Data Communication Protocol

HOPELAND RFID READERS PC

Editor: Paul

Shenzhen Hopeland Technologies Co., Ltd

V 1.12

Revision record

Version	Revision content	Editor/Date
V1.0	1st version finished	2014-9-28
V1.1	Add PR9200 feedback parameter calibration	2015-8-28
V1.2	Add new GB, antenna expanding function	2015-8-1
V1.3	Add breakpoint resume, ACK response	2016-5-12
V1.4	Add buffer clear function, change the buffer response instruction type into 0x01; Read labels to increase the frequency, phase upload.	2016-6-23
V1.5	Function extension EPC C2G2 V2.0 encryption authentication read function Added the tag data untraceable function of EPC C2G2 V2.0	2018-9-4
V1.6	Update configuration description of RF power	2020-11-10
V1.7	Add the description of custom output data format	2022-5-31
V1.8	Add the baseband extended paramters	2022-6-30
V1.9	Add description of frequency band and EPC baseband speed	2022-11-7
V1.10	Add querying RFID temperature	2023-12-20
V1.11	Add optional reporting parameters and update tag data output format	2024-2-28
V1.12	Add querying working status	2024-10-31

Contents

1 Introduction

1.1 Purpose

This document is to define the data communication interface between Hopeland RFID reader and upper computer (controller). The designing between upper computer (controller) and Hopeland RFID reader must comply with data interface protocol.

1.2 Application

The models applied: CL7206A/B/C/D series. This document is aimed at reader developers, API interface developers, system integration developers, and reader technical support staff.

1.3 Definition

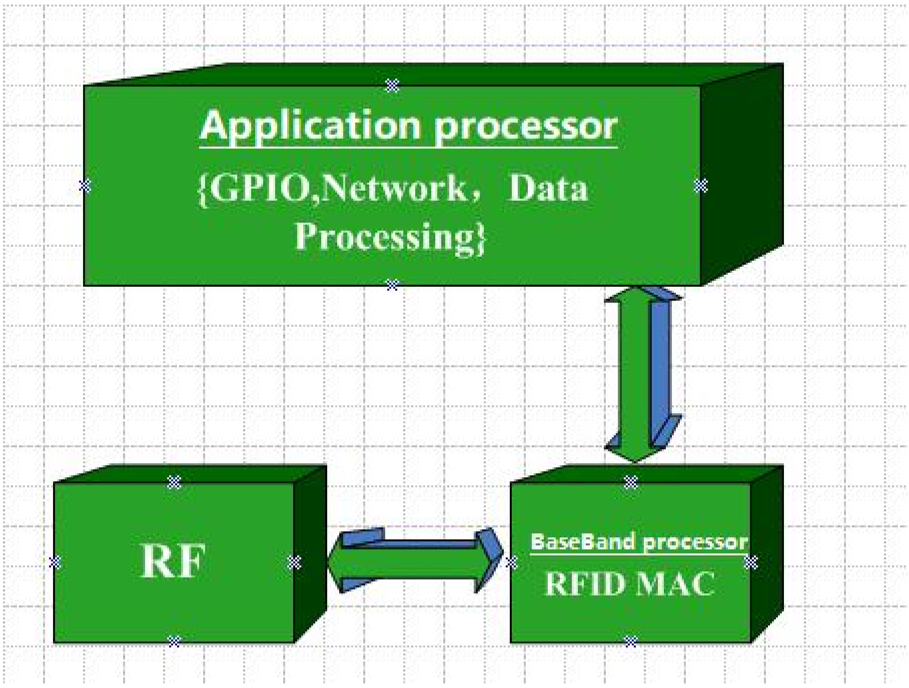
HRP: Hopeland Reader Protocol
U8，unsigned char
S8，signed char
U16，unsigned short
S16，signed short
U32，unsigned long
S32，signed long

1.4 Reference document

1. EPC™ Radio-Frequency Identity Protocols Class-1 Generation-2 UHF RFID Protocol for Communications at 860 MHz–960 MHz Version 1.2.0

2 Overview

2.1 Basic hardware framework



RFID reader basic hardware is composed by: application processor unit, RFID baseband processor unit, RF hardware circuit unit.

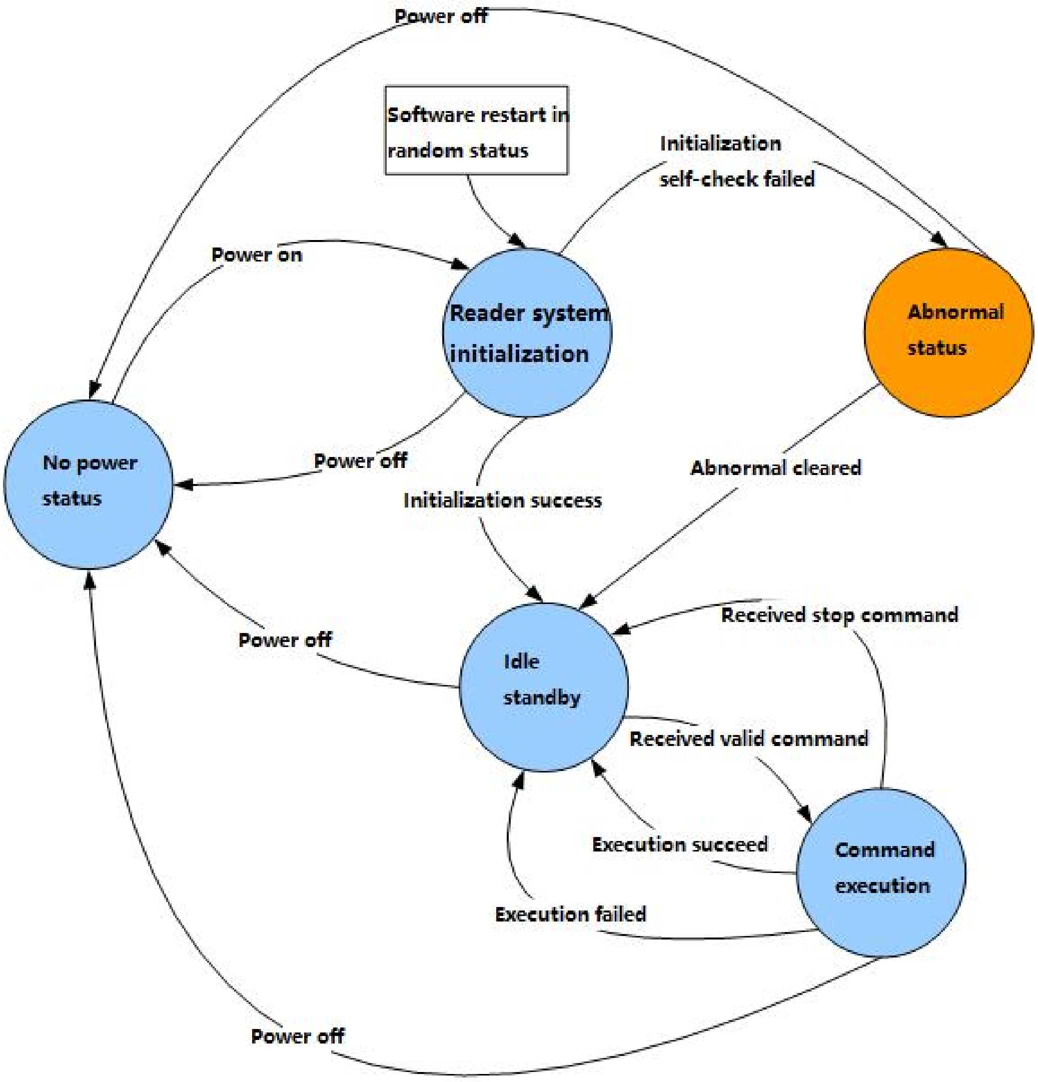
Application processor: mainly in charge of reader & Upper computer network communication, data processing, GPIO etc. which are related with applications.

RFID baseband processor: in charge of data exchange and protocol procedure control between reader and tag.

RF circuit unit: in charge of physical signal transmission between reader and tag.

In real reader designing, application processor and baseband processor can adopt two processor to realize separately or can be combined into one processor.

2.2 Basic Operation Mechanism



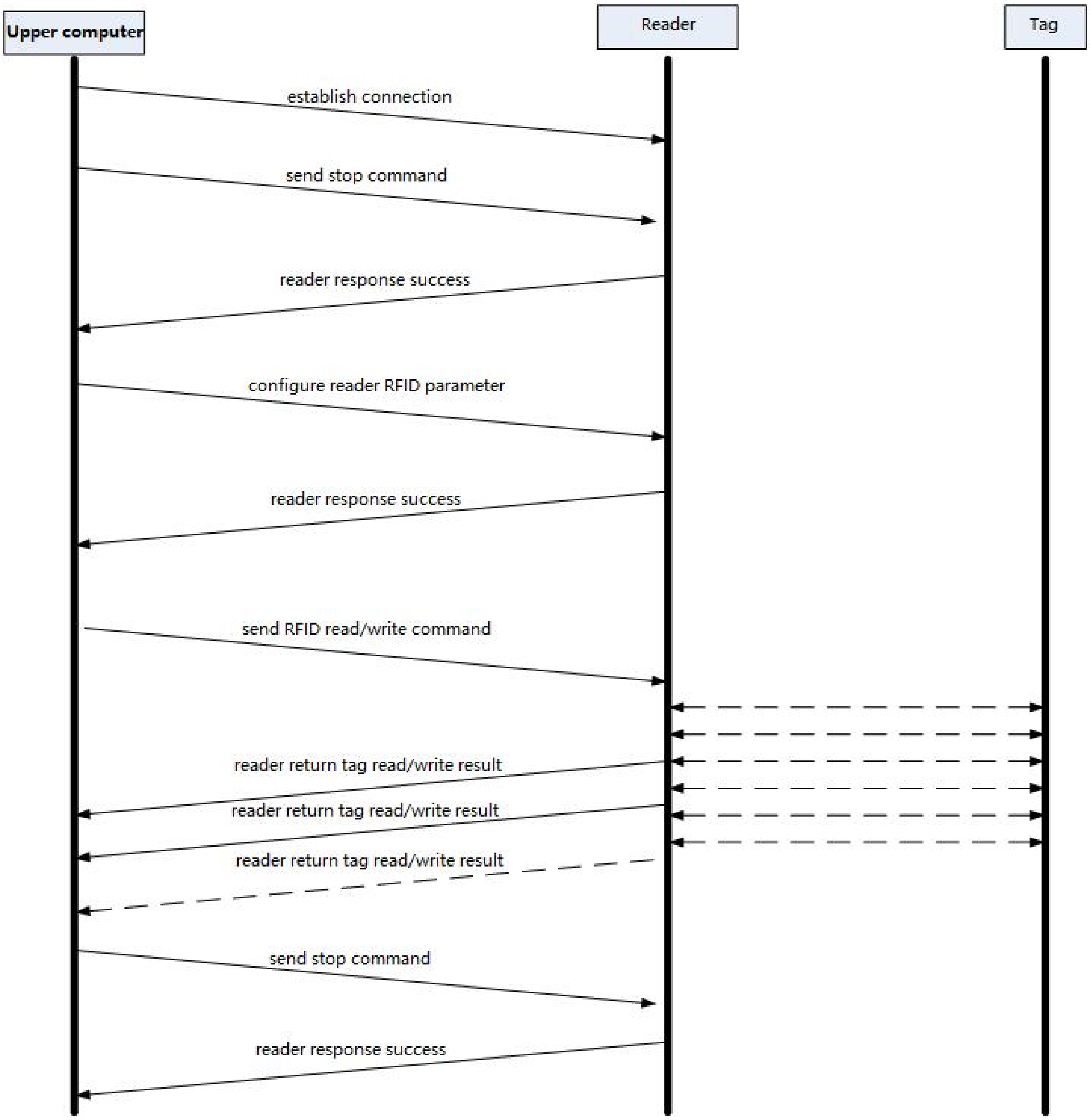
Reader system initiation: operation system started, each function module hardware status self-check, reader system parameter initialize. In this status reader cannot receive and execute any Upper computer command.

Idle standby: reader finished initialization and wait for Upper computer commands. In this status reader can receive command and execute.

Execute command: reader received complete eligible upper computer instruction and switch to execution status. When executing recycle read/write operations, reader will only response to stop operation, GPIO input/output operation, parameter query operation.

Abnormal status: when there is abnormal during system initialization and self-check, system will enter abnormal status. This status is for realizing abnormal warning and system debugging interface, for RD debugging and locate abnormal quickly causing in production.

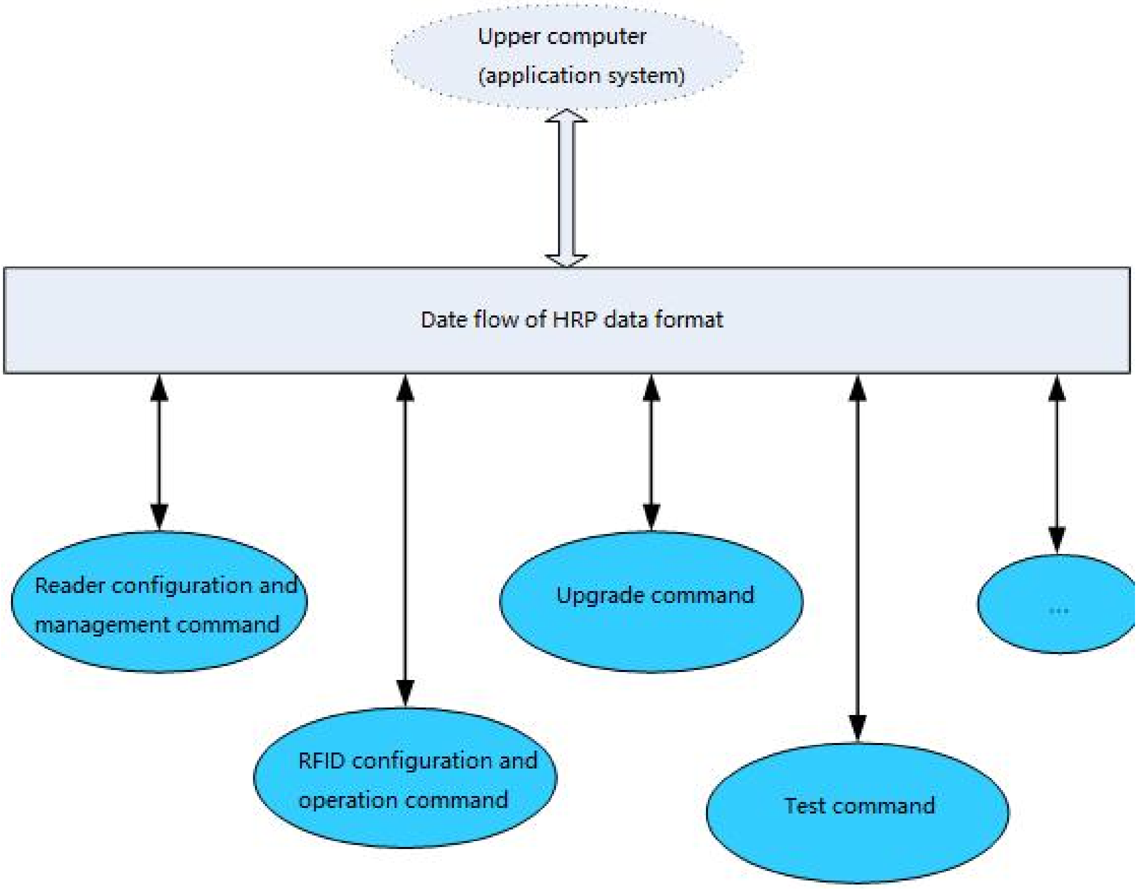
2.3 RFID Read/Write Basic Procedure


Upper computer
Reader
Tag
establish connection
send stop command
reader response success
configure reader RFID parameter
reader response success
send RFID read/write command
reader return tag read/write result
reader return tag read/write result
reader return tag read/write result
send stop command
reader response success

Upper computer initiates connection with reader through designated port, after connection succeed,upper computer firstly sends stop command to reader. The purpose of upper computer sending stop command is: 1, reader switch to idle status, can response to following commands; 2, can confirm if the reader is in normal status by the response from reader.

