VIKITEK

6100 系列读写器通信协议

简介：通信协议设计说明

规定 PC 机发给读写器的数据帧为命令，读写器返回给 PC 机的数据帧为响应。命令或响应数据帧是变长字节数，采用组包方法并用校验和方法进行后向检错。

命令或响应数据帧最长为 252 字节。

1 1 通信协议结构

1．1 命令帧格式**定义**

命令帧是主机操作读写器的数据帧，格式如下表所示：

Head	Addr	Len	Cmd	Parameter	…	Parameter	Check
0x0A	1 byte	n+2	1 byte	Byte 1		Byte n	cc

- Head 是帧头标志，定义为 0x0A
- Addr 是读写器地址，一般地址从 0～240，255（0xFF）为公用地址，254（0xFE）为广播地址。读写器接收自身地址、公用地址和广播地址的命令，对广播地址命令不做回复。
- Len 是包长域，表示 Length 域后帧中字节数。
- Cmd 是命令码域。
- Parameter 是命令帧中的参数域。
- Check 是校验和域，规定校验范围是从帧头域到参数域最后一个字节为止所有字节的校验和（相加取反加 1，取最后两位）。读写器接收到命令帧后需要计算校验和来检错。

1．2 响应帧格式**定义**

响应帧是读写器返回给主机的数据帧，响应帧包含了读写器需要采集的数据，其格式定义如下表所示：

Head	Addr	Len	Status	Response	…	Response	Check
0x0B	1 byte	n+2	1 byte	Byte 1		Byte n	cc

- Head 是包类型域，响应帧包类型固定为 0x0B。
- Addr 是读写器自身地址。
- Len 是包长域，表示 Length 域后帧中字节数。
- Status 表示命令所规定的操作执行的结果，0 表示正确执行，其他表示执行中发生异常。
- Response 是响应帧中的返回数据。
- Check 是校验和域，规定校验范围是从包类型域到参数域最后一个字节为止所有字

节的校验和。PC 机接收到命令帧后需要计算校验和来检错。

Status 域取值规定如下表所示：

序号	值	名 称	描　　叙
1	0x00	ERR_NONE	命令成功完成
	0x01	ERR_ GENERAL_ERR	笼统的错误
	0x02	ERR_PAR_SET_FAILED	参数设置失败
	0x03	ERR_PAR_GET_FAILED	参数读取失败
	0x04	ERR_NO_TAG	无标签
	0x05	ERR_READ_FAILED	标签读失败
	0x06	ERR_WRITE_FAILED	标签写失败
	0x07	ERR_LOCK_FAILED	标签锁定失败
	0x08	ERR_ERASE_FAILED	标签擦除失败
	0x09		
	0x0A		
	0xFE	ERR_CMD_ERR	命令不支持或参数超出范围
	0xFF	ERR_UNDEFINED	未定义错误

2 2命令帧定义

2.1 2.1 系统配置命令

2.1.1 Set Baud Rate

设置读写器 RS232 通信波特率。

Head	Addr	Len	Cmd	Parameter	Check
0x0A		0x03	0x20	baudrate	cc

baudrate 为需要设置的波特率参数。具体参数含义为：0x00，9600bps；0x01，19200bps；0x02，38400bps；0x03，57600bps；0x04，115200bps。

读写器接收到此命令帧后，以原来波特率返回无数据应答帧后修改读写器参数以新波特率进行通信。

2.1.2 Reset Reader

复位读写器命令帧。

Head	Addr	Len	Cmd	Check
0x0A		0x02	0x21	cc

读写器收到此命令帧后，先返回无数据应答帧，然后读写器复位。

2.1.3 Get Firmware Version

读取读写器软件版本命令帧。

Head	Addr	Len	Cmd	Check
0x0A		0x02	0x22	cc

当读写器收到此命令帧后，返回响应帧，响应帧中命令数据为 BootLoader 或读写器软件的固件版本，响应帧格式如下表所示：

Head	Addr	Len	Status	Response	Response	Check
0x0B		0x04	0x00	Major	Minor	cc

Major 为固件程序主版本。

Minor 为固件程序次版本。

2.1.4 Set Rf Power

设置读写器射频功率。

Head	Addr	Len	Cmd	Par1	Par2	Par3	Par4	Check
0x0A		0x06	0x25	Pwr1	Pwr2	Pwr3	Pwr4	cc

