UHF RFID Reader
U2861/U2881ADV
User Manual v2.21

Contents

1 Interface specification

Communication between host and reader is based on RS232 or RS485 protocols. Host delivers commands on these interfaces and reader will produces response and execute the delivered commands.

Data Frame Format	1 start bit, 8 data bits, 1 stop bit
Parity	NONE
Default Baud Rate	57600 bps
Transmission order	Least-significant bit first

2 Protocol Description

In a typical communication, host delivers command and parameters to reader, reader should execute the command and provide result or data response Reader will receive and execute ONE command in every communication cycle. Reader will not able to receive new command before the last execution and response delivery is completed. Any command which is transmitted during command execution will be ignored by the reader.

Command delivery from host:

Host	Direction	Reader
Command frame	→	

Description:
Once a command is received by reader, the reader will produce a response to host within the predefined inventory time. Data communication time is negligible here.

During communication, the transmitting time gap between every two consecutive bytes should be less than **15ms**. If the time gap exceeds 15ms, all the received data should be discarded and a normal receiving process restarts from the next byte.

Response delivery from reader:

Reader	Direction	Host
Response frame	→	

Description:
During communication, the transmitting time gap between every two consecutive bytes should be less than **15ms**.

A typical communication process is stated below:
1. Host delivers command to reader and wait for response;
2. Reader receives command, starts specific operation according to the received frame and produce response (of operation status and/or data) to host;
3. Host receives response from reader.

3 Formats of data frames

3.1 Command Frame Format (From HOST)

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

Format definition:

	Length (in byte)	Description
Len	1	Length of the command frame, defined by the amount of bytes between Adr and MSB_CRC16, i.e. the length of Data[] + 4.
Adr	1	Reader device address, the valid range of device address is 0x00 ~ 0xFE. 0xFF is the broadcast address. Reader will only response to command frame stated with a identical address or 0xFF. Default device address: 0x00.
Cmd	1	Command code.
Data[]	Variable	Parameter field, host may or may not provide parameters according to different commands formats.
LSB-CRC16	1	Low byte of CRC16. These 2 bytes are the CRC16 calculation of Len to Data[].
MSB-CRC16	1	High byte of CRC16

3.2 Response Frame Format (From READER)

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

Format description:

	Length (in byte)	Description
Len	1	Length of the response frame, defined by the amount of bytes between Adr and MSB_CRC16), i.e. the length of Data[] + 5.
Adr	1	Reader address.
reCmd	1	reCmd indicates which command this frame is responding to. For unrecognised command, reCmd should be 0x00.
Status	1	Command execution status/result.
Data[]	Variable	Data field, reader may or may not provide parameters according to actual commands.
LSB-CRC16	1	Low byte of CRC16. These 2 bytes are the CRC16 calculation of Len to Data[].
MSB-CRC16	1	High byte of CRC16

C language algorithm of CRC16:

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

pucY is the pointer of the array entry for CRC16 calculation, ucX is the amount of bytes included in this calculation. A 0x0000 return value indicates the input data had passed the CRC16 verification.

Whenever the host receive a data frame from reader, the host should always verify the frame by calling this CRC16 algorithm.

4 Command summary

4.1 EPC C1 G2（ISO18000-6C）Commands

No.	Command code	Function
1	0x01	Tag Inventory
2	0x02	Read data command
3	0x03	Write data command
4	0x04	Write EPC number
5	0x05	Kill tag
6	0x06	Set memory read/write protection for specific memory
7	0x07	Block erase
8	0x08	Read protection configuration (according to EPC number)
9	0x09	Read protection configuration (Without EPC number)
10	0x0a	Unlock read protection
11	0x0b	Read protection status check
12	0x0c	EAS configuration
13	0x0d	EAS alert detection
14	0x0f	Single tag inventory
15	0x10	Write blocks
16	0x11	Obtain Monza4QT working parameters
17	0x12	Modify Monza4QT working parameters
18	0x15	Extended data reading with assigned mask
19	0x16	Extended data writing with assigned mask
20	0x18	Inventory with memory buffer
21	0x19	Mix inventory
22	0x1a	Inventory with EPC number
23	0x1b	QT inventory

4.2 18000-6B Commands

No.	Command code	Function
1	0x50	Inventory command for SINGLE tag. This command will only inquire one tag in every cycle, with NO inventory condition.
2	0x51	Inventory command for MULTIPLE tags. Inquire tags according predefined condition and only return UIDs of the corresponding tags.
3	0x52	Read data command. Read data from tag, maximum 32 bytes in every command cycle.