2.4 Protocol Basic Framework

Reader protocol framework as per in below picture. Reader commands mainly includes: reader parameter & configuration, RFID reader/write, stop command, GPIO command.


Upper computer
(application system)
Date flow of HRP data format
Reader configuration and management command
Upgrade command
...
RFID configuration and operation command
Test command

3 Data Format

3.1 Frame structure

Frame head	Protocol control word	Serial device address	Data length	Data parameter	Calibration code
0xAA	2 bytes	1 byte	2 bytes(U16)	N bytes	2 bytes

Frame head： Take hexadecimal“0xAA” as start marking of a frame data.

Protocol control word： for marking current message type. Detailed bit definition as following:

Bit segment	Definition	Description
15-14	Reserved bit	Keep as 0
13	RS485 flag bit	0,This message is not applied for RS485 communication. 1, This message is used for RS485 communication.
12	Reader actively upload message flag bit	0， Means this message is upper computer command or reader response to upper computer command. Not initiated by reader. 1， Means this message is initiated by reader.
11-8	Message type number	0， Reader error or warning message 1， Reader configuration and management message. 2， RFID Configuration and operation message. 3， Reader log message. 4， Reader application processor software and baseband software upgrade message. 5， Testing command. 0x6~0xF，reserved.
7-0	Message ID	0x00~0xFF，differentiate detailed message below same type message. For short in below: MID。

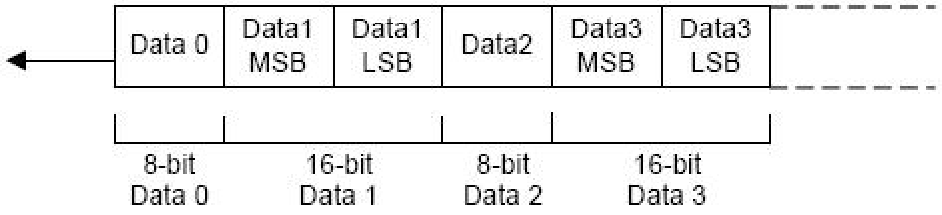
Serial device address： For marking target reader RS485 address, value range 0x00~0xFF. Only when protocol control word RS485 flag bit is 1, message will include this field, or message don't include this field.

Data length: indicates data content byte length. Currently the maximum data content length that reader support is 1024bytes.

Data parameter: Upper computer command and parameter information or reader uploaded message content.

Checksum: data CRC16 checksum except for frame head. Calibration algorithm adopt CCITT-16, calibration polynomials is $X^{16} + X^{15} + X^{2} + 1$, initiation value is set as 0.

During data transmission, byte ordering adopt big-endian. As in below chart:



3.2 Data parameter format

The data contents in frame format can be divided into two types: one is parameter contents command must include. Mark as (M) in below description table. This type parameter **DO NOT** have parameter ID. The other type is optional parameter contents. This type parameter has ID number (PID).

When there are "Variable" data, data format is: parameter length + parameter contents, in them parameter length field is 2bytes data. Length unit is bytes. For fixed length parameter, there is no parameter length field. Basic format is as below table.

(M)Data0	(M)Data1	(M)Data1	...	PID0	Data0	PID1	Data1	Dat	...
	length(U16)						length(U16)	a1	

3.3 Illegal command response

Reader may receive un-executable command or wrong frame, and then reader will initiate a message to upper computer.

Message content：MID=0x00

Parameter name	PID	Data type	Parameter length	Parameter description
Error type	(M)	U8	1	0. Error type number 1. CRC calibration error 2. Wrong MID 3. protocol control word other error 4. current status can not execute the command 5. command list full 6. message parameter incomplete 7. Frame length exceed limitation 8. Other error
Reader status	(M)	U8	1	0. Idle status 1. Execution status 2. Error status
Received protocol control word	(M)	U16	2	Received current illegal command protocol control word
Received message content length	(M)	U16	2	The data length of current illegal command content received

4 Configuration Management

4.1 Introduction

This type command is mainly used for getting and management reader name, edition information, reader communication port parameter, GPIO status.

4.2 Message table

Command ID(MID)	Description	Executable status
0x00	Query reader information	Any status
0x01	Query baseband software version	Any status
0x02	Configure RS232 parameter	Idle status
0x03	Query RS232 parameter	Any status
0x04	Configure reader IP	Idle status
0x05	Query reader IP	Any status
0x06	Query reader MAC	Any status
0x07	Configure server/client mode parameter	Idle status
0x08	Query server/client mode parameter	Any status
0x09	Configure GPO status	Any status
0x0A	Query GPI status	Any status
0x0B	Configure GPI trigger parameter	Idle status
0x0C	Query GPI trigger parameter	Any status
0x0D	Configure wiegand communication parameter	Idle status
0x0E	Query wiegand communication parameter	Any status
0x0F	Re-start reader	Any status
0x10	Configure reader system time	Idle status
0x11	Query reader system time	Any status
0x12	Connection status confirmation	Any status
0x13	Configure reader MAC	Idle status
0x14	Restore reader default configuration	Idle status
0x15	Configure reader RS485 device address	Idle status
0x16	Query reader RS485 device address	Any status

Reader configuration management upload message table

Command ID(MID)	Command description
0x00	Trigger start message
0x01	Trigger stop message
0x12	connection status confirmation

4.2.1 Query reader information

This command is used for Upper computer to get reader software edition and reader name etc basic information.

Upper computer command content: MID = 0x00

Parameter name	PID	Data type	Parameter length	Parameter description
-	-	-	-	-

Reader response content: MID = 0x00

Parameter name	PID	Data type	Parameter length	Parameter description
Application Processor software version	(M)	U32	4	Version V1.0.0 is expressed as 0x00010000.
Reader name	(M)	U8	Variable	Reader name is a character string of "reader + serial number".
Reader power-on time	(M)	U32	4	The seconds from power-on to current time.

Example:

Send(Hex): AA 01 00 00 00 94 03

Receive(Hex):AA 01 00 00 1A 00 01 00 13 00 10 43 4C 37 32 30 36 43 5F 32 30 31 37 30 36 30 32 00 00 03 9D EF AF

AA 01 00 00 00 94 03 //send data analysis

AA //Data frame start identification

0100//Protocol control word, 01 represents the reader configuration management message, and 00 represents the query reader information

0000// data length

9403//checksum

AA 01 00 00 1A 00 01 00 13 00 10 43 4C 37 32 30 36 43 5F 32 30 31 37 30 36 30 32 00 00 03 9D EF AF //receive data analysis

AA //Data frame start identification

0100//Protocol control word, where 01 represents the reader configuration management message, and 00 represents the query reader information

001A //data length

00010013//application processor software version

0010 // The length of the reader name message

434C37323036435F3230313730363032 //reader name CL7206C_20170602

00 00 03 9D//The seconds from power-on to current time

EF AF//checksum

4.2.2 Query baseband software version

Upper computer command content: MID = 0x01

Example:

Send(Hex): AA010100001414

Receive(Hex): AA010100040003001090A9

Parameter name	PID	Data type	Parameter length	Parameter description
-	-	-	-	-

Reader response content： MID=0x01

Parameter name	PID	Data type	Parameter length	Parameter description
Baseband software version	(M)	U32	4	Version V1.0.0 is expressed as 0x00010000

4.2.3 Configure RS232 parameter

This command is used for configuration of reader RS232 communication baud rate.

Upper computer command content： MID = 0x02

Example: Configure baud rate to 115200 bps

Send(Hex): AA01020001022E74

Receive(Hex): AA0102000100AE7B

Parameter name	PID	Data type	Parameter length	Parameter description
Serial port baudrate	(M)	U8	1	0， 9600 bps 1， 19200 bps 2， 115200 bps 3， 230400 bps 4， 460800bps Others: don't support Reader default 115200 bps

Reader response content： MID=0x02

Parameter name	PID	Data type	Parameter length	Parameter description
Configuration result	(M)	U8	1	0. Configuration successful 1. Failed, don't support this baudrate

4.2.4 Query RS232 parameter

This command is used for upper computer to get reader RS232 communication baud rate parameter.

Upper computer command content： MID = 0x03

Example:
Send(Hex): AA01030000943F
Receive(Hex): AA0103000102BA77

Parameter name	PID	Data type	Parameter length	Parameter description
-	-	-	-	-

Reader response content: MID=0x03

Parameter name	PID	Data type	Parameter length	Parameter description
RS232 baudrate	(M)	U8	1	0， 9600bps 1， 19200 bps 2， 115200 bps 3， 230400 bps 4， 460800 bps

4.2.5 Configure device IP

This command is used for configuration of reader IP address parameters.
Upper computer command content: MID = 0x04
Example: Configure device IP as flow: 192.168.1.116 255.255.255.0 192.168.1.1
Send(Hex): AA0104000CC0A80174FFFFFF00C0A801016DB7
Receive(Hex): AA0104000100D67B

Parameter name	PID	Data type	Parameter length	Parameter description
Reader IP	(M)	U32	4	192.168.1.100 equals 0xC0A80164
Reader sub-net mask	(M)	U32	4	255.255.255.0 equals 0xFFFFFF00
Reader default gateway	(M)	U32	4	192.168.1.1 equals 0xC0A80101

Reader response content： MID=0x04

Parameter name	PID	Data type	Parameter length	Parameter description
Configuration result	(M)	U8	1	0. Configure successful 1. Reader IP parameter error

4.2.6 Query device IP

This command is used for upper computer to get reader IP address.

Upper computer command content： MID = 0x05

Example:

Send(Hex): AA010500009447

Receive(Hex): AA0105000CC0A80174FFFFFF00C0A801016CB1

Parameter name	PID	Data type	Parameter length	Parameter description
-	-	-	-	-

Reader response content： MID=0x05

Parameter name	PID	Data type	Parameter length	Parameter description
Reader IP	(M)	U32	4	192.168.1.100 equals 0xC0A80164
Reader subnet mask	(M)	U32	4	255.255.255.0 equals 0xFFFFFF00
Reader default gateway	(M)	U32	4	192.168.1.1 equals 0xC0A80101

4.2.7 Query device MAC

This command is used for upper computer to get reader MAC address.

Upper computer command content： MID = 0x06

Example:

Send(Hex): AA01060000947B

Receive(Hex): AA010600066CECA1FE6BB29DFC

Parameter name	PID	Data type	Parameter length	Parameter description
-	-	-	-	-

Reader response content: MID=0x06

Parameter name	PID	Data type	Parameter length	Parameter description
MAC address	(M)	U8	6	Standard MAC address format

4.2.8 Configure server/client mode parameters

This command is used to configure reader network port server /client mode and parameters.

Upper computer command content： MID = 0x07

Example 1: Configure device to server mode, the server port is 9090

Send(Hex): AA0107000400012382DF8E

Receive(Hex): AA0107000100EA7B

Example 2: Configure device to client mode, the server ip and port is 192.168.1.1:9090.

Send(Hex): AA010700090102C0A8010103238329C0

Receive(Hex): AA0107000100EA7B

Parameter name	PID	Data type	Parameter length	Parameter description
Server/client mode	(M)	U8	1	0. Server mode 1. Client mode
TCP port No. in server mode	0x01	U16	2	Reader TCP port No., is recommended to take value in 1024~65535. Default 9090.
Server IP in client mode	0x02	U32	4	192.168.1.1 equals 0xC0A80101.
Server port No. in client mode	0x03	U16	2	Upper computer TCP server port No., is recommended to take value from 1024~65535， default 9090.

Reader response content: MID=0x07

Parameter name	PID	Data type	Parameter length	Parameter description
Configuration result	(M)	U8	1	0. Configure successfully 1. Server IP parameter error

4.2.9 Query server/client mode parameters

This command is used for query reader network port server/client mode & parameters.

Upper computer command content: MID = 0x08

Example:

Send(Hex): AA0108000014A0

Receive(Hex): AA01080009002382C0A801012382CB33

Parameter name	PID	Data type	Parameter length	Parameter description
-	-	-	-	-

Reader response content: MID=0x08

Parameter name	PID	Data type	Parameter length	Parameter description
Server /client mode	(M)	U8	1	0, Server mode 1, client mode
TCP port number in server mode	(M)	U16	2	Reader TCP server port number, default 9090
Server IP in client mode	(M)	U32	4	192.168.1.1 equals 0xC0A80101
Server port number in client mode	(M)	U16	2	Upper computer TCP service port number, default 9090

4.2.10 Configure GPO status

This command is used for configuration to reader GPIO output port electricity level.