Pwr1~4 分别是 4 个天线的功率

读写器接收到此命令帧后，修改读写器 RF 功率值，并返回无数据应答帧。

2.1.5 Get Rf Power

查询读写器射频功率。

Head	Addr	Len	Cmd	Check
0x0A		0x02	0x26	cc

读写器返回帧如下：

Head	Addr	Len	Status	Par1	Par2	Par3	Par4	Check
0x0B		0x06	00	Pwr1	Pwr2	Pwr3	Pwr4	cc

2.1.6 Set Frequency

设置读写器频率。

Head	Addr	Len	Cmd	Par1	Par2	Check
0x0A		XX	0x27	Freq num(n)	Freq points(n bytes)	cc

Freq num：频率点数，如果 Freq num 为非零，则频率为 Freq points 中各项频点；如果 Freq num 为 0，则 Freq points 中一字节表示频率地区类型，分别为：

0：中国

1：北美

2：欧洲

Freq points 中自定义的频率范围是 900～930MHz 之间，以 250kHz 为步进的频率点索引。

2.1.7 Get Frequency

查询读写器频率。

Head	Addr	Len	Cmd	Check
0x0A		0x02	0x28	cc

读写器响应帧如下：

Head	Addr	Len	Status	Par1	Par2	Check
0x0B		XX	00	Freq num	Freq points(n bytes)	cc

2.1.8 Set Antenna

设置读写器天线工作状态。

Head	Addr	Len	Cmd	Parameter	Check
0x0A		0x03	0x29	Work ant	cc

Work ant:表示工作的天线，用掩码的方式表示。低 4 位分别表示四个天线是否开通，1 表示开通，0 表示不开通；高 4 位没有意义。

读写器收到此命令帧后，返回无数据应答帧

2.1.9 Query Antenna

查询读写器天线工作状态。

Head	Addr	Len	Cmd	Check
0x0A		0x02	0x2A	cc

读写器返回帧格式如下：

Head	Addr	Len	Status	Response	Response	Check
0x0B		0x04	0x00	Work ant	Ant Status	cc

Work ant 表示当前开通的天线状态，用掩码表示。

Ant Status 表示当前实际可用的天线，用掩码表示，1 表示可用，0 表示天线未接或不匹配。

2.1.10 Set Single Fast Tag Mode

读卡模式设置

Head	Addr	Len	Cmd	Parameters	Check
0x0A		0x03	0x15	Mode	cc

Mode: 0 为单卡（含少量多卡）快速模式，非 0 为大量卡（多卡）模式。

读写器收到此命令帧后，返回无数据应答帧

2.1.11 Get Single Fast Tag Mode

查询读卡模式

Head	Addr	Len	Cmd	Check
0x0A		0x02	0x16	cc

读写器返回帧格式如下：

Head	Addr	Len	Status	Response	Check
0x0B		0x03	0x00	Modulate_type	cc

2.1.12 Set Test Mode

设置读写器测试模式：

Head	Addr	Len	Cmd	Mode	Check
0x0A		0x03	0x2F	Mode	cc

Mode: 00 为打开功放；

01 为关闭功放；

02 为天线校准，天线校准在四个天线全部断开时使用

2.1.13 Set OutPort

设置可编程 IO 口（可编程 IO 口上电后默认为高电平输出）

Head	Addr	Len	Cmd	Parameter	Parameter	Check
0x0A		0x04	0x2D	Num	level	cc

Num 为 IO 口序号：00、01 分别为两个输出端口；02 为继电器输出

Level 为输出电平：0 为低电平，1 为高电平。

2.1.14 Set IP

设置 IP 地址

Head	Addr	Len	Cmd	IP	PORT	Check
0x0A		0x10	0x2C		AA+BB	cc

IP 为 4 字节的 IP 地址:

