical Antenna Number pairs，第一字节为 TX，第二字节为 RX。具体根据模块的天线口数以及所要使能工作的天线数，单口天线模块就只有一组。模块默认上电是使能物理天线口 1 工作，设置多个天线工作时，天线的工作顺序是按照从物理天线口 1->2>...->32 顺序工作的。天线逻辑号对参数在命令中可以不分顺序。

设置天线端口(0x91）设置天线口的发射功率与天线配置时间发送指令时带有 Data 字段，此时 Data 字段包含了以下的域，如表：

域	字节长度	描述
Option	1	Option=0x03 时只是设置发射功率； Option=0x04 时设置发射功率与天线配置时间。
TX Logical Antenna Power Configuration	N*5/N*7	N 个 TX Logical Antenna Power Configuration

TX Logical Antenna Power Configuration

域	字节长度	描述
TX Logical Antenna Number	1	
Read Power	2	读取相关操作的发射功率，单位为 0.01dBm，目前实际精度为 1dBm。
Write Power	2	写入相关操作的发射功率，单位为 0.01dBm，目前实际精度为 1dBm。
Setting Time	0/2	在天线切换时，用于配置天线所需的稳定时间，单位μs。Option=0x04 才存在此域

指令实例：

例子 1：设置天线端口 1 作为标签访问操作使用的天线（Option = 0x00）

发送指令：

FF	03	91	00	01	01	62 87
Header	Data Length	Command Code	Option	TX Logical Antenna Number	RX Logical Antenna Number	CRC

例子 2：设置物理天线端口 1 和 4 作为标签盘存使用的天线（Option = 0x02）

发送指令：

FF	05	91	02	01	01	04	04	2B C6
Header	Data Length	Command Code	Option	TX Logical Antenna Number	RX Logical Antenna Number	TX Logical Antenna Number	RX Logical Antenna Number	CRC

例子 3：设置天线功率（Option = 0x03），设置物理天线端口 2 和 3 的功率 30dBm。

发送指令：

FF	0B	91	03	02	03 E8	0B B8	03	03 E8	0B B8	F2 F5
Header	Data Length	Command Code	Option	TX Logical Antenna Number	Read Power	Write Power	TX Logical Antenna Number	Read Power	Write Power	CRC

例子 4：设置天线端口 1,2,3 和 4 的的功率和 Setting Time（Option = 0x04）

发送指令：

FF	1D	91	04	01	03 E8	0B B8	01 F4	03	03 E8	0B B8
Header	Data Length	Command Code	Option	TX Logical Antenna Number	Read Power	Write Power	Setting Time	TX Logical Antenna Number	Read Power	Write Power

01 F4	02	03 E8	0B B8	01 F4	04	03 E8	0B B8	01 F4	78 85
Setting Time	TX Logical Antenna Number	Read Power	Write Power	Setting Time	TX Logical Antenna Number	Read Power	Write Power	Setting Time	CRC

7.2 设置当前标签协议(0x93)

指令描述

设置操作使用的标签协议。目前所有读写器都只支持 GEN2（18000-6C）协议。当读写器开机时，默认使用 GEN2（18000-6C）协议，因此您无需使用此命令。

指令属性

Command Code	Bootloader 指令	App Firmware 指令	Data 字段
0x93	否	是	发送指令有， 接收指令无。

发送指令 Data 字段格式

设置当前标签协议(0x93) 发送指令时带有 Data 字段，此时 Data 字段包含了以下的域：

域	字节长度	描述
Current Protocol	2	目前所有读写器都只支持 GEN2（18000-6C）协议，该字段必须为 0x0005。

指令实例：

发送指令：

FF	02	93	00 05	51 7D
Header	Data Length	Command Code	Current Protocol	CRC

7.3 设置跳频配置(0x95)

指令描述

此命令设置读写器的跳频表以及可选的跳频时间，每个频率编码为以 kHz 为单位的 32 位值。

命令可设置的最大频率数量为 50。某个工作区域的可设置频率可以参考附录 3 工作区域以及区域频率表。

指令属性

Command Code	Bootloader 指令	App Firmware 指令	Data 字段
0x95	否	是	发送指令有， 接收指令无

发送指令 Data 字段格式

设置跳频配置(0x95) 发送指令时带有 Data 字段，此时 Data 字段包含了以下的域，如表：

域	字节长度	描述
frequencies	N*4	N 个频率，每个频率 4 个字节长

设置异步盘存天线驻留时间或跳频时间(0x95) 发送指令时带有 Data 字段，此时 Data 字段包含了以下的域，如表：

域	字节长度	描述
Option	1	Option=0x01 时为跳频时间，Option=0x02 时为天线驻留时间 目前 Option=0x01 无效。
Timeout	4	单位毫秒，取值范围为 20-60000

注意事项：

●目前仅有中国版跟 CE 版模块可设置频点，其他国家版本不行
若设置的频点非当前工作区域频段则先要修改正确的工作区域（0x97）再设置频点

指令实例：

设置跳频表，设置三个频率：915250kHz，903250kHz 和 926750kHz。

发送指令：

FF	0C	95	00 0D F7 32	00 0D C8 52	00 0E 24 1E	E5 24
Header	Data Length	Command Code	915250kHz	903250kHz	926750kHz	CRC

7.4 设置 GPO(0x96)

指令描述

此命令有两种格式用于设置 gpo 和获取 gpo 状态。不同的读写器类型具有不同的 gpio 数量。该系列模块支持 2 路输出

指令属性

Command Code	Bootloader 指令	App Firmware 指令	Data 字段
0x96	否	是	用于设置功能时发送指令有，接收指令无。 用于获取功能是发送指令无，接收指令有。

发送指令 Data 字段格式

0x96 指令用于设置时，发送指令时带有 Data 字段，此时 Data 字段包含了以下的域，如表：

域	字节长度	描述
Gpo Number and Status pairs	N*2	N 个 Gpo 编号和状态对，每对是 2 个字节（第一个字节是 GPO 编号，第二个字节是状态）

接收指令 Data 格式

0x96 指令用于获取时， 接收指令时带有 Data 字段，此时 Data 字段包含了以下的域：

域	字节长度	描述
Status of Gpo pins	N	按数字顺序返回的所有 gpo 的状态。每个引脚状态为一字节，0 为低电平，1 为高电平。

指令实例：

例子 1：设置 Gpo

发送指令：

FF	04	96	01	01	02	00	2F 68
Header	Data Length	Command Code	Output #1	Status of Output #1	Output #2	Status of Output #2	CRC

例子 2：获取上次设置的 Gpo 状态

接收指令：

FF	02	96	00 00	01	00	28 E1
Header	Data Length	Command Code	Status Code	Status of Output #1	Status of Output #2	CRC

7.5 设置当前工作区域(0x97)

指令描述

每个国家都有其合法的工作区域

指令属性

Command Code	Bootloader 指令	App Firmware 指令	Data 字段
0x97	否	是	发送指令有， 接收指令无

发送指令 Data 字段格式

设置工作区域(0x97) 发送指令时带有 Data 字段，此时 Data 字段包含了以下的域，如表：

域	字节长度	描述
Region Code	1	请参考附录 3 工作区域以及区域频率表

注意事项：

●当使用 0x95 命令设置频点时，当前设置模块工作在哪个频段区域，就只能设置该区域对应的跳频表里面的频点。

指令实例：

实例 1：设置工作区域为 North America.

发送指令：

FF	01	97	01	4B BC
Header	Data Length	Command Code	Region Code	CRC

实例 2：设置工作频率区域为中国 1 频段。

发送指令：

FF	01	97	06	4B BB
Header	Data Length	Command Code	Region Code	CRC

接收指令：

FF	00	97	00 00	77 9E
Header	Data Length	Command Code	Status	CRC

7.6 设置读写器配置(0x9A)

指令描述

该命令用于设置读写器的多个配置选项。

指令属性

Command Code	Bootloader 指令	App Firmware 指令	Data 字段
0x9A	否	是	发送指令有， 接收指令无

发送指令 Data 字段格式

0x9A 指令，发送指令时带有 Data 字段，此时 Data 字段包含了以下的域，如表：

域	字节长度	描述
Option	1	必须是 0x01
Key	1	配置项，详细说明请参见后面键值描述表
Value	1	配置项的值，详细说明请参阅后面键值描述表

键值描述表

Key	Value	描述
0x00：使用天线端口作为标签缓冲区条目的唯一标识之一	0x00	天线端口是标签缓冲区条目的唯一标识之一（上电默认值），即不同天线相同标签 EPCID 的两条盘点数据在缓冲产生两条条目。
	0x01	天线端口不作为标签缓冲区条目的唯一标识之一，即同一 EPCID 的标签，不同天线端口的两条盘点数据在缓冲只产生一条条目。记录最后的天线端口。
0x06：记录所见的最大 RSSI	0x00	盘存时不记录标签最大 RSSI 值，读到同一标签时记录最后一次读到的 RSSI 值（上电默认值）
	0x01	盘存时记录标签最大 RSSI 值
0x08:将 bank 数据（附加数据)作为标签缓冲区条目的唯一标识之一	0x00	标签 bank 数据是标签缓冲区条目的唯一标识之一，即不同附加数据相同标签 EPCID 的两条盘点数据在缓冲产生两条条目。
	0x01	标签 bank 数据不是标签缓冲区条目的唯一标识之一(上电默认值)。即同一 EPCID 的标签，不同附加数据的两条盘点数据在缓冲只产生一条条目。记录最后的附加数据。

指令实例：

设置使用天线端口作为标签缓冲区条目的唯一标识之一

发送指令：

FF	03	9A	01	00	01	AF 5C
Header	Data Length	Command Code	Option	Key	Value	CRC

接收指令：

FF	00	9A	00 00	A6 33
Header	Data Length	Command Code	Status Code	CRC

7.7 设置标签协议配置(0x9B)

指令描述

该命令用于设置协议特定的配置参数。

指令属性

Command Code	Bootloader 指令	App Firmware 指令	Data 字段
0x9B	否	是	发送指令有， 接收指令无

发送指令 Data 字段格式

设置标签协议配置(0x9B)，发送指令时带有 Data 字段，此时 Data 字段包含了以下的域：

域	字节长度	描述
Protocol Value	1	必须是 0x05，现在所有读写器都只支持 Gen2 协议。
Parameter	1	协议参数，详细说明请参见协议参数选项表。
Option	1	参数的一个选项，对于某些参数，没包括这个字段。 详细说明请参阅协议参数选项表。
Value	1	带有 Option 的 Parameter 的值，对于某些参数，没有这个字段，详细说明请参阅协议参数选项表。