Upper computer command content: MID = 0x09

Example: Configure GPO1 to high level(or relay close)

Send(Hex): AA0109000201017D96

Receive(Hex): AA0109000100B278

Parameter name	PID	Data type	Parameter length	Parameter description
GPO1	0x01	U8	1	0, output low level (or relay open) 1, output high level (or relay close)
GPO2	0x02	U8	1	0, output low level (or relay open) 1, output high level (or relay close)
GPO3	0x03	U8	1	0, output low level (or relay open) 1, output high level (or relay close)
GPO4	0x04	U8	1	0, output low level (or relay open) 1, output high level (or relay close)

Reader response content: MID=0x09

Parameter name	PID	Data type	Parameter length	Parameter description
Configuration result	(M)	U8	1	0, configure successfully 1, reader hardware don't support port parameter

4.2.11 Query GPI status

This command is used for upper computer to get reader GPI electricity level status.

Upper computer command content: MID = 0x0A

Example:

Send(Hex): AA010A0000948B

Receive(Hex): AA010A00020100FD1B

Parameter name	PID	Data type	Parameter length	Parameter description
-	-	-	-	-

Reader response content: MID=0x0A

Parameter name	PID	Data type	Parameter length	Parameter description
GPI1 level	0x01	U8	1	0, low level 1, high level
GPI2 level	0x02	U8	1	0, low level 1, high level
GPI3 level	0x03	U8	1	0, low level 1, high level
GPI4 level	0x04	U8	1	0, low level 1, High level

4.2.12 Configure GPI triggering parameter

This command is used for configuration of reader GPI input port trigger parameter.

Upper computer command content: MID = 0x0B

Example: Configure GPI1 high level trigger reader to inventory EPC, and the stop trigger is GPI low level.

Send(Hex): AA010B000B0002000602100002010101C56F

Receive(Hex): AA010B0001001A7B

Parameter name	PID	Data type	Parameter length	Parameter description
Triggering GPI port number	(M)	U8	1	0， GPI1 1， GP2 2， GP3 3， GP4
Triggering start condition	(M)	U8	1	0，close triggering 1， low level triggering 2，high level triggering 3，Rising edge triggering 4，falling-edge triggering 5，Either side triggering
Triggering combined command	(M)	U8	Variable	Triggering combined command don’t include frame header & CRC16 checksum field
Triggering stop condition	(M)	U8	1	0, not stop 1, low level triggering 2, high level triggering 3, Rising edge triggering 4, falling-edge triggering 5, Either side triggering 6, delay stop When triggering stop condition is reached, reader will execute stop command.
Delay stop time	0x01	U16	2	Take 10ms as unit, 0 means delay time infinite, make sense only when stop condition is delay stop.
GPI level change upload switch when trigger does not stop	0x02	U8	1	0, do not upload 1, upload

Reader response content: MID=0x0B

Parameter name	PID	Data type	Parameter length	Parameter description
Configure result	(M)	U8	1	0, configure successful 1, Reader don't support port parameter. 2, Parameter miss.

When trigger start condition is reached, reader will upload a notification message actively, to notify upper computer trigger operation already starts. Now reader upload message flag is 1.

Trigger start message content: MID=0x00

Parameter name	PID	Data type	Parameter length	Parameter description
Trigger GPI port number	(M)	U8	1	0， GPI1 1， GP2 2， GP3 3， GP4
GPI port level	(M)	U8	1	0， Low level 1， High level
current system second time	(M)	U32	4	UTC second time
Current system microsecond time	(M)	U32	4	UTC micro-second time

When trigger stop condition is reached, reader will upload a notification message actively, to notify upper trigger operation already starts. Now reader upload message flag is 1.

Trigger stop message content: MID=0x01

Parameter name	PID	Data type	Parameter length	Parameter description
Trigger GPI port number	(M)	U8	1	0， GPI1 1， GP2 2， GP3 3， GP4
GPI port level	(M)	U8	1	0， Low level 1， High level
current system second time	(M)	U32	4	UTC second time
Current system microsecond time	(M)	U32	4	UTC micro-second time

4.2.13 Query GPI triggering parameter.

This command is used for Upper computer to get reader designated input port GPI trigger parameter.

Upper computer command content: MID = 0x0C

Example:

Send(Hex): AA010C000100F678

Receive(Hex): AA010C000D02000602100002010101000000EBC2

Parameter name	PID	Data type	Parameter length	Parameter description
GPI port No.	(M)	U8	1	0， GPI1 1， GPI2 2， GPI3 3， GPI4

Upper computer command content: MID = 0x0C

Parameter name	PID	Data type	Parameter length	Parameter description
Trigger start condition	(M)	U8	1	0，Close trigger 1， Low level trigger 2，high level trigger 3，rising edge trigger 4，falling edge trigger 5，random edge trigger
Trigger combined command	(M)	U8	variable length	Triggering combined command don't include frame header & CRC16 calibration field
Trigger stop condition	(M)	U8	1	0，not stop 1， low level triggering 2，high level triggering 3, Rising edge triggering 4, falling-edge triggering 5, random edge triggering 6, delay stop
Delay stop time	(M)	U16	2	Take 10ms as unit, 0 means delay time infinite, make sense only when stop condition is delay stop time.。

4.2.14 Configure wiegand communciation parameter

This command is used to configure reader wiegand communication parameter.

Upper computer command content: MID = 0x0D

Example: Configure wiegand ON, wigand26, wiegand data is the end of EPC.

Send(Hex): AA010D00030100006508

Receive(Hex): AA010D000100627B

Parameter name	PID	Data type	Parameter length	Parameter description
Wiegand communication switch	(M)	U8	1	0， close wiegand communication port 1， Enable wiegand communication port
Wiegand communication format	(M)	U8	1	0， Wiegand 26 1， Wiegand 34 2， Wiegand 66
Wiegand transmission data content	(M)	U8	1	Reader intercept EPC or TID ending data based on wiegand communication format and output through wiegand signal. Wiegand 26 format intercept ending 3 bytes of designated data. Wiegand 34 format intercept ending 4 bytes of designated data. Wiegand 66 format intercept ending 8 bytes of designated data. 0, designate transmission EPC ending data 1, designate transmission TID ending data

Reader response content：MID=0x0D

Parameter name	PID	Data type	Parameter length	Parameter description
Configure result	(M)	U8	1	0， Configure successful 1， Reader hardware don’t support wiegand interface. 2， The wiegand communication format that reader don’t support. 3， The data content reader don’t support.

4.2.15 Query wiegand communication parameter.

This command is used for upper computer to get reader wiegand communication parameters.

Upper command content: MID = 0x0E

Example:

Send(Hex): AA010E000014D8

Receive(Hex): AA010E0003010000ED08

Parameter name	PID	Data type	Parameter length	Parameter description
-	-	-	-	-

Reader response content： MID = 0x0E

Parameter name	PID	Data type	Parameter length	Parameter description
Wiegand communication switch	(M)	U8	1	0, close wiegand communication port 1, Enable wiegand communication port
Wiegand communication format	(M)	U8	1	0, Wiegand 26 1, Wiegand 34 2, Wiegand 66
Wiegand transmission data content	(M)	U8	1	Reader intercept EPC or TID ending data based on wiegand communication format and output through wiegand signal. Wiegand 26 format intercept ending 3 bytes of designated data. Wiegand 34 format intercept ending 4 bytes of designated data. Wiegand 66 format intercept ending 8 bytes of designated data. 0, designate transmission EPC ending data 1, designate transmission TID ending data

4.2.16 Re-start device

This command is used for Upper computer to restart reader through software.

Upper command content: MID = 0x0F

Example:

Send(Hex): AA010F000094CF

Receive(Hex): NA

Parameter name	PID	Data type	Parameter length	Parameter description
-	-	-	-	-

Reader will be re-started when get this message.

4.2.17 Configure reader system time.

This command is used for upper computer to configure reader system time.

Upper computer command content: MID = 0x10

Example: Configure reader system time to 2017-01-10 10:19:38 am (East eight district).

Send(Hex): AA01100008587444BA00000000820

Receive(Hex): AA0110000100467E

Parameter name	PID	Data type	Parameter length	Parameter description
UTC second time	(M)	S32	4	UTC Standard time second format
UTC micro-second time	(M)	S32	4	UTC standard time micro-second format.

Reader response content: MID=0x10

Parameter name	PID	Data type	Parameter length	Parameter description
Configure result	(M)	U8	1	0， Configure successful 1， RTC setting failure

4.2.18 Query system time

This command is used for upper computer to Query reader system time.

Upper computer command content: MID = 0x11

Example:

Send(Hex): AA011100009557

Receive(Hex): AA01110008587445140009158023 20

Parameter name	PID	Data type	Parameter length	Parameter description
-	-	-	-	-

Reader response content： MID=0x11

Parameter name	PID	Data type	Parameter length	Parameter description
UTC second time	(M)	S32	4	UTC Standard time second format
UTC micro-second time	(M)	S32	4	UTC standard time micro-second format.

4.2.19 Connection status confirmation

This message is used for confirmation of the reader connection with upper computer. Both reader and upper computer can send connection status confirmation message. The other party need reply message immediately. If the initiator can not receive confirmation message from the other party, it means the connection is failed. When reader actively sends the connection confirmation message, the reader active upload message flag bit is set to 1.

Initiator message content： MID = 0x12

Example: AA011200040000000382CF

Parameter name	PID	Data type	data length	Parameter description
Message No.	(M)	S32	4	connection confirmation message sequence no.

Responsor reply content: MID=0x12

Parameter name	PID	Data type	Data length	Parameter description
Confirmation message no.	(M)	S32	4	The message sequence no. for connection confirmation, which should be the same as the initiator's message sequence no.

For example:

Heartbeat packet actively sent by the reader: AA 11 12 00 04 00 00 00 BF 07 22

The upper computer sends: AA 01 12 00 04 00 00 00 BF 87 47 // the sequence number of the message is the same as that actively sent by the reader

Received by the upper computer: AA 01 12 00 00 95 6B // the data returned by the reader after executing the connection confirmation message sent by the upper computer

4.2.20 Restore default configuration

This command is used for upper software to restore reader default configuration. This operation will restore all parameters except for system time and MAC address to ex-factory setting, including RFID configurations.

Upper command content: MID = 0x14

Example:

Send(Hex): AA011400045AA5A55A1BAC

Receive(Hex): AA0114000100967D

Parameter name	PID	Data type	Data length	Parameter description
Confirmation code	(M)	U32	4	This parameter is fixed as 0X5AA5A55A。

Reader response content： MID=0x14

Parameter name	PID	Data type	Data length	Parameter description
Configuration result	(M)	U8	1	0 , configure successfully 1， other errors

4.2.21 Configure RS485 parameters.

This command is used for upper computer to set the RS485 communication parameters of the reader, including communication baud rate and 485 address.

Upper computer command content: MID = 0x15

Example: Configure reader's RS485 parameters as follows： RS485 address=1, baud rate=115200.

Send(Hex): AA01150003010102A31F

Receive(Hex): AA0115000100027E

Parameter name	PID	Data type	Data length	Parameter description
Reader RS485 address	(M)	U8	1	0~255， reader RS485 trunk device address
Baud rate	0x01	U8	1	0， 9600bps 1， 19200 bps 2， 115200 bps 3， 230400 bps 4， 460800 bps

Reader response content: MID=0x15

Parameter name	PID	Data type	Data length	Parameter description
Configuration result	(M)	U8	1	0 , configure successfully 1， other errors

4.2.22 Query RS485 parameters

Upper command content: MID = 0x16

Example:

Send(Hex): AA011600001538

Receive(Hex): AA011600020102F8B7

Parameter name	PID	Data type	Data length	Parameter description
-	-	-	-	-

Reader response content: MID=0x16

Parameter name	PID	Data type	Data length	Parameter description
Reader RS485 address	(M)	U8	1	0~255, reader RS485 bus device address
Baud rate	(M)	U8	1	0, 9600bps 1, 19200 bps 2, 115200 bps 3, 230400 bps 4, 460800 bps

4.2.23 Configure Breakpoint resume

Breakpoint resume is that the reader will store the tag data to the native non-volatile memory of reader when the communication link of the reader and upper computer software is disconnected, after the communication link is restored the upper computer software can retrieve the saved data from the reader cache.

In order to determine whether to store the tag data to reader's cache, 8 bytes UTC timestamp and 4 bytes tag packet sequence number are added to the end of the uploaded tag data. When the upper computer receive tag data, it should answer the reader with the tag data' s 4 bytes sequence number, If no answer is received, the reader assumes that the upper computer has not received this tag data and saves the tag data to the native flash.

This command is used to set the function of breakpoint resume, the function of breakpoint resume is disabled by default.

The upper computer command content: MID = 0x17

Example: configure reader breakpoint resume ON

Send(Hex): AA01170001012A78

Receive(Hex): AA0117000100AA7D

Parameter name	PID	Data type	Data length	Parameter description
Breakpoint switch	(M)	U8	1	0. Close the port 1. Enable the port

The reader response： MID=0x17

Parameter name	PID	Data type	Data length	Parameter description
Result	(M)	U8	1	0. Succeed 1. Fail

4.2.24 Query breakpoint resume function

This command is used for the upper computer software query reader breakpoint resume function switch, breakpoint resume function is turned off by default.

The upper computer instruction content： MID = 0x18

Example:

Send(Hex): AA0118000095E3

Receive(Hex): AA0118000101E678

Parameter name	PID	Data type	Data length	Parameter description
-	-	-	-	-

The reader response： MID=0x18

Parameter name	PID	Data type	Data length	Parameter description
Breakpoint switch status	(M)	U8	1	0. Close the port 1. Enable the port

4.2.25 Get cached data

This command is used for the upper computer software to get the cached data , which is same as the normal returned data.

The upper computer instruction content： MID = 0x1B

Example:

Send(Hex): AA011B000095DF

Parameter name	PID	Data type	Data length	Parameter description
Get cached data	(M)	U8	0	

The reader response,

After the reader receives the instruction, then to check whether there exist cache data;

When there exist cached data,it return the cached data, the return cached data format as the data format when reading the tag;

Example:

Receive(Hex): AA011B0001005A7D

When there is no cached data,

Example:

Receive(Hex): AA011B000101DA78

After the data is uploaded, it returns the end mark.

Example:

Receive(Hex): AA011B000102DA72

The reader response： MID = 0x1B

Parameter name	PID	Data type	Data length	Parameter description
Get cached data	(M)	U8	1	0 exist cached data 1 no cached data 2 data uploaded end

4.2.26 Clear cached data

This instruction is used for the upper computer software to clear the cache tag data. After receiving the instruction, the reader will clear the temporary cached data and the stored tag data in flash.