4 字节的子网掩码

4 字节的网关

PORT 为端口号 2 字节的数据 其中 AA 为底位 BB 为高位

如,配置读写器 IP 地址为 192.168.1.200 端口号为 100 时的命令如下:

0A FF 10 2C C0 A8 01 C8 FF FF FF 00 C0 A8 01 01 64 00 BF

C0 A8 01 C8 = 192.168.1.200

FF FF FF 00 = 255.255.255.0

C0 A8 01 01 = 192.168.1.1

Port: 64 =100

2.1.15 Get IP

查询 IP 地址

Head	Addr	Len	Cmd	Check
0x0A		0x02	0x2B	cc

返回

Head	Addr	Len	Status	Response	Check
0x0B		0x10	0x00	IP	cc

IP 为 4 字节的 IP 地址:

4 字节的子网掩码

4 字节的网关

PORT 为端口号 2 字节的数据 其中 AA 为底位 BB 为高位

2.1.16 更新读写器参数

更新读写器所有参数并重置读写器（不同于复位读写器）:

Head	Addr	Len	Cmd	Parameter	Check
0x0A		0x03	0x2F	05	cc

2.1.17 设置 LED 和蜂鸣器开关

设置 LED 和蜂鸣器提示开启和关闭:

Head	Addr	Len	Cmd	Parameter	Parameter	Check
0x0A		0x04	0x23	1B	level	cc

Level 为开关控制：00 为关闭声光提示，03 为打开声光提示。

2.2.2.2 ISO18000-6B标签操作命令

2.2.1 Iso Multi Tag Identify

Iso18000 多标签识别。

Head	Addr	Len	Cmd	Check
0x0A		0x02	0x60	cc

读写器收到此命令帧后，进行多标签识别操作。识别完成后返回本次识别的标签数目，标签数据存入读写器缓存区。应答帧格式如下：

Head	Addr	Len	Status	Response	Check
0x0B		0x03	0x00	TagCount	cc

TagCount 为标签数量。

2.2.2 Iso Multi Tag Read

Iso18000 多标签用户数据读取。

Head	Addr	Len	Cmd	Parameter	Check
0x0A		0x03	0x61	Start Addr	cc

Start Addr 为要读的用户数据的起始地址。

读写器收到此命令帧后，进行多标签用户数据读操作，读取每张标签由起始地址开始的 8 字节数据。识别完成后返回本次识别的标签数目，标签数据存入读写器缓存区。应答帧格式如下：

Head	Addr	Len	Status	Response	Check
0x0B		0x03	0x00	TagCount	cc

2.2.3 Iso Write

Iso18000 标签单字节写。

Head	Addr	Len	Cmd	Parameter	Parameter	Check
0x0A		0x04	0x62	Addr	Value	cc

Addr 为要写的标签地址；

Value 为要写入的数据。

读写器返回无数据应答帧。

2.2.4 Iso Read With UID

已知 UID 的情况下，读取数据。

Head	Addr	Len	Cmd	Parameter	Parameter	Check
0x0A		0x0B	0x63	UID(8byte)	Addr	cc

Addr 为起始地址,UID 为已知标签的 ID 号。读写器返回 9 字节数据。

Head	Addr	Len	Status	Response	Check
0x0B		0x0B	0x00	9 字节	cc

返回数据中，第一字节为天线号，后 8 字节为数据。

2.2.5 Iso Write With UID

已知 UID 的情况下，写标签数据。

Head	Addr	Len	Cmd	Parameter	Parameter	Parameter	Check
0x0A		0x0B	0x64	UID(8byte)	Addr	Value	cc