4	0x53	Write data command. Write data to tag, maximum 32 bytes in every command cycle.
5	0x54	Obtain lock status command. Check the lock status of a particular memory unit.
6	0x55	Byte locking command. Lock a particular (unlocked) byte in a tag.

4.3   Reader customised command

No.	Command code	Function
1	0x21	Obtain reader information
2	0x22	Modify working frequency
3	0x24	Modify reader address
4	0x25	Modify reader inventory time
5	0x28	Modify serial baud rate
6	0x2f	Modify RF power
7	0x33	LED/Buzzer control
8	0x35	Modify reader working mode
9	0x36	Obtain auto-mode parameters
10	0x37	Modify EAS check accuracy and notification configuration
11	0x3b	Modify mask configuration
12	0x3c	Modify answering form configuration
13	0x3d	Modify inventory time break
14	0x3e	Modify inventory tag type
15	0x3f	Setup antenna multiplexing
16	0x40	Enable/disable buzzer
17	0x41	Adjust Real time clock
18	0x42	Obtain current time from real time clock
19	0x43	Obtain tag information from reader memory
20	0x44	Clear reader memory buffer
21	0x45	Relay control
22	0x46	GPIO control
23	0x47	Obtain GPIO state
24	0x48	Notification pulse configuration
25	0x49	Modify delay configuration in trigger-mode
26	0x4a	Modify configuration for TID inventory
27	0x4c	Obtain the reader unique serial number
28	0x4d	Switch network mode of reader
29	0x4e	Network AT transparent command
30	0x3a	Modify tag customised function
31	0x66	Enable antenna check

32	0x70	Modify maximum EPC/TID length configuration for memory buffer
33	0x71	Load the maximum EPC/TID length configuration
34	0x72	Obtain data from memory buffer
35	0x73	Clear memory buffer
36	0x74	Obtain the total tag amount from memory buffer
37	0x75	Modify parameters of real time inventory mode
38	0x77	Load real time inventory mode parameters
39	0x78	Load/modify heartbeat packet time break of real time inventory
40	0x79	Modify RF power configuration separately for write operations
41	0x7a	Load the RF power configuration of write operations
42	0x7b	Modify or load maximum write retry time configuration
43	0x81	Modify auto-mode inventory parameters
44	0x82	Obtain auto-mode inventory parameters
45	0x83	Obtain R2000 module firmware version
46	0x84	Update internal ROM
47	0x6e	Modify or load Antenna return loss threshold configuration
48	0x90	Modify or load DRM configuration
49	0x91	Measure antenna return loss

5 List of the response status

Response frame						Status definition	Description
Len	Adr	reCmd	Status	Data[]	CRC16		
5 + the length of Data[] field	0xXX	0xXX	0x00	...	LSB + MSB	Operation succeed	Command is successfully executed, all the requested data is included in the Data[] field of response frame.
5 + the length of Data[] field	0xXX	0x01	0x01	...	LSB + MSB	Inventory succeed	Host delivered **G2** tag inventory command, tag inventory was completed successfully and reader is able to deliver data response within the predefined inventory time.