协议参数选项表

Parameter	Option	Value
0x00：盘存时使用的 Session	无此域	0x00: Session 0 (上电默认值)
		0x01: Session 1
		0x02: Session 2
		0x03: Session 3
0x01：盘存时使用的 Target	0x01：静态 Target	0x00: Target A (上电默认值)
		0x01: Target B
	0x00：动态 Target，从 A 翻转到 B 或从 B 翻转到 A。	0x00：从 A 启动盘存并翻转到 B，直到找不到标签。 （仅适用于 0x22 命令;如果动态 Target 用于 0x22 命令，并且静态 Q 未针对其他命令操作（如读取，写入和锁定）重置，则使用 Target A 执行其他命令操作）
		0x01：从 B 启动盘存并翻转到 A，直到找不到标签。 （仅适用于 0x22 命令;如果动态目标用于 0x22 命令操作，并且静态 Q 未针对其他命令操作（如读取，写入和锁定）重置，则使用目标 A 执行其他命令操作）
0x02：RF MODE 选项	无此域	设置值对应的 RF MODE*
0x12: Q 值	0x00：动态 Q（读写器根据盘存状况自动更改 Q 值，开机默认值）	无此字段

Parameter	Option	Value
	0x01:静态 Q	0x00~0x0F (1 字节, Q value)

注意事项：

●RF MODE 设置值对应的 RF MODE 如下，设置值为下面的 MODE ID 值加一百，比如设置值 0x65（十进制 101）表示使用 MODE ID 1，设置值 0x70（十进制 112）表示使用 MODE ID 12：

Table 10: Impinj Reader Chip RF Mode Parameters and Performance

Mode ID	Mode Optimization	Forward Link Modulation	Tari (µs)	PIE	BLF (kHz)	Reverse Link Modulation	Chip Receive Sensitivity Minimum* (dBm)			Maximum Read Rate** (tags/s)
							E710	E510	E310	
11	Read Rate	PR-ASK	7.5	2	640	FM0	-78	N/A	N/A	700+
1	Read Rate	PR-ASK	7.5	2	640	Miller M=2	-81	-75	N/A	550+
15	Read Rate	PR-ASK	7.5	2	640	Miller M=4	-84	-78	N/A	400+
12	ETSI	PR-ASK	15	2	320	Miller M=2	-84	-78	-71	300+
3	ETSI	PR-ASK	20	2	320	Miller M=2	-84	-78	-71	250+
5	ETSI DRM	PR-ASK	20	2	320	Miller M=4	-87	-81	-74	200+
7	FCC DRM	PR-ASK	20	2	250	Miller M=4	-88	-82	-75	150+
13	Sensitivity	PR-ASK	20	2	160	Miller M=8	-93	-87	-80	50+

指令实例：

实例 1：设置 Session 1

发送指令：

FF	03	9B	05	00	01	DC E9
Header	Data Length	Command Code	Protocol Value	Parameter	Value	CRC

实例 2：设置静态 Q 值为 3

发送指令：

FF	04	9B	05	12	01	03	80 AC

Header	Data Length	Command Code	Protocol Value	Parameter	Option	Value	CRC

实例 3：设置 Target B

发送指令：

FF	04	9B	05	01	01	01	A2 FC
Header	Data Length	Command Code	Protocol Value	Parameter	Option	Value	CRC

8 获取指令

下表中列出的获取命令用于从读写器获取参数，选项和工作状态等。获取指令遵从通用指令通信协议格式。

获取命令概述

命令	Command Code	描述
获取天线端口配置	0x61	获取天线端口的配置（标签访问操作的天线，盘存使用的天线以及天线端口的发射功率等）
获取读功率发射信息	0x62	获取默认功率，功率范围
获取当前标签协议	0x63	获取当前标签操协议。
获取跳频设置	0x65	获取跳频表和监管跳频时间。
获取 GPI	0x66	获取 Gpi 引脚的状态
获取当前工作区域	0x67	获取当前读写器工作区域
获取可用工作区域	0x71	获取读写器支持工作区域
获取读写器配置	0x6A	获取读写器的配置
获取标签协议配置	0x6B	获取标签协配置
获取当前温度	0x72	获取读写器当前温度

8.1 获取天线端口配置(0x61)

指令描述

该命令返回读写器的天线配置，配置内容包括使用哪些天线发送和接收，天线端口的发射功率等。 命令有多种格式，我们将分别介绍每一种命令格式。

指令属性

Command Code	Bootloader 指令	App Firmware 指令	Data 字段
0x61	否	是	发送指令有， 接收指令有

发送指令 Data 字段格式

获取天线端口配置(0x61)，发送指令时带有 Data 字段，此时 Data 字段包含了以下的域：

域	字节长度	描述
Option	1	详细说明参见下表

Option 值	描述
0x00	如果使用过 0x91 命令设置标签访问操作使用的天线，此命令将返回 0x91 命令设置过的信息。 如果没有使用过 0x91 命令设置标签访问操作使用的天线，则将返回最小的逻辑天线编号。
0x02	获取盘存使用的逻辑天线。
0x03	获取所有逻辑天线端口的读写发射功率。
0x04	获取所有逻辑天线端口的读写发射功率和天线设置时间。

Option 值	描述
0x05	获取所有逻辑天线端口的连接状态。目前模块是采用开关电平状态来判断是否有天线连接，只能判别闭环的天线

接收指令 Data 格式

获取天线端口配置(0x61) 接收指令时带有 Data 字段，此时 Data 字段根据 Option 值不同而不同，如表：

Option 值	字节长度	描述
0	2	1 对天线配置信息。第一字节为 TX Logical Antenna Number，第二字节为 RX Logical Antenna Number
2	2*N	N 对天线配置信息。
3	5*N	N 对天线功率信息，天线功率信息由按以下项顺序组成： 1 字节 Logical Antenna，2 字节 Read Power，2 字节 Write Power
4	7*N	N 对天线功率时间信息，天线功率时间信息由按以下项顺序组成：1 字节 Logical Antenna，2 字节 Read Power，2 字节 Write Power，2 字节 Setting Time。注意：设置时间目前没有实际意义。
5	2*N	N 对天线连接状态信息。天线连接状态信息由按以下项顺序组成：1 字节 Logical Antenna，1 字节 connection status，1 为连接状态 0 为未连接状态。

指令实例：

例子 1：获取标签访问操作的天线。

发送指令：

FF	01	61	00	BD BD
Header	Data Length	Command Code	Option	CRC

接收指令：

FF	02	61	00 00	03	03	4C 20
Header	Data Length	Command Code	Status Code	TX Logical Antenna Number	RX Logical Antenna Number	CRC

例子 2：获取盘存使用的天线

发送指令：

FF	01	61	02	BD BF
Header	Data Length	Command Code	Option	CRC

接收指令：

FF	05	61	00 00	02	03	03	04	04	74 39
Header	Data Length	Command Code	Status Code	Option	TX Logical Antenna Number	RX Logical Antenna Number	TX Logical Antenna Number	RX Logical Antenna Number	CRC

例子 3：获取所有天线端口的读写发射功率，假定为 30dBm。

发送指令：

FF	01	61	03	BD BE
Header	Data Length	Command Code	Option	CRC

接收指令：

FF	15	61	00 00	03	01	0B B8	0B B8	02	0B B8	0B B8
Header	Data Length	Command Code	Status Code	Option	TX Logical Antenna Number	Read Power	Write Power	TX Logical Antenna Number	Read Power	Write Power

03	0B B8	0B B8	04	0B B8	0B B8	F7 6F
TX Logical Antenna Number	Read Power	Write Power	TX Logical Antenna Number	Read Power	Write Power	CRC

例子 4：获取所有天线端口的读/写发射功率和设置时间，假设为 30dBm，设置时间目前没有实际意义。

发送指令：

FF	01	61	04	BD B9
Header	Data Length	Command Code	Option	CRC

接收指令：

FF	1D	61	00 00	04	01	0B B8	0B B8	01 F4	02	0B B8	0B B8
Header	Data Length	Command Code	Status Code	Option	TX Logical Antenna Number	Read Power	Write Power	Setting Time	TX Logical Antenna Number	Read Power	Write Power

01 F4	03	0B B8	0B B8	01 F4	04	0B B8	0B B8	01 F4	25 27
Setting Time	TX Logical Antenna Number	Read Power	Write Power	Setting Time	TX Logical Antenna Number	Read Power	Write Power	Setting Time	CRC

例子 4：获取所有逻辑天线口的连接状态

发送指令：

FF	01	61	05	BD B8
Header	Data Length	Command Code	Option	CRC

接收指令：

FF	11	61	00 00	05
Header	Data Length	Command Code	Status Code	Option

01	00	02	00	03	00
TX Logical Antenna Number	connection status	TX Logical Antenna Number	connection status	TX Logical Antenna Number	connection status

04	01	05	00	06
TX Logical Antenna Number	connection status	TX Logical Antenna Number	connection status	TX Logical Antenna Number

00	07	00	08	01	9C E2
connection status	TX Logical Antenna Number	connection status	TX Logical Antenna Number	connection status	CRC

8.2 获取读发射功率信息(0x62)

指令描述

获取模块上电默认读发射功率，最大发射功率，最小发射功率。

指令属性

Command Code	Bootloader 指令	App Firmware 指令	Data 字段
0x62	否	是	发送指令有， 接收指令有

发送指令 Data 字段格式

获取读发射功率信息(0x62) 发送时带有 Data 字段，此时 Data 字段包含了以下的域，如表：

域	字节长度	描述
Option	1	目前的值只能设置为 0 跟 1。0 只返回上电默认读发射功率，1 返回上电默认读发射功率，最大发射功率，最小发射功率。

接收指令 Data 字段格式

获取读发射功率信息(0x62) 接收时带有 Data 字段，此时 Data 字段包含了以下的域，如表：

域	字节长度	描述

域	字节长度	描述
Option	1	同发送指令。
Read TX power	2	上电默认读发射功率。单位 dBm。此值不建议使用，要获取当前实际读发射功率值，请参考 0x61 命令。
Max TX power	0/2	当 Option=1 时存在，模块最大发射功率，单位 dBm。
Min TX power	0/2	当 Option=1 时存在，模块最小发射功率，单位 dBm。

指令实例：

发送指令：

FF	01	62	01	BE BC
Header	Data Length	Command Code	Option	CRC

接收指令：

FF	07	62	00 00	01	0C E4
Header	Data Length	Command Code	Status Code	Option	Read TX power
0C E4	00 00	06 EF			
Max TX power	Min TX power	CRC			

8.2 获取当前标签协议(0x63)

