MR6100 RFID Reader Communication Protocol

Brief introduction：Communication protocol design description

Data frame sent by PC to reader is defined as COMMAND，and the data frame returns from reader to PC is as REPONSE。COMMAND or REPONSE data frames are specified in bytes numbers，using group package and checksum methods for Backward error detection。

The maximum length of COMMAND or REPONSE data frame is 252 bytes。

1 Communication protocol structure

1.1. Command frame format definition

Command frame is the data frame used by PC to operate on the reader. The format is as the following table indicates：

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

- Head is the frame header's mark，define as 0x0A
- Addr is set as reader's address. Generally the address from 0～240，255（0xFF）is assigned as public address and 254（0xFE）as broadcast address. Reader receives the command of its own address、public address and broadcast address，but not does answer to broadcast address。
- Len is Packet length field, which indicates the bytes number in the rear frame of Length field。
- Cmd is Command code field。
- Parameter is the parameter field of the command frame。
- Checks is Checksum field，The check area is defined as all the bytes checksum of the last bytes from header field to parameter field (Reversed sum plus one，with the last two bytes retained). After receiving command frame, reader needs to calculate checksum for error detection.

1.2 Response frame format definition

Response frame is the data frame returned from reader to PC.. It includes the data that reader needs to collect. The format definition is as the following table indicates：

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

- Head is packet types field. Response frame packet type is fixed to 0x0B。
- Addr is the address of reader
- Len is packet length field，which indicates the number of bytes in the frame domain of Length。
- Status means the operating result from the command execution? 0 means correct operation，others mean error in the operation。
- Response is the data returned by response frame。
- Check is checksum field. The check area is defined as all bytes checksum of the last byte from packet type field to parameter field。When PC receives command frame, checksum needs to be calculated for error detection。

Status field to get value is like following table indicates：

NO.	Vale	Name	Description
1	0x00	ERR_NONE	Command successfully completed
	0x01	ERR_ GENERAL_ERR	General error
	0x02	ERR_PAR_SET_FAILED	Parameter setting failed
	0x03	ERR_PAR_GET_FAILED	Parameter reading failed
	0x04	ERR_NO_TAG	No tag
	0x05	ERR_READ_FAILED	Tag reading failed
	0x06	ERR_WRITE_FAILED	Tag writing failed
	0x07	ERR_LOCK_FAILED	Tag locking failed
	0x08	ERR_ERASE_FAILED	Tag erase failed
	0x09		

	0x0A		
	0xFE	ERR_CMD_ERR	Command not supported or parameter out of range
	0xFF	ERR_UNDEFINED	no definition error

2 Command frame definition

2.1 System setting command

2.1.1 Set Baud Rate

Set reader RS232 communication band rate。

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

Baudrate is the band rate parameter that need to be set。The specific parameters are：0x00，9600bps；0x01，19200bps；0x02，38400bps；0x03，57600bps；0x04，115200bps

After the reception of this command frame，the reader will use the previous band rate to return no data response frame, then will modify reader parameter and use new band rate for communication.

2.1.2 Reset Reader

Reset reader command frame。

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

After the reception of this command frame，the reader will return no data response frame, and then reader will be reset

2.1.3 Get Firmware Version

Read reader software version command frame。

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

After the reception of this command frame，the reader will return response frame. The command data of response data is BootLoader or firmware version of the reader software，The response frame format is as follows：

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

Major is the main version of the firmware。

Minor is the firmware minor version。

2.1.4 Set Rf Power

Set reader RF power。

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

Pwr1~4 is the power of four antennas

After the reception fo this command frame，the reader will modify the RF power value of reader，and return no data response frame

2.1.5 Get Rf Power

Query the reader RF power。

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

The reader back frame is as follows：

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

2.1.6 Set Frequency

Set reader frequency。

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

Freq num：meaning frequency points. A non zero value of Freq num means the frequency is defined by the various frequencies points in Freq points. Value 0 of Freq num means that a byte represents the frequency region type in Freq points. The region types are as follows：

0：China

1：North America

2：Europe

Self-defined frequency range of Freq points is 900～930MHz，using 250kHz stepping frequency point for index