5 + the length of Data[] field	0xXX	0x01	0x02	...	LSB + MSB	Inventory timeout	Host delivered **G2** tag inventory command, reader fails to complete the inventory within the predefined inventory time.
5 + the length of Data[] field	0xXX	0x01	0x03	...	LSB + MSB	Further data is waiting to be delivered	Host delivered **G2** tag inventory command, reader is not able to response all the data in a single frame, further data will be transmitted in the following frames.
5 + the length of Data[] field	0xXX	0x01	0x04	...	LSB + MSB	Reader memory is full	Host delivered **G2** tag inventory command, reader has completed parts of the inventory and run out of memory space due to the amount of tags. Reader will response the inquired EPC number.
5	0xXX	0xXX	0x05	N/A	LSB + MSB	Access password error	Host delivered an incorrect access password to reader.
5	0xXX	0x05	0x09	N/A	LSB + MSB	Tag killing failed	Host delivered a **G2** tag killing command, but the kill operation is failed due to incorrect tag killing password or poor communication between reader and tag.
5	0xXX	0x05	0x0a	N/A	LSB + MSB	All-zero tag killing password	It is not possible to kill a Tag with all-zero tag killing password.

5	0xXX	0xXX	0x0b	N/A	LSB + MSB	Command is not support by the tag	Some **optional** commands stated in G2 protocol and some manufacturers' customised command may not be supported by the tags.
5	0xXX	0xXX	0x0c	N/A	LSB + MSB	All-zero access password	For **NXP UCODE EPC G2X** tag, it is not possible to enable reader protection or enable EAS alert if the tag access password is all-zero.
5	0xXX	0x0a	0x0d	N/A	LSB + MSB	Fail to enable read protection	The read protection is enabled for the target NXP **UCODE EPC G2X** tag. It is not possible to lock a protection enabled tag.
5	0xXX	0x0a	0x0e	N/A	LSB + MSB	Fail to unlock the tag	The target **NXP UCODE EPC G2X** tag is already unlocked or the tag locking function is not support by the target tag.
5	0xXX	0x53	0x10	N/A	LSB + MSB	Fail to perform write operation	Some bytes stored in the target **6B** tag are locked.
5	0xXX	0x55	0x11	N/A	LSB + MSB	Fail to perform lock operation	Fail to perform lock operation on a **6B** tag.
5	0xXX	0x55	0x12	N/A	LSB + MSB	Fail to perform lock operation	The target **6B** tag is locked.
5	0xXX	0xXX	0x13	N/A	LSB + MSB	Fail to stored the parameter value	Fail to store the value of some preserved parameters. Configuration will still valid before reader shut down

5	0xXX	0xXX	0x14	N/A	LSB + MSB	Modification failed	Fail to adjust the RF power.
5 + the length of Data[] field	0xXX	0x51	0X15	...	LSB + MSB	response within the predefined inventory time	Host delivered **6B** tag inventory command, tag inventory was completed successfully and reader is able to deliver data response within the predefined inventory time.
5 + the length of Data[] field	0xXX	0x51	0x16	...	LSB + MSB	Inventory timeout	Host delivered **6B** tag inventory command, reader fails to complete the inventory within the predefined inventory time.
5 + the length of Data[] field	0xXX	0x51	0x17	...	LSB + MSB	Further data is waiting to be delivered	Host delivered **6B** tag inventory command, reader is not able to response all the data in a single frame, further data will be transmitted in the following frames.
5 + the length of Data[] field	0xXX	0x51	0x18	...	LSB + MSB	Reader memory is full	Host delivered 6B tag inventory command, reader has completed parts of the inventory and run out of memory space due to the amount of tags. Reader will response the inquired EPC number.
5	0xXX	0xXX	0x19	N/A	LSB + MSB	All-zero access password or function is not supported	Fail to enable EAS alert. It may caused by an all-zero tag access password or the EAS alert is not supported by the target tag.