Addr 为要写的标签地址；

Value 为要写入的数据。

UID 为已知标签的 ID 号。

读写器返回无数据应答帧。

2.2.6 Iso Lock

Iso18000 数据锁定。

Head	Addr	Len	Cmd	Parameter	Check
0x0A		0x03	0x65	Addr	cc

Addr 为要锁定的标签地址；

2.2.7 Iso Query Lock

Iso18000 锁定查询。

Head	Addr	Len	Cmd	Parameter	Check
0x0A		0x03	0x66	Addr	cc

Addr 为要查询的标签地址；

应答帧格式如下：

Head	Addr	Len	Status	Response	Check
0x0B		0x03	0x00	Lock Status	cc

Lock Status 为锁定状态，0 为未锁定，1 为锁定。

2.2.8 Iso Lock With UID

已知 UID 的情况下，锁定标签数据。

Head	Addr	Len	Cmd	Parameter	Parameter	Check
0x0A		0x0B	0x69	UID(8byte)	Addr	cc

Addr 为要锁的标签地址；

UID 为已知标签的 ID 号。

读写器返回无数据应答帧。

2.2.9 Iso Query Lock With UID

已知 UID 的情况下，查询锁定。

Head	Addr	Len	Cmd	Parameter	Parameter	Check
0x0A		0x0B	0x6A	UID(8byte)	Addr	cc

Addr 为要查询的标签地址；

UID 为已知标签的 ID 号。

应答帧格式如下：

Head	Addr	Len	Status	Response	Check
0x0B		0x03	0x00	Lock Status	cc

Lock Status 为锁定状态，0 为未锁定，1 为锁定。

2.2.10 Iso Single Tag Read

Iso18000 单标签读取。

Head	Addr	Len	Cmd	Parameter	Check
0x0A		0x03	0x68	Addr	cc

Addr 为起始地址，当 Addr 为 0 时，读取 UID。读写器返回 9 字节数据。

Head	Addr	Len	Status	Response	Check
0x0B		0x0B	0x00	9 字节	cc

返回数据中，第一字节为天线号，后 8 字节为数据。

2.3 2.3 EPC GEN2标签操作命令

2.3.1 Gen2 Multi Tag Inventory

EPC Gen2 多标签盘询。

Head	Addr	Len	Cmd	Par	Check
0x0A		0x03	0x80	01	cc

Par: 当为 00 时，读卡器进行一次 EPC GEN2 多标签识别操作。当为 01 时，读卡器进行自动读卡，识别完成后返回本次识别的标签数目，标签数据存入读写器缓存区。应答帧格式如下：

Head	Addr	Len	Status	Response	Check
0x0B		0x03	0x00	TagCount(2 bytes)	cc

TagCount 为标签数量，两字节，高字节在前。

2.3.2 Gen2 Multi Tag Inventory Stop

停止 EPC Gen2 多标签盘询。

Head	Addr	Len	Cmd	Check
0x0A		0x02	0x81	cc

读写器收到此命令帧后，停止 EPC GEN2 多标签自动识别操作。

2.3.3 Gen2 Multi Tag Read Settings

为多标签读取定义每个读取区及其对应的首地址和读取长度。

Head	Addr	Len	Cmd	Parameter	Check
0x0A		0x0B	0x84	Wordptr&length(9bytes)	cc

Wordptr&length 9 个字节，分别是：
MembankMask：存储区选择，掩码表示。从第 1 到 4 位分别表示保留区、EPC 区、TID 区和 USER 区；
ReserveWordPtr：保留区读取首地址
ReserveWordCnt：读取字数
EpcWordPtr：EPC 区读取首地址
EpcWordCnt：读取字数
TidWordPtr：TID 区读取首地址
TidWordCnt：读取字数
UserWordPtr：User 区读取首地址
UserWordCnt：读取字数
需要注意的是，EPC 区默认是要读取的，但默认读取的是 PC 区规定的最大长度，如果实际存储大于 PC 定义的长度，可以通过此命令读取。