The upper computer instruction content： MID = 0x1C

Send(Hex): AA011C000015B0

Receive(Hex): AA011C000100B67E

Parameter name	PID	Data type	Data length	Parameter description
-	-	-	-	-

The reader response： MID=0x1C

Parameter name	PID	Data type	Data length	Parameter description
Result	(M)	U8	1	0. Succeed 1. Fail

4.2.27 Tag data response

When the upper computer receives the tag data with the tag serial number flag, it should answer the reader with the tag serial number.

The upper computer instruction content: MID = 0x1D

Example:

Receive(Hex): AA011D0004000000010D30

Parameter name	PID	Data type	Data length	Parameter description
Tag serial number	(M)	U8	4	BYTE0~BYTE3: Tag serial number

4.2.28 Buzzer switch

This instruction is used for the host computer software to set the buzzer

The host computer instruction content: MID = 0x1E

Example:

Send(Hex): AA011E0001001E7D

Receive(Hex): AA011E0001001E7D

Parameter name	PID	Data type	Data length	Parameter description
Buzzer switch	-	-	1	0. reader to control 1. upper computer to control

The reader response: MID=0x1E

Parameter name	PID	Data type	Data length	Parameter description
Set buzzer switch	(M)	U8	1	0. Succeed 1. Fail

4.2.29 Buzzer control

This instruction is used for the host computer software to set the buzzer

The host computer instruction content: MID = 0x1F

Example:

Send(Hex): AA011F00020101FB05

Receive(Hex): AA011F0001008A7E

Parameter name	PID	Data type	Data length	Parameter description
Buzzer control	-	-	2	Byte0: 0. Stop 1. The buzzer rings

				Byte1: 0. Ring one time 1.The buzzer kept ringing

The reader response: MID=0x1F

Parameter name	PID	Data type	Data length	Parameter description
Buzzer control	(M)	U8	1	0. Succeed 1. Fail

4.2.30 Get whitelist

This instruction is used to get the white list stored inside the reader

The upper computer instruction content: MID = 0x20

Example:

Send(Hex): AA0120000400000000033E6

Parameter name	PID	Data type	Data length	Parameter description
White list data packet number	(M)	U32	4	White list data packet number

The reader response connect: MID = 0x20

Parameter name	PID	Data type	Data length	Parameter description
White list data packet number	(M)	U32	4	White list data packet number, 0x00000000 as the starting identity,
White list data packet number	(M)	U8	Variable length	White list data packet content

4.2.31 Import whitelist

This command is used to import a whitelist into a reader

The host computer instruction content: MID = 0x21

Parameter name	PID	Data type	Data length	Parameter description
White list data packet number	(M)	U32	4	White list data packet number , 0x00000000 as start
Whitelist data packet content	(M)	U8	Variable length	Whitelist data packet content

The reader response: MID = 0x21

Parameter	PID	Data type	Data	Parameter description

name			length	
White list data packet number	(M)	U32	4	White list data packet number
Result	(M)	U8	1	0. Succeed 1. Fail

4.2.32 Delete the whitelist

This instruction is used to delete the internal white list of the reader.

The upper computer instruction content: MID = 0x22

Example:

Send(Hex): AA0122000096AB

Receive(Hex): AA01220001002E77

Parameter name	PID	Data type	Data length	Parameter description
-	-	-	-	-

The reader response： MID=0x22

Parameter name	PID	Data type	Data length	Parameter description
Result	(M)	U8	1	0. Succeed 1. Fail

4.2.33 Set the whitelist tag action parameter

This instruction is used to set the white list tag action parameter for the upper computer software

The upper computer instruction content: MID = 0x23

Example:

Send(Hex): AA01230003010003352F

Receive(Hex): AA0123000100BA74

Parameter name	PID	Data type	Data length	Parameter description
Relay number	(M)	U8	1	1.1# relay 2. 2# relay 3. 3# relay 4. 4# relay
Relay close time	(M)	U16	1	Unit: Second

				0001—The relay closes for 1 second, then opens

The reader response： MID=0x23

Parameter name	PID	Data type	Data length	Parameter description
Set whitelist action parameter	(M)	U8	1	0. Succeed 1. Fail

4.2.34 Get the whitelist tag action parameter

This instruction is used for the upper computer software to obtain the white list RFID tag action parameter

The upper computer instruction content: MID=0x24

Example:

Send(Hex): AA0124000096D3

Receive(Hex): AA012400030100035D29

Parameter name	PID	Data type	Data length	Parameter description

The reader response： MID=0x24

Parameter name	PID	Data type	Data length	Parameter description
Relay number	(M)	U8	1-	1.1# relay 2. 2# relay 3. 3# relay 4. 4# relay
Relay close time	(M)	U16	1	Unit: Second 0001—The relay closes for 1 second, then opens

4.2.35 Set the tag data output format

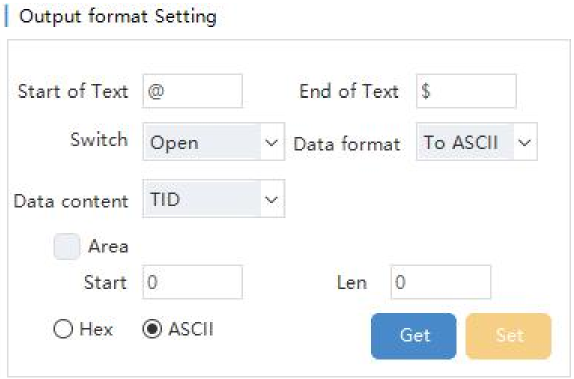
This instruction is used to configure the tag data output format.

The upper computer instruction content: MID = 0x56

Parameter name	PID	Data type	Data length	Parameter description
Switch	(M)	U8	1	0—Close

				1—Open,that is the current connection 2—UDP
Data format	(M)	U8	1	0—RAW 1—To Ascii 2—To dec
Data content	(M)	U8	1	0—epc 1—tid 2—userdata
Start of Text	(M)	U8	Variable length	The maximum frame header length is 4 bytes.
reserved	(M)	U8	1	reserved
reserved	(M)	U8	1	reserved
End of Text	(M)	U8	Variable length	The maximum tail length is 4 bytes.
Area	(0x01)	U8	3	Byte 0 + byte 1: starting byte address. Byte 2: the byte length of the data that the reader needs to read.
Multiple data separator	(0x02)	U8	Variable length	The maximum length of the separator is 4 bytes. Setting the separator will enable optional data transfer

Example:



Output format Setting

Start of Text @

End of Text $

Switch Open

Data format To ASCII

Data content TID

□ Area

Start 0

Len 0

○ Hex ● ASCII

Send(Hex): aa 01 56 00 0b 01 01 01 00 01 40 00 00 00 01 24 60 95

Analysis

aa

01 56

00 0b

01 //the current connection

01 //To Ascii

```
01 //tid
00 01 40 //Start of Text
00 00 //reserved
00 01 24 //End of Text
60 95
```

The reader response： MID=0x56

Parameter name	PID	Data type	Data length	Parameter description
Result	(M)	U8	1	0--Succeed 1--fail

4.2.36 Get the tag data output format

This instruction is used for the upper computer to obtain the tag data output format parameters.

The upper computer instruction content: MID = 0x57

Parameter name	PID	Data type	Data length	Parameter description
-	-	-	-	-

The reader response： MID = 0x57

Parameter name	PID	Data type	Data length	Parameter description
Switch	(M)	U8	1	3—Close 4—Open,that is the current connection 5—UDP
Data format	(M)	U8	1	3—RAW 4—To Ascii 5—To dec
Data content	(M)	U8	1	3—epc 4—tid 5—userdata
Start of Text	(M)	U8	Variable length	The maximum frame header length is 4 bytes.
reserved	(M)	U8	1	reserved
reserved	(M)	U8	1	reserved
End of Text	(M)	U8	Variable length	The maximum tail length is 4 bytes.
Area	(0x01)	U8	3	Byte 0 + byte 1: starting byte

				address. Byte 2: the byte length of the data that the reader needs to read.
Multiple data separator	(0x02)	U8	Variable length	The maximum length of the separator is 4 bytes. Setting the separator will enable optional data transfer

4.2.37 Get the battery power of the reader

This command is used for the upper computer to obtain the power of the reader (for devices with built-in batteries).

The upper computer Command ID: MID = 0x52

Parameter name	PID	Data type	Data length	Parameter description
-	-	-	-	-

The reader response: MID=0x52

Parameter name	PID	Data type	Data length	Parameter description
Battery level	(M)	U8	1	The value of the battery level ranges from 0 to 100

4.2.38 Start Scanning Barcode/QR code

This command is used to turn on the scanning head for bar code scanning (applicable to devices with built-in scanning heads).

The upper computer Command ID: MID = 0x53

Parameter name	PID	Data type	Data length	Parameter description
-	-	-	-	-

The reader response: MID=0x53

Parameter name	PID	Data type	Data length	Parameter description
Operate result	(M)	U8	1	0 indicates that the operation was successful. 1 indicates that the operation failed.

4.2.39 Data Reporting of Scanning Barcode/QR code

This command is used for Bluetooth reader to actively report scanning head data.

The upper computer Command ID:None

The reader response: MID=0x54

Parameter name	PID	Data type	Data length	Parameter description
Operate result	(M)	U8	1	0, Scan failed. 1, Scan successfully
Scanning result	0x01	U8	Variable length	The content of the QR code/Barcode returned by scanning successfully, but there is no such content when scanning fails.

5 RFID configuration & operation

5.1 RFID configuration & operation description

This command set is designed for RFID configuration and operation..

5.2 RFID configuration & operation commands list

Command ID(MID)	Command description	Command executable status
0x00	Query reader RFID ability	Any status
0x01	Configure reader power	Idle status
0x02	Query reader power	Any status
0x03	Configure reader RF frequency band	Idle status
0x04	Query reader RF frequency band	Any status
0x05	Configure reader working frequency	Idle status
0x06	Query reader working frequency	Any status
0x07	Configure reader antenna	Idle status
0x08	Query reader antenna	Any status
0x09	Configure tag upload parameters	Idle status
0x0A	Query tag upload parameters	Any status
0x0B	Configure EPC baseband parameters	Idle status
0x0C	Query EPC baseband parameters	Any status
0x0D	Configure reader auto-idle mode	Idle status
0x0E	Query reader auto-idle mode	Any status

0x0F	Reserved	NA
0x10	Read EPC tag	Idle status
0x11	Write EPC tag	Idle status
0x12	Lock tag	Idle status
0x13	Kill tag	Idle status
0x14~0x3F	Reserved	NA
0x40	read 6B tag	Idle status
0x41	Write 6B tag	Idle status
0x42	Lock 6B tag	Idle status
0x43	Query 6B tag locking	Idle status
0x44~0xFE	Reserved	NA
0xFF	Stop command	Any status

RFID reader actively upload message

Command ID(MID)	Command description
0x00	EPC tag data upload message
0x01	EPC tag reading finish message
0x02	6B tag data upload message
0x03	6B tag reading finish message

5.2.1 Query reader RFID ability

This command is used for upper computer to get reader RF transmission power range, antenna qty, supported frequency table, supported RFID air interface protocol table.

Upper computer command content: MID = 0x00

Example:

Send(Hex):AA02000000A803

Receive(Hex):AA0200000E0024040005000102030400020001527C

Parameter name	PID	Data type	Data length	Parameter description
-	-	-	-	-

Reader response content： MID = 0x00

Parameter name	PID	Data type	Data length	Parameter description
Min. Rf output power	(M)	U8	1	0~36, unit: dBm,1dB step-by-step
Max. Rf output power	(M)	U8	1	0~36, unit: dBm,1dB step-by-step
Antenna qty	(M)	U8	1	antenna port qty the reader support

Frequency list	(M)	U8	Variable	Frequency list as below: 0， 920~925MHz 1， 840~845MHz 2， 840~845MHz&920~925MHz 3， FCC，902~928MHz 4，ETSI，866~868MHz
RFID protocol list	(M)	U8	Variable	Air interface protocol list: 0， ISO18000-6C/EPC C1G2 1， ISO18000-6B 2， China standard GB/T 29768-2013 3， China Military GJB 7383.1-2011

5.2.2 Configure reader RF Port power

This command is used for upper computer to configure reader each antenna port output power.

Upper computer command content: MID = 0x01

Example: Configure Antenna port 1 RF output power to 30 dBm.

Send(Hex): AA02010002011EF614

Receive(Hex): AA020100010092F3

Parameter name	PID	Data type	Data length	Parameter description
Antenna port 1 RF power	0x01	U8	1	0~33, unit: dBm,1dB step-by-step
Antenna port 2 RF power	0x02	U8	1	0~33, unit: dBm,1dB step-by-step
Antenna port 3 RF power	0x03	U8	1	0~33, unit: dBm,1dB step-by-step
Antenna port 4 RF power	0x04	U8	1	0~33, unit: dBm,1dB step-by-step
Antenna port 5 RF power	0x05	U8	1	0~33, unit: dBm,1dB step-by-step
Antenna port 6 RF power	0x06	U8	1	0~33, unit: dBm,1dB step-by-step
Antenna port 7 RF power	0x07	U8	1	0~33, unit: dBm,1dB step-by-step
Antenna port 8 RF power	0x08	U8	1	0~33, unit: dBm,1dB step-by-step
Antenna port 9 RF power	0x09	U8	1	0~33, unit: dBm,1dB step-by-step
Antenna port 10 RF power	0x0A	U8	1	0~33, unit: dBm,1dB step-by-step
Antenna port 11 RF power	0x0B	U8	1	0~33, unit: dBm,1dB step-by-step
Antenna port 12 RF power	0x0C	U8	1	0~33, unit: dBm,1dB step-by-step

…	…	…	…	…
Antenna port 24 RF power	0x18	U8	1	0~33, unit: dBm,1dB step-by-step

Reader response content： MID=0x01

Parameter name	PID	Data type	Data length	Parameter description
Configure result	(M)	U8	1	0， Configuration successful 1， Reader hardware don't support the port parameter 2， reader hardware don't support power parameter 3， save failed.

5.2.3 Query reader power

This command is used for upper computer to get reader each antenna port output power.

Upper computer command content： MID = 0x02

Example:

Send(Hex): AA020200002828

Receive(Hex): AA02020008011E021E031E041E4616

Parameter name	PID	Data type	Data length	Parameter description
-	-	-	-	-

Reader response content： MID = 0x02

Parameter name	PID	Data type	Data length	Parameter description
Antenna port 1 power	0x01	U8	1	0~33, unit: dBm,1dB step-by-step
Antenna port 2 power	0x02	U8	1	0~33, unit: dBm,1dB step-by-step
Antenna port 3 power	0x03	U8	1	0~33, unit: dBm,1dB step-by-step
Antenna port 4 power	0x04	U8	1	0~33, unit: dBm,1dB step-by-step
…	…	…	…	…
Antenna port 24 power	0x18	U8	1	0~33, unit: dBm,1dB step-by-step

5.2.4 Configure reader RF frequency Region

This command is used for configuration of reader working frequency region, this parameter requires compliance with local radio regulations.