5	0xXX	0xXX	0x1A	N/A	LSB + MSB	Fail to execute tag customised command	Some special tag functions are enabled, but fail to execute some commands.
5 + the length of Data[] field	0xXX	0x01	0x26	...	LSB + MSB	This frame contains statistic data packet	Host delivered **G2** tag inventory command, tag inventory was completed successfully and reader is now delivering statistic data packet.
5 + the length of Data[] field	0xXX	0xee	0x28	...	LSB + MSB	This frame contains heartbeat packet	In real time inventory mode, no tag is detected within the heartbeat packet time break, reader will upload heartbeat data.
5	0xXX	0xXX	0xF8	N/A	LSB + MSB	Antenna connection check failure	Antenna detuning occurred, reader starts self-protection, stop frequency signal output
5	0xXX	0xXX	0xF9	N/A	LSB + MSB	Fail to execute command	Command execution error.
5	0xXX	0xXX	0xFA	N/A	LSB + MSB	Operation failed	Tags are detected within the effective field, but failed to complete the operation due to poor communication between reader and tags.
5	0xXX	0xXX	0xFB	N/A	LSB + MSB	No operatable tags	No operatable tag is detected in the effective range.
6	0xXX	0xXX	0xFC	Err_code	LSB + MSB	Error code returned from tags	RFID tag reported an error to reader, reader will present this code in the "Err_code" field in the response.

5	0xXX	0xXX	0xFD	N/A	LSB + MSB	Command length error	Host delivered a command frame with incorrect frame length
5	0xXX	0x00	0xFE	N/A	LSB + MSB	Illegal command	Host delivered a incorrect command frame, e.g. unrecognised command code or a command frame with CRC error (failed to pass CRC16 check)
5	0xXX	0xXX	0xFF	N/A	LSB + MSB	Parameter error	Host delivered unrecognised parameters in a command frame.

6 RFID tag error code

EPC C1G2（ISO18000 -6C）RFID tag error code

Error code type	Error code	Error code definition	Error description
Specified error code	0x00	Other errors	All other errors supported by the tag.
	0x03	Memory full, or illegal PC value	Memory location is not found or unsupported PC value.
	0x04	Memory locked	Memory is being temporarily / permanently locked, unable to perform write operation.
	0x0b	Insufficient power supply	Unable to perform write operation due to insufficient power supply to tag.
Non-specified error code	0x0f	Undefined error	Tag unsupported errors.

7 Tag memory and access instructions

A. EPC C1G2 tags (G2 tags)

There are 4 memory areas in a G2 tags, reserved memory (also known as password memory), EPC memory, EID memory and user memory.

Reserved memory: 4 bytes, the first 2 bytes are the kill tag password, and the other 2 bytes are the

access password. This memory is readable and writeable by default. The read/write protection configurations of the two password blocks are isolated, they can be modified separately.

EPC memory: the EPC number of tag is stored in this memory. Word0 is CRC16 of PC value and EPC number. Word1 is PC value, indicates the length of EPC number. Actual EPC number stars from Word2. This memory is readable and writable by default.

TID memory: the inlay manufacturer predefined tag ID is stored in this memory. It is readable by default but unwritable.

User memory: user data is stored in this memory. It is readable and writable by default.

NOTE:
- Data length is required in many G2 commands, the unit of data length is either word or byte. The length of 1 word is equal to length of 2 bytes.

- Some commands may require access password, if access password is not setup in the target tag, fill the password field with 0. The password field can not be empty.

B. 18000-6B tags
There is one memory area in 6B tag only. The lower 8 bytes is the tag UID and it is un-modifiable. The rest of the memory is modifiable and lockable. Once memory is locked, this particular part of memory will be un-writable and un-lockable.

8 Command detail description

8.1 Overview

There are 3 types of commands:
- protocol related commands;
- reader related commands;
- tag customised commands.

If an incorrect command frame is delivered from host, e.g. unrecognised command code or command frame with CRC error (failed to pass CRC16 check). A similar frame as shown below will be responded from reader.

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

For incorrect command frame length, the response will be similar to the following frame,

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

There are 2 situations which commands will be ignored by reader:
- Incorrect address (neither broadcasting address 0xff, nor corresponding reader address)
- Incomplete command frame, i.e. the actual command frame length is less than the value indicated in the "Len" field

Reader will not provide any response for the situations stated above.

8.2 EPC C1G2 commands

8.2.1 Tags inventory

Inventory command is used for inquire RFID tags with corresponding protocol and obtain tag information within the effective field. In order to process further operation on a new tag with unknown EPC, user should firstly obtain tag EPC number by using inventory command.