2.1.7 Get Frequency

Query reader frequency。

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

The reader response frames is as below：

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

2.1.8 Set Antenna

Set working mode of reader antennas。

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

Work ant: means working antenna，represented by mask off code. Low 4 indicates whether the four antennas are opening，1 = opening，0 = not opening；High 4 has no meaning。

After the reception of this command frame，the reader will returns no data response frame

2.1.9 Query Antenna

Query working mode of reader antennas。

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

Reader back frame format is as below：

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

Work ant means the present opening antenna mode，represented by mask off code. Ant Status mean the antenna that can be used now，represented by mask off code，1 = able to use，0 = no antenna connects or antenna doesn’t match。

2.1.10 Set Single Fast Tag Mode

Reading mode setting

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

Mode: 0 = single tag（includes a small amount of multi-tag）fast mode，Not 0 = a large number of tags（multi-tag）mode。

After the reception fo this command frame, the reader returns no data response frame

2.1.11 Get Single Fast Tag Mode

Query reading mode

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

Reader back frame format is as below：

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

2.1.12 Set Test Mode

Set reader testing mode：

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

Mode: 00 = opening amplifier；

01 = real time amplifier；

02 = antenna calibration， antenna calibration is used when four antennas disconnect at the same time

2.1.13 Set OutPort

Set programmable IO port（The default programmable IO port uses high-;level output after power-on）

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

Num is IO port NO.：00、01 = the two ports for output；02 = relay output

Level = output level. 0 = low level. 1 = high level。

2.1.14 Set IP

Set IP address

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

IP is 4 bytes IP address:

4 bytes subnet Mask off code

4 bytes gateway

PORT is port Number with 2 bytes data AA is button byte BB is high byte.

Example to set reader: IP address 192.168.1.200 port number is 100. The command is as below:

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

Query IP address

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

Returns

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

IP is 4 bytes IP address:

4 bytes subnet Mask off code

4 bytes gateway

PORT is port number with 2 bytes data. AA is button byte BB is high byte.

2.1.16 Update the reader parameter

Update all of the reader parameters and refresh the reader (Note: difference to the reset)

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

2.1.16 Update the reader parameter

Update all parameters of the reader and reset the reader (different from reset reader）：

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

2.1.17 Set LED and buzzer switch

Set LED and buzzer switch open and close：

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

Level is switch control：00 means to close sound and light，03 means to open sound and light。

2.2 ISO18000-6B tag operation command

2.2.1 Iso Multi Tag Identify

ISO18000 multi-tag idenfity。

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

After the reception of this command frame，the reader operates multi-tag identify。Then it returns the tags number detected. The tags data will be stored to reader buffer。The response frame format is as below：

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

TagCount means tags quantity

。

2.2.2 Iso Multi Tag Read

Iso18000 multi-tag user data reading。

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

Start Addr means the start address of user data that needs to be read。

After the reception of this command frame，the reader operates multi-tag user data identifying，by reading every tag from start address to the 8th bytes data。 Then it will return the tag numbers detected. The tags data will be stored to reader buffer。The response frame is as below：

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

2.2.3 Iso Write

ISO18000 ttag single byte write

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

Addr is the tag address needs to write

Value is the data needs to write

The reader will return no data response frame.

2.2.4 Iso Read With UID

Read the data when UID is known

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

Addr is the starting address, UID is the ID NO.of the known tag. The reader will return 9 bytes data.

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

In the returned data, the first byte is antenna number and the latter 8 bytes are data.

2.2.5 Iso Write with UID

Write tag data when UID is known

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

Address is the tag address f needs to write

Value is the data needed to be written

UID is the ID number of the known tag

The reader returns No Data response frame.

2.2.6 Iso Lock

ISO18000 tag lock

Head	Addr	Len	Cmd	Parameter	Check
0x0A		0x02	0x65	Addr	cc

Address is the address for the tag needs to lock

2.2.7 Iso Query Lock

Iso18000IB locking inquiry。

ISO18000 query lock

Head	Addr	Len	Cmd	Parameter	Check
0x0A		0x02	0x66	Addr	cc

Address is the tag address needs to query.