Upper computer command content： MID = 0x03

Example: Configure reader RF frequency region to FCC.

Send(Hex): AA02030001033AFA

Receive(Hex): AA02030001003AF0

Parameter name	PID	Data type	Data length	Parameter description
RF frequency range	(M)	U8	1	0, CHN, China band 920~925MHz (16 points, fc=920.625 + 0.25n, n=0~15) 1, CHN2, China band 2, 840~845MHz (16 points, fc=840.625 + 0.25n, n=0~15) 2, CHN3, Chinese hybrid band, 840~845MHz and 920~925MHz (32 points, fc=920.625 + 0.25n, n=0~15 and fc=840.625 + 0.25n, n=0~15) 3, FCC, US band, 902~928MHz (50 points, fc=902.750 + 0.50n, n=0~49) 4, ETSI, Europe band, 866~868MHz (4 points, fc=865.7 + 0.60n, n=0~3) 5, JPN, Japan band, 916.8~920.8 MHz (6 points, fc=916.8 + 1.20n, n=0~3, and 920.6,920.8) 6, TWN, Taiwan band, 922.25~927.75 MHz (23 points, fc=922.25 + 0.25n, n=0~22) 7, IDN, Indonesia band, 923.125 to 925.125 MHz (9 points, fc=923.125 + 0.25n, n=0~8) 8, RUS, Russian band, 866.6~867.4 MHz (5 points, fc=866.600 + 0.2n, n=0~4) 9, GBT, Chinese Standard Test band 920~925MHz (20 points, fc=920.125 + 0.25n, n=0~19) 10, KOR, Korean band 917.1 to 923.3 MHz (32 points, fc=917.1 + 0.2n, n=0~31) 11, BRA, Brazil band, 902 to 907 MHz sub-band 10 points(fc=902.750 + 0.50n, n=0~9), 915~928MHz sub-band 25 points(fc=915.250 + 0.50n, n=0~24) 12, MYS, Malaysia band, 919-923MHz, (8

				points, fc=919.250 + 0.50n, n=0~7) 13, LKA, Sri Lanka band, 920-924MHz, (6 points, fc=920.750 + 0.50n, n=0~5) 14, FCC2, upper half of FCC band, 902-915MHz (25 points, fc=902.750 + 0.50n, n=0~24) 15, FCC3, lower half of FCC band, 915~928MHz (25 points, fc=915.250 + 0.50n, n=0~24) 16, ETSI2, ETSI band 2, 915~917MHz (4 points, fc=915.50 + 0.40n, n=0~3) 17, AUS, Australia band, 920-926Mhz (10 points, fc=920.250 + 0.50n, n=0~9) 18, VIE, Vietnam band, 920-923Mhz (6 points, fc=920.250 + 0.50n, n=0~5) 19, ISR, Israel band 915-916.8 Mhz (1 point, fc=916.250 + 0.50n, n=0~0) 20, ZAF, South African band 915.4 Mhz-919 Mhz (18 points, fc=915.400 + 0.20n, n=0~17) 255: Custom bands
Custom bands	0x01	U8	8	BYTE0-BYTE3: Start frequency(kHz) BYTE4-BYTE5: Step (kHz) BYTE6: points BYTE7: hopping interval(10ms)

Reader response content： MID=0x03

Parameter name	PID	Data type	Data length	Parameter description
Configuration result	(M)	U8	1	0, Configured successfully 1, The channel number is not in the current band. 2, Invalid frequency point number. 3, Other parameter error 4, Save failed

5.2.5 Query Reader RF frequency Region

Upper computer command content： MID = 0x04

Example:

Send(Hex): AA020400002850

Receive(Hex): AA0204000103D6F9

Parameter name	PID	Data type	Data length	Parameter description
-	-	-	-	-

Reader response content: MID = 0x04

Parameter name	PID	Data type	Data length	Parameter description
RF frequency band	(M)	U8	1	0, CHN, China band 920~925MHz (16 points, fc=920.625 + 0.25n, n=0~15) 1, CHN2, China band 2, 840~845MHz (16 points, fc=840.625 + 0.25n, n=0~15) 2, CHN3, Chinese hybrid band, 840~845MHz and 920~925MHz (32 points, fc=920.625 + 0.25n, n=0~15 and fc=840.625 + 0.25n, n=0~15) 3, FCC, US band, 902~928MHz (50 points, fc=902.750 + 0.50n, n=0~49) 4, ETSI, Europe band, 866~868MHz (4 points, fc=865.7 + 0.60n, n=0~3) 5, JPN, Japan band, 916.8~920.8 MHz (6 points, fc=916.8 + 1.20n, n=0~3, and 920.6,920.8) 6, TWN, Taiwan band, 922.25~927.75 MHz (23 points, fc=922.25 + 0.25n, n=0~22) 7, IDN, Indonesia band, 923.125 to 925.125 MHz (9 points, fc=923.125 + 0.25n, n=0~8) 8, RUS, Russian band, 866.6~867.4 MHz (5 points, fc=866.600 + 0.2n, n=0~4) 9, GBT, Chinese Standard Test band 920~925MHz (20 points, fc=920.125 + 0.25n, n=0~19) 10, KOR, Korean band 917.1 to 923.3 MHz (32 points, fc=917.1 + 0.2n, n=0~31) 11, BRA, Brazil band, 902 to 907 MHz sub-band 10 points(fc=902.750 +

				0.50n, n=0~9), 915~928MHz sub-band 25 points(fc=915.250 + 0.50n, n=0~24) 12, MYS, Malaysia band, 919-923MHz, (8 points, fc=919.250 + 0.50n, n=0~7) 13, LKA, Sri Lanka band, 920-924MHz, (6 points, fc=920.750 + 0.50n, n=0~5) 14, FCC2, upper half of FCC band, 902-915MHz (25 points, fc=902.750 + 0.50n, n=0~24) 15, FCC3, lower half of FCC band, 915~928MHz (25 points, fc=915.250 + 0.50n, n=0~24) 16, ETSI2, ETSI band 2, 915~917MHz (4 points, fc=915.50 + 0.40n, n=0~3) 17, AUS, Australia band, 920-926Mhz (10 points, fc=920.250 + 0.50n, n=0~9) 18, VIE, Vietnam band, 920-923Mhz (6 points, fc=920.250 + 0.50n, n=0~5) 19, ISR, Israel band 915-916.8 Mhz (1 point, fc=916.250 + 0.50n, n=0~0) 20, ZAF, South African band 915.4 Mhz-919 Mhz (18 points, fc=915.400 + 0.20n, n=0~17) 255: Custom bands
Custom bands	0x01	U8	8	BYTE0-BYTE3: Start frequency(kHz） BYTE4-BYTE5: Step （kHz） BYTE6: points BYTE7: hopping interval(10ms)

5.2.6 Configure reader working frequency Sequence

This command is used for configuration of reader working frequency sequence.

Upper computer command content: MID = 0x05

Example: Configure reader working frequency sequence 0~49(frequency Region = FCC)

Send(Hex):
AA020500360001003200010203040506070809 0A0B0C0D0E0F101112131415161718191A1B1C1D1E1F202122232425262728292A2B2C2D2E2F3031BF13

Receive(Hex): AA020500010042F0

Parameter name	PID	Data type	Data length	Parameter description
Frequency auto setting	(M)	U8	1	0， Reader can only use frequency point from designated frequency list. 1， Reader auto select frequency point in RF frequency band.
Frequency list	0x01	U8	Variable	used for designating reader working frequency point in non-auto frequency selection mode. Frequency list is signal channel No. list in current working frequency. For example, in 920~925MHz, need to designate 920.625、922.375、924.375MHz three frequency points, then frequency list should be {0,7,15}. Frequency point qty minimum is 1, maximum 50.

Reader response content： MID=0x05

Parameter name	PID	Data type	Data length	Parameter description
Configuration result	(M)	U8	1	0， Configure successful 1， Signal channel not in current frequency band. 2， Invalid frequency point qty. 3， other parameter error 4， save error

5.2.7 Query reader working frequency

Upper computer command content： MID = 0x06

Example:

Send(Hex): AA02060000A87B

Receive(Hex):
AA0206003500003200010203040506070809 0A0B0C0D0E0F101112131415161718191A1B1C1D1E1F202122232425262728292A2B2C2D2E2F30310AE5

Parameter name	PID	Data type	Data length	Parameter description
-	-	-	-	-

Reader response content： MID = 0x06

Parameter name	PID	Data type	Data length	Parameter description
Frequency auto setting	(M)	U8	1	0, Reader can only use frequency point from designated frequency list. 1, Reader auto select frequency point in RF frequency band.
Frequency list	(M)	U8	Variable	Used for designating reader working frequency point in non-auto frequency selection mode. Frequency list is signal channel list in current working frequency. For example, in 920~925MHz, need to designate 920.625、922.375、924.375MHz three frequency points, then frequency list should be {0,7,15}. Frequency point qty minimum is 1, maximum 50.

5.2.8 Configure reader antenna

This instruction is used to configure the antenna used by the reader

Upper computer command content: MID = 0x07

Example: Configure reader 1~4 antennas enable

Send(Hex): AA020700010FEAD1

Receive(Hex): AA0207000100EAF3

Parameter name	PID	Data type	Data length	Parameter description
Enable antenna configuration	(M)	U8	1	Used to specify the antenna used by the reader for tag operation or rf work. Bit0： enable antenna 1 Bit1： enable antenna 2 Bit2： enable antenna 3 Bit3： enable antenna 4 Bit4： enable antenna 5 Bit5： enable antenna 6 Bit6: enable antenna 7 Bit7： enable antenna 8
Enable antenna configuration	0x19	U16	2	Used to specify the antenna used by the reader for tag operation or rf work. Bit0: enable antenna 9

				Bit1: enable antenna 10 Bit2: enable antenna 11 Bit3: enable antenna 12 Bit4: enable antenna 13 Bit5: enable antenna 14 Bit6: enable antenna 15 Bit7: enable antenna 16 Bit8: enable antenna 17 Bit9: enable antenna 18 Bit10: enable antenna 19 Bit11: enable antenna 20 Bit12: enable antenna 21 Bit13: enable antenna 22 Bit14: enable antenna 23 Bit15: enable antenna 24

Reader response content： MID = 0x07

Parameter name	PID	Data type	Data length	Parameter description
Configuration result	(M)	U8	1	0， Configure success 1， Antenna port not existed. 2， save failed

5.2.9 Query reader antenna

Upper computer command content： MID = 0x08

Example:

Send(Hex): AA0208000028A0

Receive(Hex): AA020800010F26D1

Parameter name	PID	Data type	Data length	Parameter description
-	-	-	-	-

Reader response content: MID = 0x08

Parameter name	PID	Data type	Data length	Parameter description
Enable antenna configuration	(M)	U8	1	Used to specify the antenna used by the reader for tag operation or rf work. Bit0： enable antenna 1 Bit1： enable antenna 2 Bit2： enable antenna 3 Bit3： enable antenna 4 Bit4： enable antenna 5

				Bit5： enable antenna 6 Bit6： enable antenna 7 Bit7： enable antenna 8
Enable antenna configuration	0x19	U16	2	Used to specify the antenna used by the reader for tag operation or rf work. Bit0: enable antenna 9 Bit1: enable antenna 10 Bit2: enable antenna 11 Bit3: enable antenna 12 Bit4: enable antenna 13 Bit5: enable antenna 14 Bit6: enable antenna 15 Bit7: enable antenna 16 Bit8: enable antenna 17 Bit9: enable antenna 18 Bit10: enable antenna 19 Bit11: enable antenna 20 Bit12: enable antenna 21 Bit13: enable antenna 22 Bit14: enable antenna 23 Bit15: enable antenna 24

5.2.10 Configure tag upload parameters

This command is used for configuration of tag data uploading rules.

Upper computer command content： MID = 0x09

Example: Configure reader Repeat tag filtering time : 1000 ms; RSSI threshold : 40.

Send(Hex): AA020900050100640228 8FAB

Receive(Hex): AA0209000100B2F0

Parameter name	PID	Data type	Data length	Parameter description
Repeat tag filtering time	0x01	U16	2	Means in an inventory period, in designated repeat filtering time, same tag ID will be uploaded one time only. 0~65535, unit: 10ms
RSSI threshold	0x02	U8	1	Tag RSSI value is lower than threshold, this tag data won't be

				uploaded and will be discard.

Reader response content： MID = 0x09

Parameter name	PID	Data type	Data length	Parameter description
Configuration result	(M)	U8	1	0， Configure success 1， Parameter error 2， Saving failed

5.2.11 Query tag upload parameters

Upper computer command content: MID = 0x0A

Example:

Send(Hex): AA020A0000A88B

Receive(Hex): AA020A0003006428D6DF

Parameter name	PID	Data type	Data length	Parameter description
-	-	-	-	-

Reader response content： MID = 0x0A

Parameter name	PID	Data type	Data length	Parameter description
Repeat tag filtering time	(M)	U16	2	Means in an inventory period, in designated repeat filtering time, same tag ID will be uploaded one time only. 0~65535, unit: 10ms
RSSI threshold	(M)	U8	1	Tag RSSI value is lower than threshold, this tag data won't be uploaded and will be discard.

5.2.12 Configure EPC baseband parameters

Upper computer command content： MID = 0x0B

Example: Configure reader EPC baseband speed:Tari=25us，Miller4，LHF=250KHz; Q=4; Session=1; Inventory Flag=2.