According to different circumstances, user can modify the setting of maximum operation time (inventory time). Reader will return an inventory result within the predefined inventory time. If the reader fails to complete inventory processes for all the tags in the effective field within the predefined inventory time, reader will not perform further inventory after inventory time is exceed. Reader will report all the already inquired tags, as well as the current (uncompleted) inventory status to host. Reader will then wait for the next command from host.

Default inventory time is 1s, it can be modified by using reader customised command "modify reader inventory time" (refer to chapter 8.4.4). The valid range of inventory time is from 3*100ms to 255*100ms (the actual responding time may slightly larger than the setting value and this difference will varies from 0 up to 75ms).
Note: an unreasonable short inventory time setting may cause tag inventory failure.

Command frame:

Len	Adr	Cmd	Data[]	CRC-16	
0xXX	0xXX	0x01	——	LSB	MSB

Parameters of Data[]:

Data[]							
QValue	Session	MaskMem	MaskAdr	MaskLen	MaskData	AdrTID	LenTID
0xXX	0xXX	0xXX	2 bytes	0xXX	Variable	0xXX	0xXX

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

Parameters definition
QValue: 1 byte.

bit7: Statistic data packet flag.
  0 – after inventory，DO NOT deliver statistic data packet of inventory process;
  1 – after inventory，deliver statistic data packet of inventory process
bit6 ~ bit0: the original Q-value of the EPC tag inventory, the setting of Q-value should follow the
    rule: $2^Q \approx$ total amount of tags within the effective field. The range of Q-value is 0 ~ 15,
    if other value is delivered in this field, reader will return a parameter error status in the
    response frame.

Session: 1 byte, the Session-value of the EPC tag inventory.
    0x00 – apply S0 as Session value;
    0x01 – apply S1 as Session value;
    0x02 – apply S2 as Session value;
    0x03 – apply S3 as Session value;
    0xff – apply reader smart configuration (only valid in EPC inventory).
All other values are reserved, reader will return a parameter error status in the response frame if
other value is delivered in this field.

MaskMem: 1 byte, mask area indication.
    0x01 – EPC memory;
    0x02 – TID memory;
    0x03 – User memory.
All other values are reserved, reader will return a parameter error status in the response frame if
other value is delivered in this field.

MaskAdr: 2 bytes, entry bit address of the mask, the valid range of MaskAdr is 0 ~ 16383.

MaskLen: 1 byte, bit length of mask (unit: bits).

MaskData: mask data. The length of MaskData equals to MaskLen/8. If MaskLen is not a multiple
of 8 integer, the length of MaskData is equal to the int[MaskLen/8]+1. Non-specified lower
significant figures should be filled up with 0.

AdrTID: initial word address of inventory TID memory. If command delivered this parameter and
LenTID at the same frame, the mode of inventory should be TID, not EPC.

LenTID: data length for TID inventory operation, the valid range of LenTID is 0 ~ 15.
All other values are reserved, and reader will return a parameter error status in the response frame if
other value is delivered in this field. If command delivered this parameter and AdrTID, the mode of
inventory should be TID, not EPC.

Target (optional parameter): 1 byte, the Target value of EPC tag inventory.
        0x00 – apply A as Target value;
        0x01 – apply B as Target value.

All other values are reserved, reader will return a parameter error status in the response frame if other value is delivered in this field.

Ant (optional parameter): 1 byte, antenna selection for the current inventory.

> 0x80 – antenna 1;
> 0x81 – antenna 2;
> 0x82 – antenna 3;
> 0x83 – antenna 4.

All other values are reserved, and reader will return a parameter error status in the response frame if other value is delivered in this field.

ScanTime (optional parameter): 1 byte, the inventory time configuration for the current inventory. Reader will set the maximum operation time as ScanTime*100ms.