指令描述

获取操作的标签协议。目前所有读写器只支持 GEN2（18000-6C）协议。

指令属性

Command Code	Bootloader 指令	App Firmware 指令	Data 字段

Command Code	Bootloader 指令	App Firmware 指令	Data 字段
0x63	否	是	发送指令无， 接收指令有

接收指令 Data 字段格式

获取当前协议(0x63) 接收指令时带有 Data 字段，此时 Data 字段包含了以下的域，如表：

域	字节长度	描述
Current Protocol	2	目前所有读写器只支持 GEN2（18000-6C）协议，此字段现在始终为 0x0005。

8.2 获取跳频设置(0x65)

指令描述

该命令用于获取跳频表和跳频时间的信息。该命令有两种格式。

指令属性

Command Code	Bootloader 指令	App Firmware 指令	Data 字段
0x65	否	是	发送获取跳频指令时无， 发送获取跳频时间或驻留时间指令时有，接收指令时有

发送指令 Data 字段格式

0x65 指令发送获取跳频时间或天线驻留时间时带有 Data 字段，此时 Data 字段包含了以下的域：

域	字节长度	描述
Option	1	目前只有 0x02 有效，0x01 无实际意义

接收指令 Data 字段格式

0x65 指令获取跳频表时 接收指令时带有 Data 字段，此时 Data 字段包含了以下的域：

域	字节长度	描述
frequencies	4*M	M 个频率，每个频率长度为 4 个字节。

0x65 指令获取跳频时间或天线驻留时间时 接收指令时带有 Data 字段，此时 Data 字段包含了以下的域：

域	字节长度	描述
Option	1	同发指令的 Option
Hop time	4	Option=0x01 时为跳频时间，单位毫秒。目前该值无意义。 Option=0x02 时为天线驻留时间，天线驻留时间限制了每个天线口工作的最长时间，在该最长时间达到后或者是没到达前没有盘点到新标签了就跳转到下一个天线

指令实例：

获取跳频表

发送指令：

FF	00	65	1D 6A
Header	Data Length	Command Code	CRC

接收指令：

FF	0C	65	00 00	00 0D F9 26	00 0D C8 52	00 0E 24 1E	2C B5
Header	Data Length	Command Code	Status Code	915250kHz	903250kHz	926750kHz	CRC

8.4 获取 GPI(0x66)

指令描述

此命令获取读写器所有 GPI 引脚状态。

指令属性

Command Code	Bootloader 指令	App Firmware 指令	Data 字段
0x66	否	是	发送指令无， 接收指令有

接收指令 Data 字段格式

获取 GPI(0x66) 接收指令时带有 Data 字段，此时 Data 字段包含了以下的域，如表：

域	字节长度	描述
Status of Gpi pins	N	读写器所有的 gpi 引脚的状态，按数字顺序排列。每一个 gpi 引脚占一个字节。该系列模块输入 GPIO 口总共 2 个。

指令实例：

发送指令：

FF	00	66	1D 69
Header	Data Length	Command Code	CRC

接收指令：假设输入 GPIO #1 为 0，GPIO # 2 为 1

FF	02	66	00 00	00	01	CA B2

Header	Data Length	Command Code	Status Code	Input #1	Input #2	CRC

8.5 获取当前工作区域(0x67)

指令描述

获取当前工作区域

指令属性

Command Code	Bootloader 指令	App Firmware 指令	Data 字段
0x67	否	是	发送指令无， 接收指令有

接收指令 Data 字段格式

获取当前工作区域(0x67) 接收指令时带有 Data 字段，此时 Data 字段包含了以下的域：

域	字节长度	描述
Region Code	1	请参阅附录 3 工作区域以及区域频率表

指令实例：

接收指令：

FF	01	67	00 00	01	B4 80
Header	Data Length	Command Code	Status Code	Region Code	CRC

8.6 获取读写器配置(0x6A)

指令描述

该命令用于获取读写器配置。

指令属性

Command Code	Bootloader 指令	App Firmware 指令	Data 字段
0x6A	否	是	发送指令有， 接收指令有

发送指令 Data 字段格式

获取读写器配置(0x6A)发送指令时带有 Data 字段，此时 Data 字段包含了以下的域，如表：

域	字节长度	描述
Option	1	必须是 0x01
Key	1	配置项，详细说明请参见键值描述表

接收指令 Data 字段格式

获取读写器配置(0x6A)接收指令时带有 Data 字段，此时 Data 字段包含了以下的域，如表：

域	字节长度	描述
Option	1	必须是 0x01
Key	1	配置项，详细说明请参见键值描述表

域	字节长度	描述
Value	1	配置项的值，详细说明请参阅键值描述表

指令实例：

获取使用天线端口作为标记缓冲区条目唯一标识符的配置项

接收指令：

FF	03	6A	00 00	01	00	01	3E 45
Header	Data Length	Command Code	Status Code	Option	Key	Value	CRC

8.6 获取标签协议配置(0x6B)

指令描述

该命令用于获取特定标签协议的配置参数。

指令属性

Command Code	Bootloader 指令	App Firmware 指令	Data 字段
0x6B	否	是	发送指令有， 接收指令有

发送指令 Data 字段格式

获取标签协议配置(0x6B)发送指令时带有 Data 字段，此时 Data 字段包含了以下的域:

域	字节长度	描述
Protocol Value	1	必须是 0x05，现在所有读写器都只支持 Gen2 协议。
Parameter	1	协议参数，详细说明请参见协议参数选项表。

接收指令 Data 字段格式

获取标签协议配置(0x6B)接收指令时带有 Data 字段，此时 Data 字段包含了以下的域：

域	字节长度	描述
Protocol Value	1	必须是 0x05，现在所有读写器都只支持 Gen2 协议。
Parameter	1	协议参数，详细说明请参见协议参数选项表。
Option	1	参数的一个选项，对于某些参数，没有这个字段。详细说明请参阅协议参数选项表。
Value	1	带有 Option 参数的值，对于某些参数，没有这个字段。详细说明请参阅协议参数选项表。

指令实例：

例子 1

获取 Session 配置

发送指令：

FF	02	6B	05	00	3A 6F
Header	Data Length	Command Code	Protocol Value	Parameter	CRC

接收指令：

FF	03	6B	00 00	05	00	00	08 74
Header	Data Length	Command Code	Status Code	Protocol Value	Parameter	Value	CRC

例子 2

获取 Target 配置

发送指令：

FF	02	6B	05	01	3A 6E
Header	Data Length	Command Code	Protocol Value	Parameter	CRC

接收指令：

FF	04	6B	00 00	05	01	01	00	2C 68
Header	Data Length	Command Code	Status Code	Protocol Value	Parameter	Option	Value	CRC

8.7 获取可用标签协议(0x70)

指令描述

该命令用于获取支持的标签协议。目前只有 GEN2，18000-6C 协议。

指令属性

Command Code	Bootloader 指令	App Firmware 指令	Data 字段
0x70	否	是	发送指令无， 接收指令有

接收指令 Data 字段格式

0x70 指令接收时带有 Data 字段，此时 Data 字段包含了以下的域，如表：

域	字节长度	描述
Protocol Value	2	此字段现在始终为 0x0005。

8.8 获取可用的工作频率区域(0x71)

指令描述

该命令用于获取支持的工作频率区域。中国国内版本模块目前可用的有北美频段、中国频段、CE_LOW、全频段；而国外版本的只能使用对应国家的频段。

指令属性

Command Code	Bootloader 指令	App Firmware 指令	Data 字段
0x71	否	是	发送指令无， 接收指令有

接收指令 Data 字段格式

(0x71)指令接收指令时带有 Data 字段，此时 Data 字段包含了以下的域，如表：

域	字节长度	描述
Regions	1*N	N 个可用的区域代码

指令实例：

发送指令：

FF	00	71	1D 7E
Header	Data Length	Command Code	CRC

接收指令：

FF	04	71	00 00	01	06	08	FF	DB 40
Header	Data Length	Command Code	Status Code	NA	CN	European		CRC

8.9 获取模块温度(0x72)

指令描述

目前读写器支持的最高工作温度约为 90°C，当温度超过此值时，读写器将报告错误。

指令属性

Command Code	Bootloader 指令	App Firmware 指令	Data 字段
0x72	否	是	发送指令无， 接收指令有

接收指令 Data 字段格式

获取模块温度(0x72)接收指令时带有 Data 字段，此时 Data 字段包含了以下的域，如表：

域	字节长度	描述
Temperature	1	温度值，1 字节，有符号数。

注意事项：

●SIMX600 系列模块没有温度检测功能；如 SIM7600，SIM5600 等

指令实例：

发送指令：

FF	00	72	1D 7D
Header	Data Length	Command Code	CRC

接收指令：获取温度为 39℃

FF	01	72	00 00	27	48 20
Header	Data Length	Command Code	Status Code	Temperature	CRC

9 永久保存配置指令

与普通设置指令不同，用这类修改上电默认值配置指令能够做到永久保存功能。永久保存配置指令遵从扩展指令通信协议格式。

指令码固定为 0xAA。扩展指令的子指令称为 SubCommand Code，固定 2 个字节。

SubCommand Code 对应的数据域为 Subcommand Data 域，以下简称 SubData 域。

获取与配置模块永久保存参数命令 SubCommand Code 为 AA40。

指令属性

SubCommand Code	Bootloader 指令	App Firmware 指令	Subcommand Data
0xAA40	否	是	发送指令有，接收指令有

发送指令 SubData 域格式

0xAA40 发送指令时带有 SubData 域，此时 SubData 域包含了以下的域，如表：

域	字节长度	描述
KEY	1	表示是要获取或配置哪些参数
GETORSET	1	0 表示获取功能，1 表示设置功能
KEYDATA	N	参数内容，由 KEY 决定 KEYDATA 长度和组成

9.1 上电时默认采用工作天线和功率配置

9.1.1 获取上电时默认采用工作天线和功率配置

发送指令 SubData 域格式

域	字节长度	描述
KEY	1	0x91
GETORSET	1	0

域	字节长度	描述
KEYDATA	0	无此域

接收指令 SubData 域格式

域	字节长度	描述
KEY	1	0x91
GETORSET	1	0
KEYDATA	1/(4+7*N)	若返回 1 字节 0x5A 表示未配置过工作天线与功率，采用默认。若返回 4+7*N(N 为模块天线口数量)，4 字节的 Antusenum，bit0 表示天线 1，bit1 表示天线 2....bit31 表示天线 32。天线对应的位若置 1 表示使能该天线，置 0 表示未使能该天线。7 字节的天线信息，包括 1 字节 antlogicid，1 表示天线 1，8 表示天线 8；2 字节读功率，单位 0.01dBm；2 字节写功率，单位 0.01dBm；2 字节 settingtime 目前无效。将返回 N 组天线信息。注意：读功率，写功率和 settingtime 若为 FFFF，则表示该逻辑天线未配置过功率。