The response frame format format is like the following table indicated

:

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

Lock status. 0 means unlocked,　1 means locked

2.2.8 Iso Lock With UID

ISO18000-6B tag lock with UID

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

Addr is the address of the locking tag

UID is the ISO18000-6B tag Unique ID.

Response frame return without value from the reader

2.2.9 Iso Query Lock With UID

ISO18000-6B tag query lock with UID

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

Addr is the address of the querying tag.

UID is the ISO18000-6B tag Unique ID

Response frame is below like:

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

Lock Status: ‘0’ means unlocked, ‘1’ means locked.

2.2.10 Iso Single Tag Read

ISO18000 single tag read

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

Addr is the starting address. When the address is 0, the reader reads UID and returns 9 bytes data

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

In the returned data, ,the first byte is antenna number and the latter 8bytes are data.

2.3 EPC Class1 Gen2 Tag Command

2.3.1 Gen2 Multi Tag Inventory

EPC Gen2 Multi Tag inventory

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

If Par=00, reader starts the first EPC Gen2 multi tag reading. If Par=01 reader starts the active reading, and returns the tag number when finish the identity,. Tags data are stored in the reader buffer.

Response frame is as below:

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

TagCount is the tag number; displayed in two bits. Big endian bits is at the first position.

2.3.2 Gen2 Multi Tag Inventory Stop

EPC Gen2 multi tag inventory stop

Head	Addr	Len	Cmd	Check

0x0A		0x02	0x81	cc

The reader stops the EPC Gen2 multi tag inventory when the above command frame received.

2.3.3 Gen2 Multi Tag Read Settings

EPC Gen2 Multi Tag Read Setting defines EPC Tag’s Membank as well as the first addr and the length of the Address.

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

Wordptr&length has 9 bytes which define respectively the following 9 cases:
MembankMask: from 1 to 4 are Reserve Membank, EPC Membank, TID Membank and User Membank.
ReserveWordPtr: The first word address of Reserve Membank.
ReserveWordCnt: The word count of the Reserve Membank
EpcWordPtr: The first word address of EPC Membank
EpcWordCnt: The word count of the EPC Membank
TidWordPtr: The first word address of TID Membank.
TidWordCnt: The word count of the TID Membank
UserWordPtr: The first word address of User Membank.
UserWordCnt：The word count of the EPC Membank.

When reader receives the above command frame, the reader starts to read with the pre-setting to read multi-tag’s multi Membank. The tag data is stored in the reader buffer and via *Get Tag Data* command to get buffer data. Response frame is as below:

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

2.3.4 Gen2 Muti Tag Write

EPC Gen2 Multi Tag Write

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

WorldAddr means bit address to be written.

Data is the data to be written with the length of Len*2

When reader receives the above command frame, it starts the validated multi tag writing in the reader's radiation range, and returns the successfully written tag number. The written tag EPC data are stored in the reader buffer. The reader can get these tags data via *Get Tag Data* command.

2.3.5 Gen2 Kill

Epc Gen2 Tag kill

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

Password is the kill code with 4 bytes

The reader returns Without data response frame.

2.3.6 Gen2 Secured Read

Head	Addr	Len	Cmd	Parameter	Parameter	Paramet er	Parameter	Chec k
0x0A		0x09	0x88	Acc Pwd(4Bytes)	Membank	Word Addr	WordCnt	cc

Acc Pwd: Access Password

Membank represents the read Membank

Word Addr means the read Membank starting address.

WordCnt is the word counter

Attention: If access password is 0, the password is ignored, and the reader executes the normal reading of the EPC tag.

2.3.7 Gen2 Secured Write

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

Acc Pwd:= 4 bytes Access Password

World Addr = the writable address (from 0-5)

Value = 2 bytes writable value

The reader encodes 2 bytes into the tag when reception of the above command, and returns a no data response frame.