NOTE:

1. When MaskMem, MaskAdr, MaskLen and MaskData are not provided, no mask pattern will be involved in inventory

2. Target, Ant and ScanTime are optional parameters, all three parameters must be delivered in one command frame. Reader will apply default setting for these parameter, until all three parameters setting are being properly deliver from host, the new settings will then become effective for following inventory.

(1) Response status is 0x26, the response should be as following:

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

Parameters definition

Status: the status of response, detail description is shown in the following table

Status	Description
0x26	After inventory, deliver statistic data of the last inventory process

Ant: indicates which antenna had inquired a tag. For example, 0x04 is 0000 0100 in binary, this indicates Antenna 3 had inquired this specific tag. For 0x08, it is 0000 1000 in binary, then it indicates Antenna 4 had inquired tag information.

ReadRate: tag identification rate for the current inventory (time of successful identification / sec), a tag being indentified multiple times will also increase the time of successful identification.

TotalCount: the total amount of tag detected in the current inventory, a tag being accessed multiple times will also increase the total amount.

(2) Response status is not 0x26, the response should be as following:

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

Parameters definition

Status: the status of response, detail description is shown in the following table

Status	Description
0x01	Operation completed, reader will report all inquired tags information to host
0x02	Inventory timeout, operation is aborted. reader will report all the already inquired tags to host
0x03	For status = 0x03, reader is not able to response all the data in a single frame, further data will be transmitted in the following frames.
0x04	Reader only completed parts of the inventory but run out of memory space due to the amount of tags. Reader will report all the already inquired tags as well as this status value to host.
0xF8	Antenna error detected, the current antenna might be disconnected.

Ant: indicates which antenna had inquired a tag. For example, 0x04 is 0000 0100 in binary, this indicates Antenna 3 had inquired this specific tag. For 0x08, it is 0000 1000 in binary, then it indicates Antenna 4 had inquired tag information.

Num: the amount of RFID EPC/TID included in this response.

EPC ID: inquired EPC/TID data. For instance, EPC-1 is the EPC/TID length + EPC number/TID data + RSSI value of the first tag etc. The RSSI and EPC length values are one byte parameters. The unit of EPC C1 G2 data is word. During communication, the most-significant word and the most-significant byte in a word will be transmitted first.

8.2.2   Read data

The function of this command is to read data from reserved memory, EPC memory, TID memory, user memory of tag. Read operation starts from a defined address. The unit of data is word.

Command frame:

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

Parameters of Data[]:

Data[]									
ENum	EPC	Mem	WordPtr	Num	Pwd	MaskMem	MaskAdr	MaskLen	MaskData
0xXX	variable	0xXX	0xXX	0xXX	4 bytes	0xXX	2 bytes	0xXX	variable

Parameters definition

ENum:

0x00 ~ 0x0f – ENum represents the length of EPC number. The unit of ENum is word, and the length of EPC should be less than 15 words. In this situation, parameters MaskMen, MaskAdr, MaskLen, MaskData should all be left empty.

0xff – MaskMem, MaskAdr, MaskLen, MaskData should be provided instead of EPC parameters. Reader will return a parameter error status in the response frame if other value is delivered in this field.

EPC: EPC number of the target tag. Length of the EPC depends on the provided EPC number, and the length value must be an integer. The unit of EPC number is word. During communication, the most-significant word and the most-significant byte in a word will be transmitted first. It is essential to provide FULL EPC in this command.

Mem: 1 byte, the type of target memory.

      0x00 – reserved memory

      0x01 – EPC memory;

      0x02 – TID memory;

      0x03 – User memory.

All other values are reserved. Reader will return a parameter error status in the response frame if other value is delivered in this field.

WordPtr: 1 byte, the entry address of target. For instance, 0x00 represent the read operation starts from 1st word (the first 16-bit memory area), 0x01 represents operation starts from the 2nd word, etc.

Num: 1 byte, the amount of words will be read in this operation. Hence 0x00 is not a valid value for this parameter. Furthermore the value of Num should not exceed 120, i.e. the maximum reading amount is 120 words. Reader will return a parameter error status in the response frame if a 0 or a larger than 120 value is delivered in this field.