9.1.2 设置上电时默认采用工作天线和功率配置

发送指令 SubData 域格式

域	字节长度	描述
KEY	1	0x91

域	字节长度	描述
GETORSET	1	0x01
KEYDATA	1/N	当恢复出厂默认值时，KEYDATA=0x5A 当设置指定值时，KEYDATA 为 0x91 指令帧除帧头（0xFF）以及 CRC 字段之外的部分。即 KEYDATA 包括 Data Length 字段 Command Code 字段以及 Data 字段，Data 字段格式参考 0x91 命令发送指令 Data 格式（注意，只支持 Option=2 或者 Option=4 时的格式）

接收指令 SubData 域格式

域	字节长度	描述
KEY	1	0x91
GETORSET	1	0x01
KEYDATA	0	无此域

指令实例：

配置功率天线 1，2，3，4 功率各 3300

发送指令：

FF	2F	AA	4D 6F 64 75 6C 65 74 65 63 68	AA 40	91	01
Header	Data Length	Command Code	Subcommand Marker (Moduletech)	Subcommand Code	KEY	GETORSET

1D 91 04 01 0C E4 0C E4 00 00 02 0C E4 0C E4 00 00 03 0C E4 0C E4 00 00 04 0C E4 0C E4 00 00	B8	BB	CE FB
KEYDATA	SubCRC	Terminator	CRC

接收指令：

FF	0E	AA	00 00	4D 6F 64 75 6C 65 74 65 63 68	AA 40	91	01	54 5F
Header	Data Length	Command Code	Status Code	Subcommand Marker (Moduletech)	Subcommand Code	KEY	GETORSET	CRC

9.2 上电时默认工作频率，跳频时间

9.2.1 获取上电时默认工作频率，跳频时间

发送指令 SubData 域格式

域	字节长度	描述
KEY	1	0x95
GETORSET	1	0
KEYDATA	0/1	获取工作频率,无此域;获取跳频时间时，一字节，0x01。

接收指令 SubData 域格式

域	字节长度	描述
KEY	1	0x95
GETORSET	1	0
KEYDATA	1/4*N/5	若返回 1 字节 0x5A，表示未配置过采用默认。 获取工作频率时为 N*4 字节，N 为所设置工作的频点数，每个频

域	字节长度	描述
		点 4 个字节，高字节在前，单位 kHz； 当为获取跳频时间时为 0x01+HOPTIME，HOPTIME 为 4 个字节的跳频时间，单位毫秒。

9.2.2 设置上电时默认工作频率，跳频时间

发送指令 SubData 域格式

域	字节长度	描述
KEY	1	0x95
GETORSET	1	0x01
KEYDATA	1/N	当恢复出厂默认值时，KEYDATA=0x5A 当设置指定值时，KEYDATA 为 0x95 指令帧除帧头（0xFF）以及 CRC 字段之外的部分。即 KEYDATA 包括 0x95 指令帧的 Data Length 字段，Command Code 字段以及 Data 字段，Data 字段格式参考 0x95 指令的发送指令 Data 格式（注意，当设置跳频时间时，跳频时间设置范围为 20 到 4000ms，目前该设置值无效不起实际效果）

接收指令 SubData 域格式

域	字节长度	描述
KEY	1	0x95
GETORSET	1	0x01
KEYDATA	0	无此域

注意事项：

●该命令仅中国版模块可使用

●设置读写器工作在哪个频段即只能设置对应的频段内的频点。也即是当前已设置模块工作在哪个频段，则只能设置该频段内部分频点或全部频点进行工作，跳频表在后面给出。如果使用后面介绍的 0x97 命令设置了工作频段，并且不需要指定跳频表中某些特定频点工作则不需要使用 0x95 命令再进行设置；

●采用该命令设置后当前即采用所设置的频率工作，并且以后每次重新上电后默认采用所设置的频率工作。当使用该命令的恢复到出厂默认时，如修改了默认工作频段，则当前即采用所保存的上电默认的工作频段工作，如果未配置过上电默认的工作频段，则当前按模块出厂默认上电频段工作；并且设备重新上电后将恢复出厂默认。

●必须已先设置过默认上电工作频率区域才可以使用该命令设置频点，也即是必须使用保存配置的 0x97 命令设置过默认上电工作频率区域后才可以设置。

9.3 上电时默认工作频率区域

9.3.1 获取上电时默认工作频率区域

发送指令 SubData 域格式

域	字节长度	描述
KEY	1	0x97
GETORSET	1	0
KEYDATA	0	无此域

接收指令 SubData 域格式

域	字节长度	描述
KEY	1	0x97
GETORSET	1	0
KEYDATA	1	1 字节，工作频率区域码。若返回 1 字节 0x5A，表示未配置过采用默认。

9.3.2 设置上电时默认工作频率区域

发送指令 SubData 域格式

域	字节长度	描述
KEY	1	0x97
GETORSET	1	0x01
KEYDATA	1	1 字节，工作频率区域码。当恢复出厂默认值时，KEYDATA=0x5A

接收指令 SubData 域格式

域	字节长度	描述
KEY	1	0x97
GETORSET	1	0x01
KEYDATA	0	无此域

注意事项：

●该命令仅中国版模块可使用

●中国模块出厂默认工作频段为北美，外国模块即是对应国家的频段。

●采用该命令设置后当前即采用所设置的频段工作，并且以后每次重新上电后默认采用设置的频段工作。未配置过或恢复到出厂默认则按模块原本默认的工作。

9.4 上电时默认读写器配置参数

9.4.1 获取上电时默认读写器配置参数

发送指令 SubData 域格式

域	字节长度	描述
KEY	1	0x9A
GETORSET	1	0
KEYDATA	2	一字节 OPTION，一字节 KEY，请参照模块 0x9A:设置阅读器配置命令.

接收指令 SubData 域格式

域	字节长度	描述
KEY	1	0x9A
GETORSET	1	0
KEYDATA	1/3	一字节 OPTION，一字节 KEY，一字节 VALUE ，请参考 0x9A:

域	字节长度	描述
		设置阅读器配置命令。若返回 1 字节 0x5A，表示未配置过采用默认。

9.4.2 设置上电时默认读写器配置参数

发送指令 SubData 域格式

域	字节长度	描述
KEY	1	0x9A
GETORSET	1	0x01
KEYDATA	1/3	一字节 OPTION,一字节 KEY,一字节 VALUE ，对应关系请看 0x9A:设置阅读器配置命令（OPTION 只能为 0x01）。当恢复出厂默认值时，KEYDATA=0x5A

接收指令 SubData 域格式

域	字节长度	描述
KEY	1	0x9A
GETORSET	1	0x01
KEYDATA	0	无此域

9.5 上电时默认协议配置参数

9.5.1 获取上电时默认协议配置参数

发送指令 SubData 域格式

域	字节长度	描述
KEY	1	0x9B
GETORSET	1	0
KEYDATA	2	一字节 Procotol Value+一字节 Parameter，请参照模块 0x9B:设置协议配置命令；

接收指令 SubData 域格式

域	字节长度	描述
KEY	1	0x9B
GETORSET	1	0
KEYDATA	3/4	具体看所获取的是那个参数，由 Procotol Value，Parameter，Option，Value 组成，对应关系请看模块 0x9B:设置协议配置命令。若返回 1 字节 0x5A，表示未配置过采用默认。

9.5.2 设置上电时默认协议配置参数

发送指令 SubData 域格式

域	字节长度	描述
KEY	1	0x9B

域	字节长度	描述
GETORSET	1	0x01
KEYDATA	1/3/4	3 或 4 字节，具体看所设置的是那个参数，由 Procotol Value，Parameter，Option，Value 组成，对应关系请看模块 0x9B:设置协议配置命令。当恢复出厂默认值时，KEYDATA=0x5A

接收指令 SubData 域格式

域	字节长度	描述
KEY	1	0x9B
GETORSET	1	0x01
KEYDATA	0	无此域

9.6 上电时默认是否上电运行至 APP

9.6.1 获取上电时默认是否上电运行至 APP

发送指令 SubData 域格式

域	字节长度	描述
KEY	1	0x04
GETORSET	1	0
KEYDATA	0	无此域

接收指令 SubData 域格式

域	字节长度	描述
KEY	1	0x04
GETORSET	1	0
KEYDATA	4	为 0xA5A55A5A 时表示模块配置为上电即自动跳转到 APP 应用层，其他值表示未配置为上电即自动跳转到 APP 应用层.

9.6.2 设置上电时默认是否上电运行至 APP

发送指令 SubData 域格式

域	字节长度	描述
KEY	1	0x04
GETORSET	1	0x01
KEYDATA	4	为 0xA5A55A5A 时表示设置一上电即运行至 APP，其他值表示不执行一上电即运行至 APP.

接收指令 SubData 域格式

域	字节长度	描述
KEY	1	0x04
GETORSET	1	0x01
KEYDATA	0	无此域

注意事项：

●该功能为可以让模块上电即运行到 APP 应用层，不用等待接收到执行到应用层命令 0x04 命令后才跳转去 。

●模块出厂默认为上电不自动运行到 APP 应用层。

指令实例：

发送指令：

FF	14	AA	4D 6F 64 75 6C 65 74 65 63 68	AA 40	04	01	A5 A5 5A 5A	ED	BB	12 39
Header	Data Length	Command Code	Subcommand Marker (Moduletech)	Subcommand Code	KEY	GETORSET	KEYDATA	Sub CRC	Terminator	CRC

接收指令：

FF	0E	AA	00 00	4D 6F 64 75 6C 65 74 65 63 68	AA 40	04	01	C1 5F
Header	Data Length	Command Code	Status Code	Subcommand Marker (Moduletech)	Subcommand Code	KEY	GETORSET	CRC

9.7 上电时默认波特率

9.7.1 获取上电时默认波特率

发送指令 SubData 域格式

域	字节长度	描述
KEY	1	0x06
GETORSET	1	0
KEYDATA	0	无此域

接收指令 SubData 域格式

域	字节长度	描述
KEY	1	0x06
GETORSET	1	0
KEYDATA	4	模块上电默认波特率值；值为 9600、19200、38400、57600、115200、230400、460800、921600 中的一个；

指令实例：获取当前波特率

发送指令：

FF	10	AA	4D 6F 64 75 6C 65 74 65 63 68	AA 40	06	00	F0	BB	A0 51
Header	Data Length	Command Code	Subcommand Marker (Moduletech)	Subcommand Code	KEY	GETORSET	Sub CRC	Terminator	CRC