Send(Hex): AA020B000801010204030104 02E2D2

Receive(Hex): AA020B0001001AF3

Parameter name	PID	Data type	Data length	Parameter description
EPC baseband speed	0x01	U8	1	0, Tari=25us, FM0, BLF=40KHz. 1, Tari=25us, Miller4, BLF=250KHz.(dense)

				2, Tari=25us, Miller4, BLF=300KHz. 3, Tari=6.25us, FM0, BLF=400KHz.(Fast) 4, Tari=20us, Miller4, BLF=320KHz.(ETSI dense) 5, Tari=6.25us, Miller2, BLF=320KHz 6, Tari=12.5us, FM0, BLF=80KHz 7, Tari=7.5us, FM0, BLF=640KHz (very fast) 8, Tari=7.5us, Miller2, BLF=640KHz (high speed). 9, Tari=7.5us, Miller4, BLF=640KHz. 10, Tari=15us, Miller2, BLF=320KHz. 11, Tari=20us, Miller2, BLF=320KHz. 12, Tari=20us, Miller4, BLF=250KHz (FCC dense). 13, Tari=20us, Miller8, BLF=160KHz (extremely stable). 14 to 254, Reserved. 255, The reader is set automatically
Default Q value	0x02	U8	1	0~15, the start Q value reader use.
Session	0x03	U8	1	0， Session0 1， Session1 2， Session2 3， Session3
Inventory Flag parameter	0x04	U8	1	0， Use Flag A inventory only 1， Use Flag B inventory only 2， Use Flag A & Flag B double-sided inventory by turns

Reader response content: MID = 0x0B

Parameter name	PID	Data type	Data length	Parameter description
Configuration result	(M)	U8	1	0， Configure successfully 1， Baseband speed reader don’t support. 2， Q value parameter error. 3， Session parameter error. 4， Inventory parameter error. 5， Other parameter error. 6， Save failed.

5.2.13 Query EPC baseband parameter.

Upper computer command content: MID = 0x0C

Example:

Send(Hex): AA020C0000A8F3

Receive(Hex): AA020C0004FF0401022758

Parameter name	PID	Data type	Data length	Parameter description
-	-	-	-	-

Reader response content： MID = 0x0C

Parameter name	PID	Data type	Data length	Parameter description
EPC baseband speed	(M)	U8	1	0, Tari=25us, FM0, BLF=40KHz. 1, Tari=25us, Miller4, BLF=250KHz.(dense) 2, Tari=25us, Miller4, BLF=300KHz. 3, Tari=6.25us, FM0, BLF=400KHz.(Fast) 4, Tari=20us, Miller4, BLF=320KHz.(ETSI dense) 5, Tari=6.25us, Miller2, BLF=320KHz 6, Tari=12.5us, FM0, BLF=80KHz 7, Tari=7.5us, FM0, BLF=640KHz (very fast) 8, Tari=7.5us, Miller2, BLF=640KHz (high speed). 9, Tari=7.5us, Miller4, BLF=640KHz. 10, Tari=15us, Miller2, BLF=320KHz. 11, Tari=20us, Miller2, BLF=320KHz. 12, Tari=20us, Miller4, BLF=250KHz (FCC dense). 13, Tari=20us, Miller8, BLF=160KHz (extremely stable). 14 to 254, Reserved. 255, The reader is set automatically
Default Q value	(M)	U8	1	0~15， reader Q value
Session	(M)	U8	1	0， Session0 1， Session1 2， Session2 3， Session3
Inventory mark parameter	(M)	U8	1	0,Use Flag A inventory only 1,Use Flag B inventory only 2,Use Flag A & Flag B double-sided

				inventory by turns

5.2.14 Configure EPC baseband extended parameters

This command is used to configure the baseband parameters used by the reader.

Upper computer command content: MID = 0xE0

Parameter name	PID	Data type	Data length	Parameter description
TAG extended parameters	0x1	U32	4	bit3-bit0: rfu bit4: IMJ tag focus bit5: IMJ fast id bit15-bit6: rfu bit16: NXP fast ID bit31-bit17: rfu
DQN extended parameters	0x2	U8	4	Byte 1: maxQ Byte 2: minQ Byte 3: tmult Byte 4: bit 0: Dynamic Start Q Enable bit 1: Forced loop algorithm
AST extended parameters	0x03	U8	4	Byte 1:Antenna switch mode 0:Switch immediately without tags 1:running out of residence time Byte 2：Number of retries (suitable for Switch immediately without tags) Byte 3-4: Maximum antenna residence time (x10ms)
AST2 extended parameters	0x04	U8	4	Byte 1:Antenna switching wait time (x10ms) Byte 2: Antenna switching step value Byte 3:Antenna port protection threshold (dBm). If the value is set to 0, no protection is enabled. Byte 4: rfu
LBT extended parameters	0x05	U8	4	Byte 1: LBT working mode 0: Disable 1: LBT listening only 2: Read tag after listening 3: Read tag after meeting RSSI

				threshold value Byte 2: RSSI threshold value Byte 3-4: rfu

Reader response content: MID = 0xE0

Parameter name	PID	Data type	Data length	Parameter description
result	(M)	U8	1	0, Configure successfully 1. Parameters that do not support. 2. IMJ parameter error. 3. DNQ parameter error. 4. AST parameter error. 5, AST2 parameter error. 6, preservation failure 7, LBT parameter error

5.2.15 Query EPC baseband expansion parameters

This command is used to query the baseband parameters currently used by the reader.

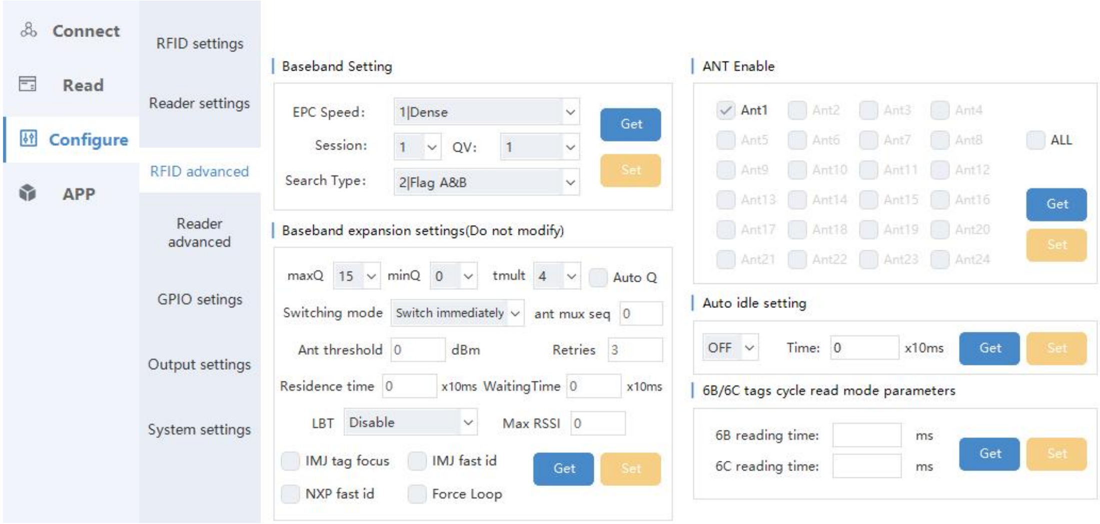
Upper computer command content: MID = 0xE1

Parameter name	PID	Data type	Data length	Parameter description
-	-	-	-	-

Reader response content: MID = 0xE1

Parameter name	PID	Data type	Data length	Parameter description
TAG extended parameters	0x1	U32	4	bit3-bit0: rfu bit4: IMJ tag focus bit5: IMJ fast id bit15-bit6: rfu bit16: NXP fast ID bit31-bit17: rfu
DQN extended parameters	0x2	U8	4	Byte 1: maxQ Byte 2: minQ Byte 3: tmult Byte 4: bit 0: Dynamic Start Q Enable bit 1: Forced loop algorithm
AST extended parameters	0x03	U8	4	Byte 1:Antenna switch mode 0:Switch immediately without tags 1:running out of residence time

				Byte 2：Number of retries (suitable for Switch immediately without tags) Byte 3-4: Maximum antenna residence time (x10ms)
AST2 extended parameters	0x04	U8	4	Byte 1:Antenna switching wait time (x10ms) Byte 2: Antenna switching step value Byte 3:Antenna port protection threshold (dBm). If the value is set to 0, no protection is enabled. Byte 4: rfu
LBT extended parameters	0x05	U8	4	Byte 1: LBT working mode 0: Disable 1: LBT listening only 2: Read tag after listening 3: Read tag after meeting RSSI threshold value Byte 2: RSSI threshold value Byte 3-4: rfu



Baseband Setting

EPC Speed: 1|Dense
Session: 1 QV: 1
Search Type: 2|Flag A&B

Baseband expansion settings(Do not modify)

maxQ 15 minQ 0 tmult 4 □ Auto Q
Switching mode Switch immediately ant mux seq 0
Ant threshold 0 dBm Retries 3
Residence time 0 x10ms WaitingTime 0 x10ms
LBT Disable Max RSSI 0
□ IMJ tag focus □ IMJ fast id
□ NXP fast id □ Force Loop

ANT Enable

☑ Ant1 □ Ant2 □ Ant3 □ Ant4
□ Ant5 □ Ant6 □ Ant7 □ Ant8 □ ALL
□ Ant9 □ Ant10 □ Ant11 □ Ant12
□ Ant13 □ Ant14 □ Ant15 □ Ant16
□ Ant17 □ Ant18 □ Ant19 □ Ant20
□ Ant21 □ Ant22 □ Ant23 □ Ant24

Auto idle setting

OFF Time: 0 x10ms

6B/6C tags cycle read mode parameters

6B reading time: ms
6C reading time: ms

5.2.16 Configure reader auto-idle mode.

This command is used for upper computer to configure reader tag reading mode.

Upper computer command content: MID = 0x0D

Example: Configure reader auto-idle mode ON, idle time=100ms.
Send(Hex): AA020D00040101000A3814
Receive(Hex): AA020D00010062F3

Parameter name	PID	Data type	Data length	Parameter description
Auto-idle mode enable	(M)	U8	1	Automatic idle mode means during reading tags continuously, all antennas didn't get tags for three polls, reader will enter idle mode for a time for saving power. After idle time is finished, reader enter tag reading status automatically. 0， Close auto-idle mode 1， Enable auto-idle mode
Auto-idle time	0x01	U16	2	used for designating staying time when reader enter auto-idle mode. 0~65535, time unit:10ms

Reader response content: MID = 0x0D

Parameter name	PID	Data type	Data length	Parameter description
Configuration result	(M)	U8	1	0， Configure successfully 1， Mode parameter error 2， Other parameter error. 3， Saving failed.

5.2.17 Query reader auto-idle mode.

Upper computer command content： MID = 0x0E
Example:
Send(Hex): AA020E000028D8
Receive(Hex): AA020E000301000AEE04

Parameter name	PID	Data type	Data length	Parameter description
-	-	-	-	-

Reader response content： MID = 0x0E

Parameter name	PID	Data type	Data length	Parameter description
Auto-idle mode Enable	(M)	U8	1	0， Close auto-idle mode 1， Enabling auto-idle mode
Auto-idle time	(M)	U16	2	used for designating staying time when reader enter auto-idle mode. 0~65535,

				time unit: 10ms.

5.2.18 Read EPC tag

This command is used for configure tag reading parameter and start tag reading operation. All tag reading operation will start from getting tag EPC code.

Upper computer command content： MID = 0x10

Example: read EPC from antenna1.

Send(Hex): AA021000020100F1A8

Receive(Hex): AA021000010046F6

Parameter name	PID	Data type	Data length	Parameter description
Antenna port No.	(M)	U8	1	Bit0: use antenna 1 Bit1: use antenna 2 Bit2: use antenna 3 Bit3: use antenna 4 Bit4: use antenna 5 Bit5: use antenna 6 Bit6: use antenna 7 Bit7: use antenna 8 Can designate one or multiple antenna at the same time.
Inventory/Single read type	(M)	U8	1	0， Single read mode:reader make one round tag reading on each enabled antenna, and then enter idle mode. 1， Inventory read mode: reader keep tag reading till it gets stop command.
Select read parameter	0x01	U8	Variable	Byte 0: data area to be matched. 1,EPC area. 2,TID area. 3,user data area. Byte 1+ byte 2: matched data start address，byte 1 is start address high 8bits, byte 2 is start address low 8bits. Byte 3: data bit length to be matched. Byte 4~ Byte N: data content to be matched.
TID read parameter	0x02	U8	2	Byte 0: TID read mode configuration. 0,TID read length self-adapter, but max. length not exceed byte 1 defined length.

				1,Read TID according to byte 1 defined length. Byte 1: TID data word length to be read (word,16bits,below same)
User data area read parameter	0x03	U8	3	Byte 0+ byte 1: start word address, byte 0 is start address high 8bits, byte 1 is start address low 8bits. Byte 2: User data word length to be read.
Reserved area read parameter	0x04	U8	3	Byte 0+ byte 1: start word address, byte 0 is start address high 8bits, byte 1 is start address low 8bits. Byte 2: reserved area word length to be read.
Access password	0x05	U32	4	access password for tag authentication
MONZA QT PEEK data read	0x06	U8	1	This value is fixed to 1 for QT PEEK reads for MONZA QT tags.
Read RFMICRON chip temperature sensing data	0x07	U8	1	This value is fixed to 1 for obtaining the temperature of the RFMICRON Magnus-S3 tag.
Get EM chip Sensor data	0x08	U8	1	This value is fixed to 1, which is used to get Sensor data for the EM tag 。
EPC area data read	0x09	U8	3	Byte 0 + byte 1: start word address, byte 0 is the starting address high 8 bits, byte 1 is the starting address low 8 bits. Byte 2: The word length of the EPC data that the reader needs to read.
Antenna port extension	0x0A	U16	2	Bit0: use antenna 9 Bit1: use antenna 10 Bit2: use antenna 11 Bit3: use antenna 12 Bit4: use antenna 13 Bit5: use antenna 14 Bit6: use antenna 15 Bit7: use antenna 16 Bit8: use antenna 17 Bit9: use antenna 18 Bit10: use antenna 19 Bit11: use antenna 20 Bit12: use antenna 21

				Bit13: use antenna 22 Bit14: use antenna 23 Bit15: use antenna 24 Can designate one or multiple antenna at the same time.
EPC G2V2 Authenticate	0x0B	U8	10	Byte 0: TAM AuthMethod Byte 1: TAM CustomData Byte 2: TAM KeyID Byte 3: Profile. 0,EPC area; 1, TID area; 2, user area Byte 4: Offset Byte 5: Block Count Byte 6: ProtMode Byte 7: Reserved Byte 8: Reserved Byte 9: Reserved

Reader response content：MID = 0x10

Parameter name	PID	Data type	Data length	Parameter description
Read operation configuration result	(M)	U8	1	0，Configure successfully. 1，Antenna port parameter error. 2，Select read parameter error. 3，TID read parameter error. 4，User data area read parameter error. 5，Reserved area read parameter error. 6，Other parameter error.

When reader received correct tag reading command, it will enter tag reading status. When reader get tag data successfully, it will upload tag data, now reader actively upload data bit marked as 1.