读写器收到此命令后，按预设的存储区、首地址和长度进行多标签数据读取，可以读取多个存储区。读取的内容存在缓存里，可以通过 Get Tag Data 命令来获取。应答帧格式如

下：

Head	Addr	Len	Status	Response	Check
0x0B		0x04	0x00	TagCount(2 bytes)	cc

2.3.4 Gen2 Muti Tag Write

EPC Gen2 多标签写入

Head	Addr	Len	Cmd	Parameter	Parameter	Parameter	Parameter	Check
0x0A		0xXX	0x85	Membank	Word Addr	len	Data	cc

World Addr 为要写入的字地址。

Data 为要写入的数据，长度为 len*2。

读写器收到此命令后，在所有辐射区域内的合法标签进行写入。写入后返回写入成功的标签数量，写入成功的标签 EPC 码会缓存，可以通过 Get Tag Data 命令来获取。

2.3.5 Gen2 Kill

EPC Gen2 单标签销毁。

Head	Addr	Len	Cmd	Parameter	Check
0x0A		0x06	0x83	Password	cc

Password 为销毁密码。为 4 个字节

读写器返回无数据应答帧。

2.3.6 Gen2 Secured Read

Head	Addr	Len	Cmd	Parameter	Parameter	Parameter	Parameter	Check
0x0A		0x09	0x88	Acc Pwd(4Bytes)	Membank	Word Addr	WordCnt	cc

Acc Pwd：4 字节访问密码；

Membank 为要读的区域

Word Addr 为要读的起始地址（以字为单位）

WordCnt 为要读的字数

如果输入密码为 0，则忽略密码执行普通的标签读。

2.3.7 Gen2 Secured Write

Head	Addr	Len	Cmd	Parameter	Parameter	Parameter	Parameter	Check
0x0A		0x0A	0x89	Acc Pwd(4Bytes)	Membank	World Addr	Value（2bytes）	cc

Acc Pwd：4 字节访问密码；

World Addr 为要写入的字地址（0～5）。

Value 为要写入的两字节数据。

读写器收到此命令后，在指定的地址对标签写入一个字（两字节）读写器返回无数据应答帧。

如果输入密码为 0，则忽略密码执行单普通的标签写。

2.3.8 Gen2 Secured Lock

Head	Addr	Len	Cmd	Parameter	Parameter	Parameter	Check
0x0A		0x08	0x8A	Acc Pwd(4Bytes)	MemBank	Level	cc

Acc Pwd：4 字节访问密码；

MemBank 为要锁定的标签区域，从 0 到 4 依次是 User,TID,EPC,Access Pwd,Kill Pwd。

Level:锁定等级，0 为不锁定，1 为永久不锁定，2 为安全锁定，3 为全锁定。

如果输入密码为 0，则忽略密码执行普通的单标签锁定。

2.3.9 Gen2 Select Config

配置标签选择功能参数

Head	Addr	Len	Cmd	Parameter	Parameter	Parameter	Parameter	Parameter	Check
0x0A		0xXX	0x8F	Action	Membank	Bit Ptr（2bytes）	Length	Mask(Nbytes)	cc

Action: 0 表示选择匹配的，1 表示选择不匹配的

Membank：匹配的区

Bit Ptr：位地址，如 EPC 的第一个字节位地址为 0x20

Length：比较的位长度

Mask：比较的数据，最大 16 字节

2.3.10 Set Gen2 Parameters

设置读写器 EPC GEN2 相关参数命令帧。

Head	Addr	Len	Cmd	Par1	Par2	Par3	Par4	Check
0x0A		0x06	0x8E	Session	Rsv	Rsv	Rsv	cc

Session：盘询 EPC 标签时使用的 Session。

其他参数预留以后使用

2.4 2.4 缓存管理命令

2.4.1 Get ID And Delete

从缓存区中取标签的 EPC 码（6B 则是取 ID 号），取完后删除数据。

Head	Addr	Len	Cmd	Parameter	Check
0x0A		0x03	0x40	Count	cc

Count 为要取出的标签数量，最大为 18。应答帧格式如下：

Head	Addr	Len	Status	Response	Response	Check
0x0B		14*n+3	0x00	Count	Data(14*n)	cc