接收指令：

FF	12	AA	00 00	4D 6F 64 75 6C 65 74 65 63 68	AA 40	06	00	00 0E 10 00	9C 5F
Header	Data Length	Command Code	Status Code	Subcommand Marker (Moduletech)	Subcommand Code	KEY	GETORSET	KEY DATA	CRC

9.7.2 设置上电时默认波特率

发送指令 SubData 域格式

域	字节长度	描述
KEY	1	0x06
GETORSET	1	0x01

域	字节长度	描述
KEYDATA	4	模块上电默认波特率值；值为 9600、19200、38400、57600、115200、230400、460800、921600 中的一个；

接收指令 SubData 域格式

域	字节长度	描述
KEY	1	0x06
GETORSET	1	0x01
KEYDATA	0	无此域

指令实例：

发送指令：

FF	14	AA	4D 6F 64 75 6C 65 74 65 63 68	AA 40	06	01	00 0E 10 00	0F	BB	79 9F
Header	Data Length	Command Code	Subcommand Marker (Moduletech)	Subcommand Code	KEY	GETORSET	KEYDATA	Sub CRC	Termin ator	CRC

接收指令：

FF	0E	AA	00 00	4D 6F 64 75 6C 65 74 65 63 68	AA 40	06	01	C3 5F
Header	Data Length	Command Code	Status Code	Subcommand Marker (Moduletech)	Subcommand Code	KEY	GETORSET	CRC

注意事项：

●模块上电时会根据模块先前所配置保存的波特率值来初始化串口通信波特率。

●模块出厂默认为 115200 波特率。

●使用该命令设置后收到模块正确应答后模块当前即采用所设置的波特率工作，并且以后每

次重新上电后也将采用所设置的波特率进行初始化串口。

9.7 恢复默认出厂配置

采用该命令复位模块保存配置参数到默认出厂配置后，当前即采用出厂默认的配置工作，并且清除掉先前所配置保存过的参数，并且以后每次上电将按照模块出厂默认工作，直到重新对模块进行配置。

发送指令 SubData 域格式

域	字节长度	描述
KEY	1	0xAA
GETORSET	1	0x01
KEYDATA	0	无此域

接收指令 SubData 域格式

域	字节长度	描述
KEY	1	0xAA
GETORSET	1	0x01
KEYDATA	0	无此域

指令实例：

发送指令：

FF	10	AA	4D 6F 64 75 6C 65 74 65 63 68	AA 40	AA	01	95	BB	8D 63

Header	Data Length	Command Code	Subcommand Marker (Moduletech)	Subcommand Code	KEY	GETORSET	SubCRC	Terminator	CRC

接收指令：

FF	0E	AA	00 00	4D 6F 64 75 6C 65 74 65 63 68	AA 40	AA	01	6F 5F
Header	Data Length	Command Code	Status Code	Subcommand Marker (Moduletech)	Subcommand Code	KEY	GETORSET	CRC

9.8 准备升级更新固件指令

该命令为准备升级指令，因可能设置了上电自动执行 0x04 指令则模块就直接运行到 APP 功能，所以每次升级前上位机需要先发送该指令，发送完该指令后只要收到模块的回复，不管是收到操作成功还是操作失败的回复，只要收到模块的正确回复，则可以继续升级模块。

发送指令 SubData 域格式

域	字节长度	描述
KEY	1	0xAB
GETORSET	1	0x01
KEYDATA	0	无此域

接收指令 SubData 域格式

域	字节长度	描述
KEY	1	0xAB
GETORSET	1	0x01

域	字节长度	描述
KEYDATA	0	无此域

指令实例：

发送指令：

FF	10	AA	4D 6F 64 75 6C 65 74 65 63 68	AA 40	AB	01	96	BB	BD 52
Header	Data Length	Command Code	Subcommand Marker (Moduletech)	Subcommand Code	KEY	GETORSET	SubCRC	Terminator	CRC

接收指令：

FF	0E	AA	00 00	4D 6F 64 75 6C 65 74 65 63 68	AA 40	AB	01	6E 5F
Header	Data Length	Command Code	Status Code	Subcommand Marker (Moduletech)	Subcommand Code	KEY	GETORSET	CRC

10 其它指令

10.1 回波检测指令(0xAA4A)

指令描述

回波检查指令用于检测天线回波值，回波值越小反应的是天线匹配越好，通常应该小于 7.

否则可能天线不匹配或者天线接触不良或者天线损坏，未接天线都有可能。

回波检测指令遵从扩展指令通信协议格式。

指令码固定为 0xAA。扩展指令的子指令称为 SubCommand Code，固定 2 个字节。

SubCommand Code 对应的数据域为 Subcommand Data 域，以下简称 SubData 域。

回波检测命令 SubCommand Code 为 AA4A。

指令属性

SubCommand Code	Bootloader 指令	App Firmware 指令	Subcommand Data
0xAA4A	否	是	发送指令有，接收指令有

发送指令 SubData 域格式

0xAA4A 发送指令时带有 SubData 域，此时 SubData 域包含了以下的域，如表：

域	字节长度	描述
data	5+3*N	第一字节:指定检测功率值的高字节； 第二字节:指定检测功率值的低字节，单位 0.01dBm（目前功率值不起实际作用设置为 0x07D0 即可）； 第三字节:指定逻辑天线号 第四字节:指定频段；中国模块可指定中国，FCC，CE_LOW，全频段四个频段；国外的只能指定对应的国家的频段； 第五字节:指定测试的频点数 N，该值不能超过指定频段包含的最大频点数，只有中国模块可指定指定频段内的个别频点进行检测，

域	字节长度	描述
		国外的该值必须为 0；N=0 时表示测试整个频段，data 的长度为 5 个字节；N>0 时表示测试的频点数量为 N 值，data 的长度为 5+3*N，每个频点用 3 个字节表示，高字节在前。设置了那个频段就只能设置对应的该频段内的频点；

接收指令 SubData 域格式

0xAA4A 接收指令时带有 SubData 域，此时 SubData 域包含了以下的域，如表：

域	字节长度	描述
data	5+4*M/5+4*N	第一字节:指定检测功率值的高字节； 第二字节:指定检测功率值的低字节，单位 0.01dBm（目前功率值不起实际作用设置为 0x07D0 即可）； 第三字节:指定逻辑天线号 第四字节:指定频段；中国模块可指定中国，FCC，CE_LOW，全频段四个频段；国外的只能指定对应的国家的频段； 第五字节:指定测试的频点数 N，该值不能超过指定频段包含的最大频点数，只有中国模块可指定指定频段内的个别频点进行检测，国外的该值必须为 0；N=0 时表示测试整个频段，data 的长度为 5+4*M 个字节，M 为该频段内的频点总数；N>0 时表示测试的频点数量为 N 值，data 的长度为 5+4*N;每个频点的测试结果由 4 个字节组成，高 3 个字节为频点，最低字节为 return loss 回波损耗值，该值为发射功率值-反射功率值的结果，单位为 0.1db.

注意事项：

●该命令如果是 FCC 标准则检测一次要 25 秒左右，类似 FCC 标准的国家都需要比较长时间，建议发送该命令后等待回复的超时时间设定为 30 秒。

指令实例： 天线 1 功率 3000，检测北美所有频点驻波值。

发送指令：

FF	13	AA	4D 6F 64 75 6C 65 74 65 63 68	AA 4A	0B B8 01 01 00
Header	Data Length	Command Code	Subcommand Marker (Moduletech)	Subcommand Code	data

B9	BB	BD 67
SubCRC	Terminator	CRC

解析：data=0B B8 | 01 | 01 | 00 ： 功率 3000 | 逻辑天线 1 | 频段北美 | 所有频点

接收指令：

FF	D9	AA	00 00	4D 6F 64 75 6C 65 74 65 63 68	AA 4A
Header	Data Length	Command Code	Status Code	Subcommand Marker (Moduletech)	Subcommand Code
0B B8 01 01 00 0D F7 32 78 0D C6 5E 82 0E 26 12 6E 0D F9 26 78 0D C8 52 82 0E 24 1E 6E 0D DB DA 78 0E 02 EA 6E 0E 16 72 6E 0D D0 22 82 0D FB 1A 6E 0D E7 92 78 0E 0E A2 6E 0D EF 62 78 0D D4 0A 82 0D F3 4A 78 0D DF C2 78 0E 06 D2 6E 0E 1A 5A 6E 0D CC 3A 82 0D FF 02 6E 0D EB 7A 78 0E 12 8A 6E 0E 0A BA 6E 0D D7 F2 82 0D F5 3E 78 0D E1 B6 78 0E 08 C6 6E 0E 1C 4E 6E 0D CE 2E 82 0D ED 6E 78 0D D9 E6 82 0E 00 F6 6E 0E 14 7E 6E 0D E3 AA 78 0E 1E 42 6E 0D E5 9E 78 0E 0C AE 6E 0E 20 36 6E 0D D2 16 82 0D F1 56 78 0D DD CE 78 0E 04 DE 6E 0E 18 66 6E 0D CA 46 82 0D FD 0E 78 0D E9 86 78 0E 10 96 6E 0E 22 2A 6E 0D D5 FE 82					BD 67
data					CRC

解析：data=0D F7 32 78 | 0D C6 5E 82 ... 每 4 个字节一组，前 3 字节表示频点值，后面为驻波值 VL,例如：VL =0x78=120。RL=10 的(VL/10/20)次方. 驻波比 VSWR 计算公式为:VSWR=(1 + RL) / (RL - 1); 计算得 VSWR=1.67. 故第一个频点及驻波比为：915250：1.67。

10.2 多标签匹配过滤数据设置指令(0xAA4C)

指令描述

匹配过滤最多支持 16 张标签，每张标签的匹配过滤长度最长为 255 位.该指令遵从扩展指

令通信协议格式。

指令码固定为 0xAA。扩展指令的子指令称为 SubCommand Code，固定 2 个字节。

SubCommand Code 对应的数据域为 Subcommand Data 域，以下简称 SubData 域。

多标签匹配过滤设置命令 SubCommand Code 为 AA4C。

指令属性

SubCommand Code	Bootloader 指令	App Firmware 指令	Subcommand Data
0xAA4C	否	是	发送指令有，接收指令无