EPC tag data upload content：MID=0x00

Example:

Receive (Hex): AA12000013000C300833B2DDD9014000000000300001015CF9E3

Parameter name	PID	Data type	Data length	Parameter description
Tag EPC value	(M)	U16	Variable	Tag EPC data
Tag PC	(M)	U16	2	tag PC value
Antenna ID	(M)	U8	1	Means the No. of antenna that read tag. 1, Antenna 1 2, Antenna 2

				3, Antenna 3 4, Antenna 4
RSSI	0x01	U8	1	Tag RSSI value
tag data read result	0x02	U8	1	If tag reading command includes read TID, user area or reserved area data parameter 0， Read successful 1， Tag no response 2， CRC error 3， Data area is locked. 4， Data area overflow. 5， Access password error. 6， Other tag error. 7， Other reader error.
Tag TID data	0x03	U16	Variable	tag TID data
Tag user area data	0x04	U16	Variable	tag user area data
tag reserved area data	0x05	U16	Variable	tag reserved area data
Sub antenna number	0x06	U8	1	Add antenna hub, there are sub antenna number 1-16
Tag reading time UTC	0x07	U32	8	BYTE0~BYTE3:UTC time second BYTE4~BYTE7:UTC Time microsecond
Tag response package sequence number	0x08	U32	4	When the field is not empty, the upper computer should reply the reader with this sequence number as a confirmation response. BYTE0 ~ BYTE3: tag package sequence number
Current frequency	0x09	U32	4	Current frequency：KHZ
Current tag phase	0x0A	U8	1	Current tag reading phase value, in the range of 0 to 128, tag phase calculation method: (phase value / 128) * 2π
EM Sensor Data	0x0B	U8	8	EM tag Sensor Data
Tag EPC data	0x0C	U16	Variable	Tag EPC data
EPC G2V2 Authenticate Challenge data	0x0D	U8	10	The original data stream used to verify the validity of the tag
EPC G2V2 Authenticate tag cypher data	0x0E	U8	Variable	Tag cypher data, length is 128*（1+N）bits

Total number of tag reads	0x10	U32	4	After the repeated tag filtering function is turned on, count the reading times, and clear the counting times when the tag leaves.
RSSI_dBm	0x11	S8	1	Tag RSSI value received (dBm)

When read operation finish, reader will upload an notification. Now reader actively upload message bit marked as 1.

EPC tag reading finish notification content: MID=0x01

Example:

Receive (Hex): AA12010001001570

Parameter name	PID	Data type	Data length	Parameter description
Tag read finish reason	(M)	U8	1	0, Single operation finished 1, received stop command. 2, hardware abnormal caused tag reading interrupted.

Reading EPC for an example

```
OUT    aa 02 ff 00 00 a4 0f   // Send Stop command to reader
IN     aa 02 ff 00 01 00 0a d8  //Reader return response: Stop successful

OUT    aa 02 10 00 02 01 01 71 ad    //configure antenna 1 reading continuously
IN     aa 02 10 00 01 00 46 f6    //Configure successfully.

IN     aa 12 00 00 0b 00 04 20 18 04 09 14 00 01 01 00 a1 2c
IN     aa 12 00 00 11 00 0a aa aa bb bb cc cc 20 18 04 11 28 00 01 01 00 73 7a
```

data analysis:

aa //Data frame start identification

12 00 //Protocol control word, 1 represents the reader's active upload data and 2 represents the RFID operation message, 00 represents MID

00 11 //The length of the following data, does not include checksum

00 0a //EPC data length

aa aa bb bb cc cc 20 18 04 11 //EPC value

28 00 //PC value

01 //antenna number which detected tag

01 00 //0x01 represents RSSI PID No. , 0x00 represents RSSI value

73 7a // checksum

```
OUT    aa 02 ff 00   00 a4 0f   // Stop command
```

IN aa 02 ff 00 01 00 0a d8 //Stop successful

IN aa 12 01 00 01 00 15 70 //End of card reading notification

5.2.19 Write EPC tag

This command is used for reader to make single time write operation to tag.

Upper computer command content: MID = 0x11

Example: Write the tag's user data, Antenna port =1, Data area= user data area, Word start address=0, Data content=0x111122223333444455556666, match the tag's TID value E2801105200054964CDE0898.

Send(Hex):

AA021100250103000000C111122223333444455556666010010020000060E2801105200054964CDE08987CC1

Receive(Hex): AA0211000100D2F5

Parameter name	PID	Data type	Data length	Parameter description
Antenna port	(M)	U8	1	Bit0：Use antenna 1 Bit1：Use antenna 2 Bit2：Use antenna 3 Bit3：Use antenna 4 Bit4：Use antenna 5 Bit5：Use antenna 6 Bit6：Use antenna 7 Bit7：Use antenna 8 Can designate one or multiple antennas.
Data area	(M)	U8	1	tag data to be written 0，Reserved area 1，EPC area 2，TID area 3，user data area
word start address	(M)	U16	2	Word start address of the tag data area to be written.
Data content	(M)	U16	Variable	Data content to be written.
Select written parameter	0x01	U8	Variable	Byte 0: data area to be matched. 1,EPC area；2,TID area；3,user data area.

				Byte 1+byte 2: matched data start address. Byte 1 means start address high 8bits, byte 2 means start address low 8bits. Byte 3: data bit length to be matched. Byte 4~Byte N: Data content to be matched.
Tag access password	0x02	U32	4	access password for tag authentication
Block write parameter	0x03	U8	1	Word length of single time block write data content, 0 means don't adopt block write.

Reader response content: MID = 0x11

Parameter name	PID	Data type	Data length	Parameter description
Write result	(M)	U8	1	0, write successful 1, antenna port parameter error 2, select parameter error 3, write parameter error. 4, CRC calibration error. 5, Power insufficient. 6, data area overflow. 7, Data area is locked 8, access password error. 9, other tag error 10, tag lost 11, reader transmit command error.
Write failure word address	0x01	U16	2	If write failure occurred. reader will upload write failure tag address.

5.2.20 Lock tag

This command is used for reader to make single time tag lock or unlock operation.

Upper computer command content: MID = 0x12

Example: Lock the tag's EPC bank, Antenna port = 1, match the tag's TID code E2801105200054964CDE0898.

Send(Hex):

AA0212001601020101001002000060E2801105200054964CDE089892C7

Receive(Hex): AA0212000100EEF5

Parameter name	PID	Data type	Data length	Parameter description
Antenna port No.	(M)	U8	1	Bit0：Use antenna 1 Bit1：Use antenna 2 Bit2：Use antenna 3 Bit3：Use antenna 4 Bit4：Use antenna 5 Bit5：Use antenna 6 Bit6：Use antenna 7 Bit7：Use antenna 8 Can designate one or multiple antennas.
Lock operation area	(M)	U8	1	Tag area to be locked: 0，Kill password area. 1，access password area. 2，EPC area 3，TID area 4，user data area.
Lock operation type	(M)	U8	1	Lock operation type 0，unlock. 1，lock 2，unlock permanently 3，lock permanently
Select lock parameter	0x01	U8	Variable	Byte 0：data area to be matched， 1，EPC area；2，TID area；3，user data area. Byte 1+ byte 2：matched data start bit address. Byte 1 is start address high 8 bit; byte 2 is start address low 8bit. Byte 3：data bit length to be matched. Byte 4~byte N：Data content to be matched.
Tag access password	0x02	U32	4	access password for tag authentication

Reader response content：MID = 0x12

Parameter name	PID	Data type	Data length	Parameter description
Lock operation result	(M)	U8	1	0，lock successfully 1，antenna port error 2，select parameter error 3，lock operation parameter error 4，CRC calibration error

				5， Power insufficiency 6， Data area overflow 7， Data area locked 8， Access password error 9， other tag error 10， tag lost 11， reader send commands error

5.2.21 Kill tag

This command is used for reader to make Kill operation to tag. The tag which is Killed will be silence permanently. This operation is irreversible. This operation is single time operation.

Upper computer command content: MID = 0x13

Example: Kill the tag's EPC bank, Antenna port = 1, match the tag's TID value E2801105200054964CDE0898.

Send(Hex):
AA02130018010000000101001002000060E2801105200054964CDE0898AC23

Receive(Hex): AA02130001007AF6

Parameter name	PID	Data type	Data length	Parameter description
Antenna port	(M)	U8	1	Bit0： Use antenna 1 Bit1： Use antenna 2 Bit2： Use antenna 3 Bit3： Use antenna 4 Bit4： Use antenna 5 Bit5： Use antenna 6 Bit6： Use antenna 7 Bit7： Use antenna 8 Can designate one or multiple antennas.
Kill password	(M)	U32	4	Tag Kill password.
Select Kill parameter	0x01	U8	Variable	Byte 0： data area to be matched, 1， EPC area； 2， TID area； 3， user data area. Byte 1+Byte 2 ： matched data start bit addres, byte 1 is start bit address high 8bits, Byte 2 is start bit address low 8bits. Byte 3： data bit length to be matched. Byte 4~Byte N ： data contents to be

				matched.

Reader response content: MID = 0x13

Parameter name	PID	Data type	Data length	Parameter description
Kill operation result	(M)	U8	1	0， Kill operation successful 1， antenna port parameter error. 2， select parameter error. 3， CRC calibration error. 4， power insufficiency. 5， Kill password error. 6， other tag error. 7， tag lost. 8， reader send command error.

5.2.22 G2V2 Untraceable operation

This instruction is used by the reader to perform Untraceable operation on a tag that supports the EPC C2G2 V2.0 optional instruction Untraceable, which is defined as a single operation.

Upper computer command content:MID = 0x20

Parameter name	PID	Data type	Data length	Parameter description
Antenna port No.	(M)	U8	1	Bit0: use antenna 1 Bit1: use antenna 2 Bit2: use antenna 3 Bit3: use antenna 4 Bit4: use antenna 5 Bit5: use antenna 6 Bit6: use antenna 7 Bit7: use antenna 8 Can designate one or multiple antenna at the same time.
Untraceable parameters	(M)	U8	5	Byte 0: U parameter. 0, Untraceable flag bit 0; 1, Untraceable flag bit 1 Byte 1: EPC hide parameters. Bit5: EPC show/hide flag bit. 0,show; 1, a Tag untraceably hides EPC memory above that set by its EPC length field. Bit4~0:

				assign new EPC length. Byte 2: TID hide parameter. 0, show; 1, the Tag untraceably hides TID memory above 20h; 2, the Tag untraceably hides all TID memory. Byte 3: USER hide parameter. 0,show; 1, hide Byte 4: tag response range. 0,normal; 1, toggle temporarily; 2, reduced
Select read parameter	0x01	U8	Variable	Byte 0: data area to be matched. 1,EPC area. 2,TID area. 3,user data area. Byte 1+ byte 2: matched data start address，byte 1 is start address high 8bits,byte 2 is start address low 8bits. Byte 3: data bit length to be matched. Byte 4~ Byte N: data content to be matched.
Access password	0x02	U32	4	access password for tag authentication

Note: A Tag only executes an Untraceable command in the secured state.

Note: The Untraceable command can only be tested on Tags with a non-zero Access password.

Note: If parts of the memory are “untraceable” they shall act as non-existing. If accessed the Tag will return the error condition "memory overrun"

Note: The UCODE DNA Tag does not support the U bit and, according to Gen2V2, ignores the provided U value and continues to process the remainder of the Untraceable command.

Example:

Send：AA0220000B0100060001000211111111D386

Data analyze:

AA // Data frame start identification

02 20 // Protocol control word，02 represents the RFID operation message, 20 represents MID

00 0B //data length

01 00 06 00 01 00//Untraceable parameters

02 11 11 11 11 //0x02 access password PID, 11111111 is access password

D3 86 //checksum

Receive：AA022000010086FC // execute successfully

5.2.23 Read 6B tag

Upper computer command content: MID = 0x40

Example: read 6B tag's TID using antenna 1.

Send(Hex): AA02400003010000BE73

Receive(Hex): AA024000010086ED

Parameter name	PID	Data type	Data length	Parameter description
antenna port	(M)	U8	1	Bit0： Use antenna 1 Bit1： Use antenna 2 Bit2： Use antenna 3 Bit3： Use antenna 4 Bit4： Use antenna 5 Bit5： Use antenna 6 Bit6： Use antenna 7 Bit7： Use antenna 8 Can designate one or multiple antennas.
continuous/single time reading	(M)	U8	1	0， Single reading mode， Reader made one roll tag reading operation on each enabled antenna. Then finished operation & enter idle status. 1， continuous reading mode: reader keep reading tag till it gets stop command.
Read contents	(M)	U8	1	0， read 6B TID only 1， read 6B TID+ user data 2， read user data only
user data read parameter	0x01	U8	2	Byte 0： user data start byte address Byte 1： user data byte length
TID to be matched	0x02	U8	8	The TID code of 6B tag to be matched.

Reader response content： MID = 0x40

Parameter name	PID	Data type	Data length	Parameter description
Read operation configuration result	(M)	U8	1	0， configure successful 1， Antenna port parameter error 2， Read content parameter error 3， User data area read parameter

				error 4， Other error

When reader get correct tag reading command, it enter tag reading status. Will upload tag data contents once get tag data successfully. Now reader upload message mark bit is 1.

6B tag data upload content： MID=0x20

Receive(Hex): AA1220000BE004000050D2C10701016CC593

Parameter name	PID	Data type	Data length	Parameter description
6B tag TID	(M)	U8	8	6B tag TID code that reader get.
Antenna ID	(M)	U8	1	Means the ID number of the antenna that gets tag data. 1, Antenna 1 2, Antenna 2 3, Antenna 3 4, Antenna 4
RSSI	0x01	U8	1	Tag RSSI value
User read result	0x02	U8	1	When tag reading command includes reading TID, user data area parameters: 0， Read successfully 1， Tag no response 2， CRC error 3， Other reader error.
Tag user data	0x03	U8	Variable	Read user data

When read operation is finished, reader will upload a notification. Now the reader upload message mark bit is 1.

6B card reading finished notification： MID=0x21

Receive(Hex): AA1221000100957C

Parameter name	PID	Data type	Data length	Parameter description
Read reading stop reason	(M)	U8	1	0， Single operation completed 1， get stop command 2， hardware abnormal cause reading break

5.2.24 Write 6B tag

This command is used for reader to make single time write operation to EPC tag.

Upper computer command content: MID = 0x41

Example: write 6B tag's user data from byte 8 using antenna 1, the written data is 0x11112222, the matching TID is 0xE004000050D2C107.