Count 为本次上传的标签数量，Data 为标签数据。标签数据以 14 字节为一组，每组第一个字节表示标签类型，第二字节表示天线号，后面 12 字节为标签数据。

2.4.2 Get Tag Data

从缓存区中取标签数据。

Head	Addr	Len	Cmd	Parameter	Check
0x0A		0x03	0x41	Count	cc

Count 为要取出的标签数量，最大为 16（数据过长时不超过最大帧长度限制）。应答帧格式如下：

Head	Addr	Len	Status	Response	Response	Check
0x0B			0x00	Count	Data	cc

Count 为本次上传的数据组数，Data 为标签数据。

Data 以组为单位，每组第一个字节是该组数据长度（不包括自身），后续为有效数据。下面是常用的几个返回数据的 Data 数据组单位：

ISO18000-6B 标签识别：

Len	ant	ID
9	1 字节	8 字节

EPC 标签识别：

Len	ant	EPC
13	1 字节	12 字节 EPC

* :EPC 识别也可能不是 12 字节，根据标签的 PC 定义。

EPC 读取：

Len	ant	EPC+DATA
n	1 字节	EPC+其它区数据

n=要读取的数据字节总数+EPC 长度。EPC 是可变长度的，所以他的长度反过来要根据 n 来减去要读取的数据长度。

2.4.3 Query ID Count

查询缓存区中的数据组数。

Head	Addr	Len	Cmd	Check
0x0A		0x02	0x43	cc

读写器应答帧格式如下：

Head	Addr	Len	Status	Response	Check
0x0B		0x03	0x00	Count（2Bytes）	cc

Count 为缓存区中的标签数量。

2.4.4 Clear ID Buffer

清空缓存区。

Head	Addr	Len	Cmd	Check
0x0A		0x02	0x44	cc

读写器返回无数据应答帧。

* :在每次发送多标签识别或读写命令时，缓存会自动清空。

*:在事件触发读卡模式下，缓存数据采用非易失性存储，掉电可保存。其控制命令同内存。

2.4.5 Clear Buffer

清空外部存储器：

Head	Addr	Len	Cmd	Check
0x0A		0x02	0x48	cc

读写器返回无数据应答帧。

数据采用非易失性存储，掉电可保存。

2.4.6 Get Buffer Count

查询外部存储器中的标签数量：

Head	Addr	Len	Cmd	Check
0x0A		0x02	0x49	cc

读写器应答帧格式如下：

Head	Addr	Len	Status	Response	Check
0x0B		0x04	0x00	Count（2Bytes）	cc

Count 为 Buffer 中的标签数量。

2.4.7 Get Buffer Data

从外部存储器中取标签数据。

Head	Addr	Len	Cmd	Check
0x0A		0x02	0x4A	cc

应答帧格式如下：

Head	Addr	Len	Status	Response	Response	Check
0x0B			0x00	Count	Data	cc

Count 为本次上传的数据总数，Data 为标签数据。

Data 以组为单位，每组第一个字节是该组数据长度（不包括自身），后续为有效数据。下面是常用的几个返回数据的 Data 数据组单位：

ISO18000-6B 标签识别：

Len	ant	ID
9	1 字节	8 字节

EPC 标签识别：

Len	ant	EPC
13	1 字节	12 字节 EPC

* :EPC 识别也可能不是 12 字节，根据标签的 PC 定义。

EPC 读取：

Len	ant	EPC+DATA
n	1 字节	EPC+其它区数据

n=要读取的数据字节总数+EPC 长度。EPC 是可变长度的，所以他的长度反过来要根据 n 来减去要读取的数据长度。

数据采用非易失性存储，掉电可保存。