发送指令 SubData 域格式

0xAA4C 发送指令时带有 SubData 域，此时 SubData 域包含了以下的域，如表：

域	字节长度	描述
SELFLAG	2	当匹配过滤标签数据一条指令能发送完时，SELFLAG=0xFFFF； 当匹配过滤标签数据二条指令才能发送完毕时，第一条的 SELFLAG=0x0000,第二条的 SELFLAG=0x00FF; 当匹配过滤标签数据三条指令及以上才能发送完毕时，第一条的 SELFLAG=0x0000,中间的 SELFLAG=0xFF00; 最后一条的 SELFLAG=0x00FF;
SELTAGCNT	1	每条指令中匹配过滤的标签数
SELTAGDATAN	N*SELTAGCNT	SELTAGDATAN 为每条过滤标签的数据。

SELTAGDATAN 域包含以下的域，如表：

域	字节长度	描述
selLEN	1	整个 SELTAGDATAN 域的字节长度
selBANK	1	过滤标签 BANK，取值 1-3，1=EPC，2=TID，3=USER；
selADDR	4	过滤位地址；
selbitsLEN	1	过滤位长度；
selDATA	N	过滤数据，若 selbitsLEN 能整除 8，则 N 为 selbitsLEN/8,否则 N 为 selbitsLEN/8+1；

注意事项：

●当使用 0x22 指令跟 0xAA48 异步盘存指令进行标签盘存时，如果 OPTION 的低 3 位都为 1，表示启用多标签匹配过滤功能，此时只有 OPTION 低 4 位有效；当使用多标签匹配过滤功能时，先前必须成功进行过匹配过滤数据的设置，否则将返回执行失败；只要进行过设置，匹配过滤数据将保存着，后期如果没再发新的设置命令下来，启动多标签匹配过滤功能就按照 先前设置的匹配过滤。

指令实例：

过滤标签 1：epcid E2008181811602531040AF36
过滤标签 2：epcid 4298
过滤标签 3：epcid 11221000000000002001000

发送指令：

FF	40	AA	4D 6F 64 75 6C 65 74 65 63 68	AA 4C	FF FF	03
Header	Data Length	Command Code	Subcommand Marker (Moduletech)	Subcommand Code	SELFLAG	SELTAG CNT
13	01	00 00 00 20	60	E2 00 81 81 81 16 02 53 10 40 AF 36		
selLEN	selBANK	selADDR	selbitsLEN	selDATA		
09	01	00 00 00 20	10	42 98		
selLEN	selBANK	selADDR	selbitsLEN	selDATA		
13	01	00 00 00 20	60	11 22 10 00 00 00 00 00 02 00 10 00		
selLEN	selBANK	selADDR	selbitsLEN	selDATA		

8D	BB	4E 77
SubCRC	Terminator	CRC

接收指令：

FF	0C	AA	00 00	4D 6F 64 75 6C 65 74 65 63 68	AA 4C	0F 27
Header	Data Length	Command Code	Status Code	Subcommand Marker (Moduletech)	Subcommand Code	CRC

10.3 私有宜链温度标签指令(0xAA50)

指令描述

特殊的读标签存储区命令如图 7，获取标签温度指令.该指令遵从扩展指令通信协议格式。

指令码固定为 0xAA。扩展指令的子指令称为 SubCommand Code，固定 2 个字节。

SubCommand Code 对应的数据域为 Subcommand Data 域，以下简称 SubData 域。

私有温度标签命令 SubCommand Code 为 AA50。

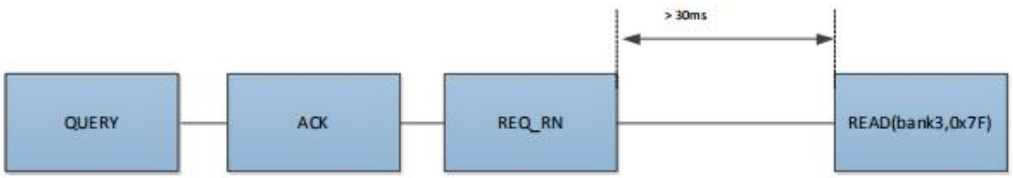


图 7

指令属性

SubCommand Code	Bootloader 指令	App Firmware 指令	Subcommand Data
0xAA50	否	是	发送指令有，接收指令有

发送指令 SubData 域格式

0xAA50 指令发送时带有 SubData 域，此时 SubData 域包含了以下的域，如表：

域	字节长度	描述
TIMEALL	2	指令执行总时间（TIMESELWAIT+TIMEREADWAIT+读标签时间），单位毫秒。读标签时间为 Timeout 域定义的值
TIMESELWAIT	2	为使用匹配过滤时设定发送完匹配过滤数据后等待的时间，单位毫秒，最大值为 300，不使用时为 0 即可
TIMEREADWAIT	2	指定在进行读内存内容前要等待的时间，单位毫秒，最大值 300，不使用时为 0 即可
Option	1	参考 0x28 指令发送时 Data 字段格式
Metadata Flags	0/2	参考 0x28 指令发送时 Data 字段格式
Read MemBank	1	参考 0x28 指令发送时 Data 字段格式

域	字节长度	描述
Read Address	4	参考 0x28 指令发送时 Data 字段格式
Word Count	1	参考 0x28 指令发送时 Data 字段格式
Access Password	0/4	参考 0x28 指令发送时 Data 字段格式
Tag Singulation	N	参考 0x28 指令发送时 Data 字段格式

0xAA50 指令 接收时带有 Data 字段

有两种不同的数据字段格式，具体取决于发送指令 Option 域 BIT4 是否为 1，为 1 包含 Metadata Flags 域。第一种是只获取存储区数据，发送指令中没有 Metadata Flags 域。另一种是存储区数据和元数据，在发送指令中必须有 Metadata Flags 域。

发送指令中中 Option 的 BIT4 为 0，没有 Metadata Flags 域时，接收指令时带有 Data 字段，此时 Data 字段包含了以下的域，如表：

域	字节长度	描述
Option	1	与发送指令的 Option 域相同。
Data Read	N	读到的标签存储区数据。
TagLenth	1	为 PC Word+EPC ID+TagCRC 总字节长度
PC Word	2	EPC bank 中的 PC 字段。PC 的高 5 位代表 EPC 的块长度。（1 块=2 bytes）。例如 0x0800 代表 EPCID 长度为 1 块，2 字节 1 块 16bit，又例如 0xF800 意味着 EPCID 62 字节 31 块 496bit。

域	字节长度	描述
EPC ID	N	Tag EPC
TagCRC	2	Tag CRC

发送指令中 Option 的 BIT4 为 1，有 Metadata Flags 域时，接收指令时带有 Data 字段，此时 Data 字段包含了以下的域，如表：

字段	字节长度	描述
Option	1	与发送指令的 Option 字段相同。
Metadata Flags	2	与发送指令中的 Metadata Flags 字段相同。
Metadata	N	Metadata 域长度由 Metadata Flags 决定
TagLenth	1	为 PC Word+EPC ID+TagCRC 总字节长度
PC Word	2	EPC bank 中的 PC 字段。PC 的高 5 位代表 EPC 的块长度。
EPC ID	N	Tag EPC
TagCRC	2	Tag CRC

注意事项：

●温度标签测温范围判断方法（PC）

目前使用的测温范围有-30~97 度, 0~120 度和-40~120 度等，计算温度前可以通过读取标签 EPC 区 PC 值判断芯片测温范围，不同测温范围使用相对应的温度计算方法，PC 值

为 EPC 区第二个字。

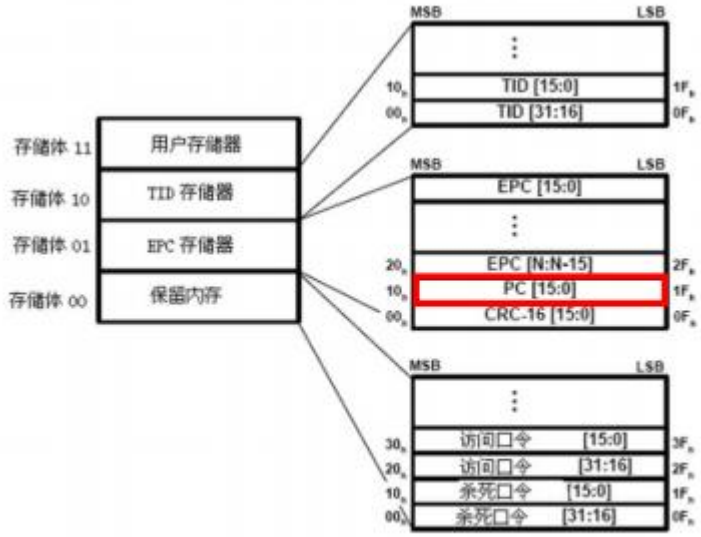


图 6.17 逻辑内存映象

如果 PC 值以十六进制 ‘48’ 结尾（即 0xXX48），就认为是 0~120 度测温范围标签，若 PC

值以十六进制’ 78’ 结尾即(0xXX78),就认为是-40~120 度标签, PC 值以十六进制’ 00’ 结尾

(0xXX00)就是-30~90 度测温范围。

几种测温范围读取的温度数据均为两个字节[byte1,byte2],第一个字节 byte1 为温度数据整数部分,第二个字节 byte2 为温度数据小数部分。

1. 对于测温范围-30~97 度标签,读到温度数据后计算方法为:

整数部分最高位为符号位，正数直接减 30，小数部分*100/256。负数整数部分取反减 30，小数部份取反加 1 后*100/256

2. 对于测温范围 0~120 度标签,读到温度数据后计算方法:

整数部分不变,小数部分*100/256

3. 对于测温范围-40~120 度标签,读到温度数据后计算方法:

整数部分减 45,小数部分*100/256

指令实例： 过滤 tid，从地址 0 开始 过滤数据 E2008；读宜链温度标签。

发送指令：

FF	29	AA	4D 6F 64 75 6C 65 74 65 63 68	AA 50	04 4C	00 00
Header	Data Length	Command Code	Subcommand Marker (Moduletech)	Subcommand Code	TIME ALL	TIMESE LWAIT

00 64	12	00 0F	03	00 00 00 7F	01
TIMEREADWAIT	Option	Metadata Flags	Read MemBank	Read Address	Word Count

00 00 00 00	00 00 00 00	14	E2 00 80	C8	BB	6C B6
Access Password	Select Address	Select Data Length	Select Data	SubCRC	Terminator	CRC

10.4 宜链标签亮灯指令(0xAA51)

指令描述

点亮宜链标签上的 led 灯。该指令遵从扩展指令通信协议格式。

指令码固定为 0xAA。扩展指令的子指令称为 SubCommand Code，固定 2 个字节。

SubCommand Code 对应的数据域为 Subcommand Data 域，以下简称 SubData 域。

宜链标签亮灯命令 SubCommand Code 为 AA51。

指令属性

SubCommand Code	Bootloader 指令	App Firmware 指令	Subcommand Data
0xAA51	否	是	发送指令有，接收指令单标签点亮时有，多标签同时点亮时无