Send(Hex): AA0241001001E004000050D2C10708000411112222FF80

Receive(Hex): AA024100010012EE

Parameter name	PID	Data type	Data length	Parameter description
Antenna port	(M)	U8	1	Bit0：Use antenna 1 Bit1：Use antenna 2 Bit2：Use antenna 3 Bit3：Use antenna 4 Bit4：Use antenna 5 Bit5：Use antenna 6 Bit6：Use antenna 7 Bit7：Use antenna 8 Can designate one or multiple antennas at the same time.
TID of tag to be write	(M)	U8	8	TID of 6B tag to be written.
Start address	(M)	U8	1	Word byte start address of data area of the tag to be written
Data content	(M)	U8	Variable	Data content to be written

Reader response content：MID = 0x41

Parameter name	PID	Data type	Data length	Parameter description
Write result	(M)	U8	1	0，write success 1，antenna port parameter error 2，write parameter error 3，other error
Write failure byte address	0x01	U8	1	When write failed, reader will upload write failure tag byte address.

5.2.25 6B tag lock

This command is used for reader to lock 6B tag data. This operation is irreversible. This command defines single time lock operation.

Upper computer command content：MID = 0x42

Example: Lock 6B tag's user data byte 8 using antenna 1, the matching TID is 0xE004000050D2C107.

Send(Hex): AA0241001001E004000050D2C10708000411112222FF80

Receive(Hex): AA024100010012EE

Parameter name	PID	Data type	Data length	Parameter description

Antenna port	(M)	U8	1	Bit0： Use antenna 1 Bit1： Use antenna 2 Bit2： Use antenna 3 Bit3： Use antenna 4 Bit4： Use antenna 5 Bit5： Use antenna 6 Bit6： Use antenna 7 Bit7： Use antenna 8 Can designate one or multiple antennas
TID of the tag to be locked	(M)	U8	8	TID of 6B tag to be locked
Lock address	(M)	U8	1	The byte address of data to be locked.

Reader response content: MID = 0x42

Parameter name	PID	Data type	Data length	Parameter description
Lock content	(M)	U8	1	0， Lock success 1， Other error
Lock failure byte address	0x01	U8	1	When lock failed, reader will upload lock failure tag byte address.

5.2.26 6B tag lock query

This command is used for single time query of 6B tag lock status.

Upper computer command content: MID = 0x43

Example: Query Lock state of 6B tag's user data byte 8 using antenna 1, the matching TID is 0xE004000050D2C107.

Send(Hex): AA0243000A01E004000050D2C10708CAC0

Receive(Hex): AA02430003000101B062

Parameter name	PID	Data type	Data length	Parameter description
Antenna port	(M)	U8	1	Bit0： Use antenna 1 Bit1： Use antenna 2 Bit2： Use antenna 3 Bit3： Use antenna 4 Bit4： Use antenna 5 Bit5： Use antenna 6 Bit6： Use antenna 7 Bit7： Use antenna 8 Can designate one or multiple antennas
TID of tag to be locked	(M)	U8	8	TID code of 6B tag to be locked

Data address	(M)	U8	1	The byte address of the data to be queried.

Reader response content： MID = 0x43

Parameter name	PID	Data type	Data length	Parameter description
Query result	(M)	U8	1	0， Query succeed 1， other error
Data lock status	0x01	U8	1	0， unlocked 1， locked

5.2.27 Stop command

This command is used for stopping all RFID operations, then reader enter idle status.

Upper computer command content: MID = 0xFF

Example:

Send(Hex): AA02FF0000A40F

Receive(Hex): AA02FF0001000AD8

Parameter name	PID	Data type	Data length	Parameter description
-	-	-	-	-

Reader response content: MID = 0xFF

Parameter name	PID	Data type	Data length	Parameter description
Query result	(M)	U8	1	0: Stop successful 1: System error.

5.2.28 Query RFID temperature

This command is used for the upper computer to obtain the temperature of RFID (for devices with built-in temperature sensors).

Upper computer command content: MID = 0x30

Parameter name	PID	Data type	Data length	Parameter description
-	-	-	-	-

Reader response content: MID=0x30

Parameter name	PID	Data type	Data length	Parameter description
RFID temperature	(M)	U8	1	-128 to 127℃

Send: AA02300000ABC3

Receive: AA0230000116468D

5.2.29 Configure optional reporting parameters

This command is used to configure the optional upload parameters of the reader.

Upper computer command content: MID = 0xE2

Parameter name	PID	Data type	Data length	Parameter description
UTC time parameter when the tag is read	0x01	U8	1	0:Do not upload 1:upload
Current frequency point	0x02	U8	1	0:Do not upload 1:upload
Current phase	0x03	U8	1	0:Do not upload 1:upload
RSSI_db	0x04	U8	1	0:Do not upload 1:upload

Reader response content: MID = 0xE3

Parameter name	PID	Data type	Data length	Parameter description
Result	(M)	U8	1	0, success. 1. Unsupported parameters.

Send: AA02E3000025BC //Query the optional reporting parameters

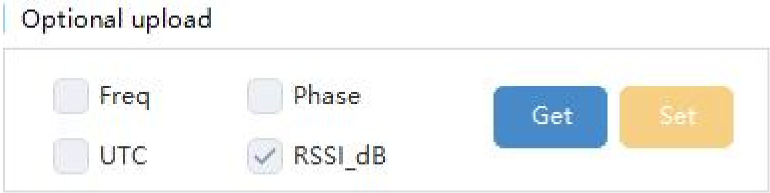
Receive:AA02E30008**01**00**02**00**03**00**04**009017 //all the optional reporting parameters don’t upload

Send: AA02E20008**01**00**02**00**03**00**04**018551 //Set RSSI_dB to upload

Receive: AA02E20001**00**2EDD //success

Send: AA02E3000025BC //Query the optional reporting parameters again

Receive: AA02E30008010002000300**04**011012 //RSSI_dB will upload



Optional upload

☐ Freq ☐ Phase

☐ UTC ☑ RSSI_dB

5.2.30 Query the optional reporting parameters

This command is used to query the optional upload parameters of the reader.

Upper computer command content: MID = 0xE3

Parameter name	PID	Data type	Data length	Parameter description

-	-	-	-	-

Reader response content: MID = 0xE3

Parameter name	PID	Data type	Data length	Parameter description
UTC time parameter when the tag is read	0x01	U8	1	0:Do not upload 1:upload
Current frequency point	0x02	U8	1	0:Do not upload 1:upload
Current phase	0x03	U8	1	0:Do not upload 1:upload
RSSI_db	0x04	U8	1	0:Do not upload 1:upload

5.2.31 Query working status

This command is used to query the working status of the reader.

Upper computer command content: MID = 0xFE

Parameter name	PID	Data type	Data length	Parameter description
-	-	-	-	-

Reader response content: MID = 0xFE

Parameter name	PID	Data type	Data length	Parameter description
Reader working status	-	U8	1	0: Idle state !0: Working state

Send: AA02FE00002418

Receive: AA02FE0001009EDB // the reader is at standby status, not reading tags.

6 Upgrade

6.1 Upgrade feature description

This instruction set is used for online upgrades of reader application software and baseband software (firmware). During the upgrade process, the host computer will split the upgrade file into a certain number of bytes. The host computer sends the upgrade packet with the serial number 0x00000000 to start the upgrade. When the upgrade is completed, the upgrade packet with the serial number 0xFFFFFFFF is sent as the end flag. The reader must confirm each upper computer upgrade packet, the upper computer must ensure that the reader has confirmed the current packet before sending the next update packet.

6.2 Upgrade message list

Readers configure a list of management instructions

Parameter name	PID	Data type
0x00	6.2.1 Device application software upgrade reader	Idle state
0x01	6.2.2 Baseband software upgrade	Idle state

6.2.1 Device application software upgrade

Power calibration This instruction is used for the reader application software to upgrade.

Upper computer command content: : MID = 0x00

Example: Initiate the upgrade process

Send(Hex): AA040000060000000000008636

Receive(Hex): AA0400000500000000008186

Example: update data

Send(Hex):

AA040000BA0000025500B400636F6E6E6563745F6E6F746966795F61636B5F6E756D00746D705F736F636B61646472006E65745F6765745F67617465776179006E737765725F627566665F7965730073716C697465335F657865630072656C61795F6F6E5F74696D655F7072616D0073796E634040474C4942435F322E30005F5F676D6F6E5F737461745F5F00496E697451756575650073747263707940404C4942435F322E3000434C3732303643325F5354445F415050C8EF2CBC302F

Receive(Hex): AA0400000500000255007FA8

Example: end

Send(Hex): AA04000006FFFFFFFF000086CA

Receive(Hex): AA04000005FFFFFFFF002B85

Parameter name	PID	Data type	Data length	Parameter description
Upgrade package serial number	(M)	U32	4	Upgrade package sequence number, 0x00000000 as the starting identity ,0xFFFFFFFF as the ending identity
Upgrade package content	(M)	U8	Variable length	Upgrade package data content

Reader response content: MID = 0x00

Parameter name	PID	Data type	Data length	Parameter description
Upgrade package serial number	(M)	U32	4	The sequence number of the upgrade package sent by the upper computer.
Upgrade package confirmation result	(M)	U8	1	0, successful 1, failed

6.2.2 Baseband software upgrade

This instruction is used for the reader application software to upgrade.

Upper computer command content: : MID = 0x01

Example: Initiate the upgrade process

Send(Hex): AA04010006000000000000000055

Receive(Hex): AA040100050000000000009180

Example: update data

Send(Hex):

```
AA0401010600000156010OFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
FFFFFFFFFF1622
```

Receive(Hex): AA040100050000015600 6592

Example: end

Send(Hex): AA04010006FFFFFFFF000000A9

Receive(Hex): AA04010005FFFFFFFF003B83

Parameter name	PID	Data type	Data length	Parameter description
Upgrade package serial number	(M)	U32	4	Upgrade package sequence number, 0x00000000 as the starting identity, 0xFFFFFFFF as the ending identity
Upgrade package confirmation result	(M)	U8	Variable length	Upgrade data content.

Reader response content: MID = 0x01

Parameter name	PID	Data type	Data length	Parameter description

Upgrade package serial number	(M)	U32	4	The sequence number of the upgrade package sent by the upper computer.
Upgrade package confirmation result	(M)	U8	1	0, successful 1, failed

7 Test commands

7.1 Test functions

This instruction set is used for device debugging and testing. Mainly used for reader power calibration, carrier RF target test.

7.2 Test command list

Command ID(MID)	Command description	Command executable status
0x00	Transmitting carrier command	Idle state
0x05	Antenna port SWR detection	Idle state

7.2.1 Transmitting carrier command

This command to appoint reader frequency point and Antenna port to Transmit RF carrier signal.

Upper computer command content: MID = 0x00

Example: Carrier wave ON, Antenna 1, frequency 0

Send(Hex): AA0500000201001E2D

Receive(Hex): AA0500000100879B

Parameter name	PID	Data type	Data length	Parameter description
Antenna port	(M)	U8	1	Bit0：Use antenna 1 Bit1：Use antenna 2 Bit2：Use antenna 3 Bit3：Use antenna 4 Bit4：Use antenna 5 Bit5：Use antenna 6

				Bit6： Use antenna 7 Bit7： Use antenna 8 Open carrier transmit command, only 1 antenna working at the same time
Frequency point	(M)	U8	1	Used to specify the current operating frequency band under the transmission channel, such as in the FCC standard 902~9285MHz band, channel 0 represents 902.750; channel 8 on behalf of 906.75; channel 15 on behalf of 910.250.
Antenna port expansion	0x01	U16	2	Bit0: Use antenna 9 Bit1: Use antenna 10 Bit2: Use antenna 11 Bit3: Use antenna 12 Bit4: Use antenna 13 Bit5: Use antenna 14 Bit6: Use antenna 15 Bit7: Use antenna 16 Bit8: Use antenna 17 Bit9: Use antenna 18 Bit10: Use antenna 19 Bit11: Use antenna 20 Bit12: Use antenna 21 Bit13: Use antenna 22 Bit14: Use antenna 23 Bit15: Use antenna 24

Reader response content： MID=0x00

Parameter name	PID	Data type	Data length	Parameter description
Carrier Transmitting result	(M)	U8	1	0， Carrier transmitting successfully 1， frequency parameter reader hardware does not support 2， the port parameter reader hardware does not support 3， phase-locked ring lock failed 4， other errors

7.2.2 Antenna port SWR detection

This command is used to detect the standing wave of the Antenna port. Before the calibration, the carrier of the specified Antenna port must be opened. At this time, the standing wave detection value obtained by the query is the forward and backward power detection value of the current port

Upper computer command content： MID = 0x05

Example:

Send(Hex): AA050500004444

Receive(Hex): AA05050002691CEFF8

Parameter name	PID	Data type	Data length	Parameter description
-	-	-	-	-

Reader response content： MID=0x05

Parameter name	PID	Data type	Data length	Parameter description
Forward power detection value	(M)	U8	1	Forward power detection normalized value
Backward power detection	(M)	U8	1	Backward power detection normalized value

The antenna port standing wave forward power detection value minus the backward value is more than 30 is considered normal, and the backward value is less than 115.

As long as the transmitting power remains unchanged, the forward power detection value is generally stable, and the better the antenna match is, the smaller the backward power detection value will be, thus the greater the difference between the two values will be.

```
OUT     aa 02 ff 00 00 a4 0f //stop
IN      aa 02 ff 00 01 00 0a d8 //stop successfully
```

Step 1

```
OUT     aa 05 00 00 02 08 01 a8 28 // start the antenna 4 to transmit RF carrier signal
IN      aa 05 00 00 01 00 87 9b // success
```

Step 2

```
OUT     aa 05 05 00 00 44 44 //query antenna 4 port SWR value
IN      aa 05 05 00 02 a7 47 ca 2d // return value
```

Step3

OUT aa 02 ff 00 00 a4 0f // stop transmitting rf carrier signal at antenna 4

IN aa 02 ff 00 01 00 0a d8 // success

7.2.3 Get SN

This command is used to obtain the serial number of the device.

Upper computer command content: MID = 0x33

Parameter name	PID	Data type	Data length	Parameter description
-	-	-	-	-

Reader response content: MID=0x33

Parameter name	PID	Data type	Data length	Parameter description
SN	(M)	U8	16	Reader Serial Number

Send: AA0533000047FC //Get reader SN

Receive: AA05330010433234303030313032313132303130 32B595 //SN is C240001021120102