If AccPwd=0, the reader ignores the Access password, and executes the normal encoding of the EPC tag

2.3.8 Gen2 Secured Lock

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

AccPwd:= Access Password

The lock MemBank from 0 to 4 are: User Membank, TID Membank, EPC Membank, Access Password Membank, Kill Password Membank.

Lock Level: ‘0’---unlock; ‘1’---unlock forever; ‘2’---secure lock; ‘3’---Lock forever

If AccPwd=0, the reader ignores the Access password, and executes the normal single tag lock.

2.3.9 Gen2 Select Config

EPC Gen2 Select Config

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

Action: ‘0’---Matched, ‘1’---unmatched

Membank represents the Match membank

Bit Ptr is bit address, for example, the first bit of the EPC address is 0x20

Length: the comparative bit length;

Mask: the comparative data, 16bits is the biggest value.

2.3.10 Set Gen2 Parameters

Set EPC Gen2 Parameters command frame:

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

Sesson: used for EPC Gen2 inventory

Rsy: reserved to the future purpose.

2.4 Buffer Management command

2.4.1 Get ID And Delete

Get tag EPC code or ISO18000-6B Tag’s ID code from reader buffer, and then delete buffer data.

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

Count is the tag number, 18bits is the biggest. Response frame is as below:

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

Count is the transmitted tag number, Data is the tag data. 14bits is a group of tag data, The first bit of the group is the tag type. The second bit is the antenna number, the left 12bits forms the EPC code.

2.4.2 Get Tag Data

Get tag data from reader buffer.

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

Count is the get tag number, 16bits, the response frame is as below:

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

Count = the upload tag data of different Membank combination. Data = the tag data.

Data group as a unit, the first byte of the unit is the length of the Membank combination (Exclude data group).

The following is the common data return of the data of different Membank combination.

ISO18000-6B tag Identify

Len	ant	ID
9	1byte	8bytes

EPC Tag Identify

Len	ant	EPC
13	1byte	12 bytes EPC code

* Attention: Depending on different EPC tag Chips, the EPC code can be more than 12bytes.

EPC Read

Len	ant	EPC+DATA
n	1byte	EPC Code + other Membank data

n= the total number of bytes of data to be read + EPC length. As EPC has a variable length, the length of EPC code in return is according to the n minus the length of to be read Membank data.

2.4.3 Query ID Count

Query buffer data group.

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

Reader response frame is below like.

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

Count is the tag number in the buffer.

2.4.4 Clear ID Buffer

Clear ID buffer

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

No data response frame from the reader

*: Auto buffer is cleared each time when the command R/W is executed by the reader.

*: In Trigger mode reading, the data is saved in nonvolatile data storage with power-down data protection. The control command is the same as RAM.

2.4.5 Clear Buffer

Clear the external memory

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

No data response frame from the reader

Nonvolatile data storage, power-down data protection.

2.4.6 Get Buffer Count

Query the external memory tag number:

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

Reader response frame is as below:

Head	Addr	Len	Status	Response	Check

0x0B		0x04	0x00	Count（2Bytes）	cc

Count is the tag number in the buffer

2.4.7 Get Buffer Data

Get tag data from the external memory:

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

Response frame is below like:

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

Count is the upload tags total number. Data is the tag data.

Data takes group as unit. The first byte of the unit is the length of the group. (Excluding data group itself). The following bytes are effective data.

The following is the common returned data unit groups:

ISO18000-6B Tag Identify

Len	ant	ID
9	1byte	8bytes

EPC Tag Identify

Len	ant	EPC
13	1byte	EPC12bytes

* Attention: According to different EPC tag Chip, the EPC code can be more than 12 bytes.

EPC read

Len	ant	EPC+DATA
n	1byte	EPC+ Other Membanks' data

n= the total number of bytes of data to be read + EPC length. As EPC has a variable length, the length of EPC code should be counted by the n minus the length of Membank data to be read.

Data is saved by nonvolatile data storage with power-down data protection.

3. Technical Support

If you need support for reader product, please note your reader's model number, serial number and firmware revision. . Marktrace is committed to providing quick and effective support to our customers and partners. Please contact Marktrace Technical support Department by sending mails to: technical@marktrace.com

4，Command Appendix