发送指令 SubData 域格式

0xAA51 指令发送时带有 SubData 域 ，此时 SubData 域包含了以下的域，如表：

域	字节长度	描述
Timeout	2	请参考 Timeout 域描述。若 Option 最高位(BIT7)为 1 时，timeout 的最高字节为点亮灯的持续时间，timeout 的低字节为去盘点标签的时间，单位 100 毫秒*。若 Option 的若 Select-Option Bits=0x07 时，timeout 的低字节须为 0xFF *。
Option	1	Option 域包含 Select-Option Bits 控制位。Option 最高位置 1 时，将会改变 Timeout 域的定义。 若 Select-Option

域	字节长度	描述
		Bits=0x07 时，实现多标签同时点亮功能，注意 Timeout 域低字节必须为 0xFF *。
Metadata Flags	0/2	同 0x21 指令
Tag Singulation	N	同 0x21 指令

接收指令 SubData 域格式

0xAA51 指令单标签点亮接收时带有 SubData 域

有两种不同的数据域格式，具体取决于发送指令 Option 的 BIT4 是否为 1，为 1 包含 Metadata Flags 域。第一种是只获取 EPC，发送指令中没有 Metadata Flags 域。 另一种是获取 EPC 和元数据，在发送指令中必须有 Metadata Flags 域。

获取 EPC

发送指令中 Option 的 BIT4 为 0 没有 Metadata Flags 域时，接收指令时带有 SubData 域，此时 SubData 域包含了以下的域，如表：

域	字节长度	描述
Option	1	与发送指令的 Option 字段相同。
PC Word	2	EPC bank 中的 PC 字段。PC 的高 5 位代表 EPC 的块长度。
EPC	M	标签的 EPC
TagCRC	2	EPC bank 中 TagCRC

获取 EPC 和元数据

发送指令中 Option 的 BIT4 为 1 有 Metadata Flags 域时，接收指令时带有 SubData 域，此时 SubData 域包含了以下的域，如表：

字段	字节长度	描述
Option	1	与发送指令的 Option 字段相同。
Metadata Flags	2	与发送指令中的 Metadata Flags 字段相同。
Metadata	N	Metadata 域长度由 Metadata Flags 决定
PC Word	2	EPC bank 中的 PC 字段。PC 的高 5 位代表 EPC 的块长度。
EPC ID	N	标签 EPC
Tag CRC	2	标签 CRC

注意事项：

●国外版本模块该指令不可用

●Option 域 最高位置 1 时，timeout 的最高字节为点亮灯的持续时间，timeout 的低字节为去盘点标签的时间，单位 100 毫秒，例如

FF 11 AA 4D 6F 64 75 6C 65 74 65 63 68 AA 51 40 05 80 C0 BB CC CF

就是盘点时间 0x05=500 毫秒，当盘点到 LED 标签后点亮时间为 0x40=6400 毫秒。使用

该点亮 LED 灯的功能，上位机发送命令后模块执行成功的返回时间是盘点时间加上持续点亮 LED 灯的时间，所以像上例，模块执行成功后的返回时间最长会是 500 毫秒+6400 毫秒左右，所以上位机等待模块回复的时间应该是这个时间再加上几秒的时间（跟其他命令一样异常处理需要更多时间），然后在这个时间后没收到模块返回才认定为命令丢失。

●Option 域为 0x07 时，实现一种多标签同时点亮功能。TIMEOUT 的低字节原先为盘点标签的时间，这里固定为 0xFF 即可，不可为 0。多标签点亮命令不用去盘点标签，所以这个时间值实际是无效的。命令执行后，只会返回操作失败或成功，因实际只是发送了匹配过滤数据而已，没有去盘点标签，所以不会有标签数据返回。

指令实例：点亮灯的持续 3200 毫秒，盘点 3200 毫秒，实现多标签同时点亮（注意：先设置多标签过滤，参考多标签匹配过滤设置指令。

发送指令：

FF	11	AA	4D 6F 64 75 6C 65 74 65 63 68	AA 51	2020	87
Header	Data Length	Command Code	Subcommand Marker (Moduletech)	Subcommand Code	Timeout	option

C2	BB	DC 50
SubCRC	Terminator	CRC

接收指令：

FF	0C	AA	00 00	4D 6F 64 75 6C 65 74 65 63 68	AA 51	0F 3A
Header	Data Length	Command Code	Status Code	Subcommand Marker (Moduletech)	Subcommand Code	CRC

状态码

下表描述了每个状态代码的详细含义。

状态码描述表

Status Code	描述
0x0000	成功
0x0100	Data 的实际长度与 Data Length 字段的值不同。
0x0101	命令不可用，常见于模块供电不稳定导致模块软复位
0x0105	参数值不可用
0x010A	波特率不可用
0x010B	不可用的区域选择
0x0200	App Firmware 层程序 CRC 不正确
0x0302	Flash 未定义错误，闪存写入失败
0x0400	未发现标签，常见于功率不足或者过滤不匹配
0x0402	协议不可用
0x0404	写嵌入读时写成功读失败
0x040A	常规标签错误（读/写锁定，kill 命令）
0x040B	读取存储区域超出限制的长度（例如，一次只能读取 96 个字）
0x040C	不可用的销毁密码

Status Code	描述
0x0420	GEN2 协议错误
0x0423	存储区越界，错误的 PC
0x0424	锁定的存储区域
0x042B	能量不足
0x042F	非特定错误
0x0430	未知错误
0x0500	频率值不可用
0x0504	温度过高
0x0505	回波损耗过大，常见于金属反射的环境，也较少发生在频点，天线等原因
0x7F00	系统不知道的错误，严重错误
0x500F	宜链温度标签检测温度超出量程
0x50FF	宜链温度标签检测温度不稳定
0xAA02	写 OEM 寄存器失败
0xAA03	读 OEM 寄存器失败
0xAA04	该命令执行失败
0xAA2A	OEM 格式化失败

Status Code	描述
0xAA31	:载波开启或关闭操作失败
0xAA40	表示保存配置命令写 OEM 寄存器失败
0xAA4A	驻波检测失败
0xAA4B	表示复位 EX10 或上下电 EX10 等操作失败
0xAA4C	表示未有有效的设置多标签匹配过滤数据
0xAA4D	表示设置 SESSION2 /SESSION3　TARGET 为 A 失败
0xAA55	用户自定义存储区命令读写执行失败
0xAA56	用户自定义命令命令配置或读取执行失败
0xEE01	芯片未执行到应用层错误
0xEE02	芯片固件启动升级失败
0xEE03	芯片固件继续升级失败
0xEE04	芯片固件结束升级失败
0xFF11	FLASH 初始化失败
0xFF12	GPIO 初始化失败
0xFF13	定时器初始化失败
0xFF14	SPI 初始化失败

Status Code	描述
0xFF15	天线控制初始化失败
0xFF16	频段初始化失败
0xFF17	EX10 初始化失败
0xFF1F	固件异常
0xFFFF	硬件版本号错误
其它非 0	表示命令执行失败

附录

附录 1 CRC-16 C 语言示例

值得注意的是代码使用时候传入的是帧头 0xFF 的数组位置，实际计算 CRC，0xFF 不参与计算。

```
#define uint16 unsigned short
#define uint8 unsigned char

#define MSG_CRC_INIT                0xFFFF
#define MSG_CCITT_CRC_POLY          0x1021
void CRC_calcCrc8(uint16 *crcReg, uint16 poly, uint16 u8Data)
{
    uint16 i;
    uint16 xorFlag;
    uint16 bit;
    uint16 dcdBitMask = 0x80;
    for(i=0; i<8; i++)
    {
        xorFlag = *crcReg & 0x8000;
        *crcReg <<= 1;
        bit = ((u8Data & dcdBitMask) == dcdBitMask);
        *crcReg |= bit;
        if(xorFlag)
        {
            *crcReg = *crcReg ^ poly;
        }
        dcdBitMask >>= 1;
    }
}


uint16 CalcCRC(uint8 *msgbuf,uint8 msglen)
{
    uint16 calcCrc = MSG_CRC_INIT;
    uint8   i;
    for (i = 1; i < msglen; ++i)
        CRC_calcCrc8(&calcCrc, MSG_CCITT_CRC_POLY, msgbuf[i]);
    return calcCrc;
}
```

//测试实例

```
int _tmain(int argc, _TCHAR* argv[])
{
	// CRC
	//测试发送指令  FF 00 03 1D 0C
	uint8 sendata[5];
	sendata[0]=0xff;
	sendata[1]=0x00;
	sendata[2]=0x03;

	uint16 crc=CalcCRC(sendata,3);
	sendata[3]=(uint8)((crc&0xff00)>>8);
	sendata[4]=(uint8)(crc&0x00ff);

	printf("CRC0:%X,CRC1:%X\n",sendata[3],sendata[4]);
	scanf("%d",&crc);
	return 0;
}
```

调用函数 uint16 CalcCRC(uint8 *msgbuf,uint8 msglen)所得的返回数据就是 CRC-16,其中参数*msgbuf 为除了 CRC-16 之外的通信协议串数据，msglen 为除了 CRC-16 之外的所有通信协议串数据的总字节数。（因函数内是从 msgbuf[1]开始取数据的，所以*msgbuf 是包含帧头的除了 CRC-16 之外的通信协议串数据）

附录 2 波特率值表

Baud Rate (deciamal)	Baud Rate (hex)
9600	0x00002580
19200	0x00004B00
38400	0x00009600
57600	0x0000E100
115200	0x0001C200
230400	0x00038400
460800	0x00070800
921600	0x000E1000

附录 3 工作区域以及区域频率表

Regin Code Table

中国版模块（认证区域为中国）设置值与对应频率区域关系如下：

区域名	Region Code
North America(902-928)	0x01
China 1(920-925)	0x06
European(865-867)	0x08
Full Frequency Band(840-960)	0xFF

国外版本设置值与对应频率区域关系如下，国外版本只能设置对应国家的频段不能设置其他国家的：

区域名	Region Code
FCC（902-928）	0x01
CHINA1（920-925）	0x06
CE_LOW（865-867）	0x08
KOREA	0x09
JAPAN (NO LBT 4FRE)	0x0B
JAPAN2 (LBT 6FRE)	0x1F
JAPAN3 (NO LBT 19FRE,MAX power 24dBm)	0x20

区域名	Region Code
CE_HIGH	0x0C
HK	0x0D
TAIWAN	0x0E
MALAYSIA	0x0F
SOUTH_AFRICA	0x10
BRAZIL	0x11
THAILAND	0x12
SINGAPORE	0x13
AUSTRALIA	0x14
INDIA	0x04
URUGUAY	0x16
VIETNAM	0x17
ISRAEL	0x18
PHILIPPINES	0x19
INDONESIA	0x1A
NEW_ZEALAND	0x1B
PERU	0x1C

区域名	Region Code
RUSSIA	0x1D

区域频率表

不同区域的跳数表只能包含下表中的某些特定频率（全频带除外）。所以设置跳频命令只能选择属于读写器当前工作区域中的频率。全频带可以使用 840-960MHZ 的任何频率。执行设置当前工作区域命令后，区域频率表中的频率是每个区域的默认跳数表。

区域	频率(kHz)
North America(902-928)	915250,902750,927250,915750,903250,926750,908250,918250,923250,905250,916250,911250,921250,913250,906250,914250,909250,919250,924250,904250,917250,912250,922250,920250,907250,914750,909750,919750,924750,904750,912750,907750,917750,922750,910250,925250,910750,920750,925750,905750,913750,908750,918750,923750,903750,916750,911750,921750,926250,906750
China 1(920-925)	922125,920625,924375,922375, 920875,924125,922625,921125,923875,921875,923625,922875, 921375,923125,921625,923375
European(865-867)	865700, 866300, 866900, 867500
Full Frequency Band(860-960)	910000,860000,960000, 900000,870000, 940000,920000,890000,950000, 930000,880000
日本频段（无 LBT，916-921MHz)	916800　918000　919200　920400
日本频段 2（有 LBT，916-921MHz)	916800　918000　919200　920400 920600 920800

区域	频率(kHz)
日本频段 3（无 LBT，916-924MHz）	916800 918000 919200 920400 920600 920800 921000 921200 921400 921600 921800 922000 922200 922400 922600 922800 923000 923200 923400
韩国频段（917-921MHz）	917300 917900 918500 919100 919700 920300
香港频段（920-925MHz）	920250 920750 921250 921750 922250 922750 923250 923750 924250 924750
台湾频段（920-927MHz）	920750 921250 921750 922250 922750 923250 923750 924250 924750 925250 925750 926250 926750 927250
MALAYSIA 频段（919-923MHz）	919250 919750 920250 920750 921250 921750 922250 922750
SOUTH_AFRICA 频段（915-918MHz）	915600 915800 916000 916200 916400 916600 916800 917000 917200 917400 917600 917800 918000 918200 918400 918600 918800
BRAZIL 频段（902-927MHz）	902750 903250 903750 904250 904750 905250 905750 906250 906750 907250 907750 908250 908750 909250 909750 910250 910750 911250 911750 912250 912750 913250 913750 914250 914750 915250 915750 916250 916750 917250 917750 918250 918750 919250 919750 920250 920750 921250 921750 922250 922750 923250 923750 924250 924750 925250 925750 926250 926750 927250
THAILAND 频段（920-925MHz）	920250 920750 921250 921750 922250 922750 923250 923750 924250 924750
SINGAPORE 频段（920-925MHz）	920250 920750 921250 921750 922250 922750 923250 923750 924250 924750
AUSTRALIA 频段（920-925MHz）	920250 920750 921250 921750 922250 922750 923250 923750 924250 924750
INDIA 频段（865-867MHz）	865100 865700 866300 866900

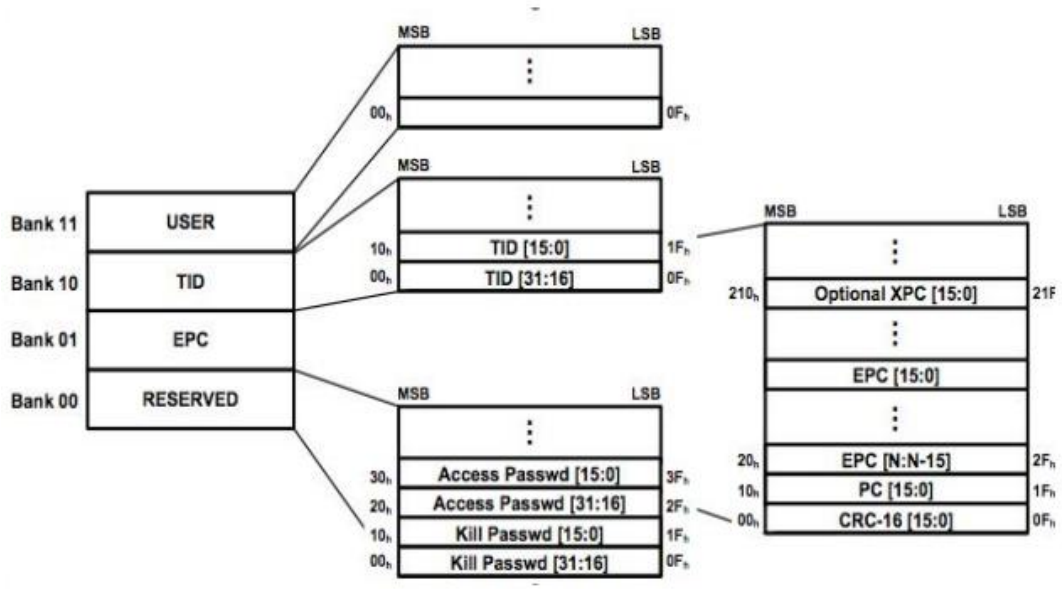
区域	频率(kHz)
URUGUAY 频段（916-927MHz）	916250 916750 917250 917750 918250 918750 919250 919750 920250 920750 921250 921750 922250 922750 923250 923750 924250 924750 925250 925750 926250 926750 927250
VIETNAM 频段（918-922MHz）	918750 919250 919750 920250 920750 921250 921750 922250
ISRAEL 频段（916MHz）	916250
PHILIPPINES 频段（918-920MHz）	918250 918750 919250 919750
INDONESIA 频段（917-922MHz）	917250 920750 921250 921750
NEW_ZEALAND 频段（922-927MHz）	922250 922750 923250 923750 924250 924750 925250 925750 926250 926750
PERU 频段（916-927MHz）	916250 916750 917250 917750 918250 918750 919250 919750 920250 920750 921250 921750 922250 922750 923250 923750 924250 924750 925250 925750 926250 926750 927250
RUSSIA 频段（916-920MHz）	916200　917400　918600　919800

附录 4 Gen2 标签内存结构

Gen2 Memory Map

When performing a Tag Singulation/Select most of the criteria specifies values of data in certain locations in a Gen2 tag's memory map. The following is a logical view of the Gen2 memory map from the Generation2 Protocol v1.2 that can be used for reference when trying to determine the memory address you are trying to match on:

Gen2 Tag Memory Map



序号	BANK	描述（1 块为 2 字节，16bits）
0	保留区	第一块，第二块为 Kill 密码区（块地址从 0 开始）。 第三块，第四块为 Access 密码区（块编号为 2，3）
1	EPC	第一块为 CRC，第二块为 PC，第三块（块编号为 2）开始为 EPCID
2	TID	从块地址 0 开始
3	USEER	从块地址 0 开始

附录 5 TagCRC C 语言示例

```
//SEED=0xFFFF;
//len 为 data 长度，单位字节
//*data 为标签 PC+EPC
//函数返回值就是标签 CRC
uint16 ISO6Ccrc16(uint16 seed,uint8 len,uint8 *data)
{
    uint8 mask;
    uint16 crcVal;
    crcVal = seed;
    for(;len;len--,data++)
    {
        for(mask = 0x80; mask; mask = mask >> 1)
        {
            if(crcVal & 0x8000)
            {
                crcVal = crcVal << 1;
                crcVal ^= 0x1021;
            }
            else
                crcVal = crcVal << 1;
            if(*data & mask)
                crcVal ^= 0x1021;
        }
    }
    return (~crcVal);
}


//tag CRC check    pc 3000    epc 05000000000000000002354        tagcrc 4AC8
uint8 pcepc[14]={0x30,0x00,0x05,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x23,0x54};

uint16 tagcrc=ISO6Ccrc16(0xFFFF,14,pcepc);
printf("CRC0:%02X,CRC1:%02X\n",(uint8)((tagcrc&0xff00)>>8),(uint8)(tagcrc&0x00ff));
```

附录 6 指令构建以及接收判断流程

构建发送指令流程

发送的指令是必须符合指令协议。

<1>首先依据功能确定操作码，由操作码决定帧指令符合通用指令通信协议格式还是扩展指令通信协议格式。

<2>其次，由操作码和具体实现功能决定指令的 Data 字段格式，Data 字段格式参考通信协议具体章节。

<3>再次，计算出 Data 字段的 Data Length 长度

<4>最后，计算整帧指令的 CRC

接收指令流程判断

返回的指令是必须符合指令协议。

接收数据可以先接收 5 个字节，这 5 个字节必须符合协议规定。

例如，前 5 个字节协议规定如下：

Header+datalen+opcode+status

<1>头字节必须是 0xFF

<2>次字节是长度，这个长度是 Data 长度，整个返回指令串长度是 datalen+5+2，5 是当前已经接收的 5 个字节，2 是结尾 2 个字节 CRC。

<3>Opcode 必须匹配发送的指令的操作码，如发送操作码 0x22，返回操作码也必须是 0x22。

<4>Status 必须是 0x0000，否则根据错误代码列表判断是何种错误。

<5>Data 字段解析参考具体章节内容。

<6>CRC 验证，如前 5 个字节已经顺利接收完毕，那么可以继续读取剩下长度指令，剩下需要读取 datalen+2 个字节数据，若取不到这个字节数可判断为丢包。顺利取完返回指令长度，最后需要计算 CRC 是否与最后两字节匹配。至此完成接收一帧的数据以及判断。

附录 7 SubCRC C 语言示例

发送指令：

FF	10	AA	4D 6F 64 75 6C 65 74 65 63 68	AA 40	AA	01	95	BB	8D 63
Header	Data Length	Command Code	Subcommand Marker (Moduletech)	Subcommand Code	KEY	GETORSET	SubCRC	Terminator	CRC

有上面指令，计算其 subCRC

```
unsigned char GetSubcrc(unsigned char *data,int len)
{
	int temp = 0;
	for (int i = 0; i < len; i++)
		temp += data[i];
	return (unsigned char)(temp & 0x000000ff);
}

unsigned char	opdata[]={0xAA,0x40,0xAA,0x01};
int len=4;
unsigned char	sbcrc=GetSubcrc(opdata,len);
printf("SubCRC:0x%02X\n",sbcrc);
```