Pwd: 4 bytes, it is the 4 bytes access password of a tag. From left to right, the first two bytes are the high bytes of access password, and the last two bytes are the low bytes. The most-significant bit of a tag 32-bit access password is the most-significant bit in the 1st byte of Pwd (from left to right). Likewise, the least-significant bit of a tag 32-bit access password is the least-significant bit in the 4th (last) byte of Pwd. Access password will only be used for verification during reserved memory reading operation, when the associated target memory is password protected and the tag access password is non-zero. Otherwise Psw should be set to all-zero or set to the correct access password.

MaskMem: 1 byte, mask area indication.

      0x01 – EPC memory;

      0x02 – TID memory;

      0x03 – User memory.

All other values are reserved, reader will return a parameter error status in the response frame if other value is delivered in this field.

MaskAdr: 2 bytes, entry bit address of the mask, the valid range of MaskAdr is 0 ~ 16383.

MaskLen: 1 byte, bit length of mask (unit: bits).

MaskData: mask data. The length of MaskData equals to MaskLen/8. If MaskLen is not a multiple of 8 integer, the length of MaskData is equal to the int[MaskLen/8]+1. Non-specified lower significant figures should be filled up with 0.

NOTE:
When MaskMem, MaskAdr, MaskLen and MaskData are not provided, full EPC number will be used as mask pattern in inventory.

Response frame:

Len	Adr	reCmd	Status	Data[]	CRC-16	
0xXX	0xXX	0x02	0x00	Word1，Word2,…	LSB	MSB

Parameters definition
Word1, Word2...: the unit of data in this field is word. Every word contains 2 bytes, most-significant byte first. Word1 is the 1st word from the starting address and the 2nd word is Word 2 etc.

8.2.3 Write data

The function of this command is to write multiple words to reserved memory, TID memory or user memory in one communication cycle.

Command frame:

Len	Adr	Cmd	Data[]	CRC-16	
0xXX	0xXX	0x03	——	LSB	MSB

Parameters of Data[]:

Data[]					
WNum	ENum	EPC	Mem	WordPtr	Wdt
0xXX	0xXX	variable	0xXX	0xXX	variable
Pwd	MaskMem	MaskAdr	MaskLen	MaskData	
4 bytes	0xXX	2 bytes	0xXX	variable	

Parameters definition
WNum: the amount of words to be written. Every word contains 2 bytes. The value of WNum must be larger than 0, and less or equal to 32, as well as identical to the actual amount of word to be written. Reader will return a parameter error status in the response frame if a 0 or an incorrect value of WNum is delivered in this field.

ENum:

0x00 ~ 0x0f – ENum represents the length of EPC number. The unit of ENum is word, and the length of EPC should be less than 15 words. In this situation, parameters MaskMen, MaskAdr, MaskLen, MaskData should all be left empty.

0xff – MaskMem, MaskAdr, MaskLen, MaskData should be provided instead of EPC parameters. Reader will return a parameter error status in the response frame if other value is delivered in this field.

EPC: EPC number of the target tag. Length of the EPC depends on the provided EPC number. The unit of EPC number is word. During communication, the most-significant word and the most-significant byte in a word will be transmitted first. It is essential to provide FULL EPC in this command.

Mem: 1 byte, the type of target memory.

      0x00 – reserved memory
      0x01 – EPC memory;
      0x02 – TID memory;
      0x03 – User memory.

All other values are reserved. Reader will return a parameter error status in the response frame if other value is delivered in this field.

WordPtr: 1 byte, the entry address of target.

Wdt: words to be written to tag memory. The amount of words in Wdt must be identical to the value of WNum. The most-significant byte comes first in a word. Words will be written to tag from lower address to higher address according to the order in Data[]. For instance, WordPtr is 0x02, the 1st word in Data[](from left to right) will be written to the address 0x02 in the memory specified by Mem, the 2nd word will then be written to 0x03 etc.

Pwd: 4 bytes, it is the 4 bytes access password of a tag. From left to right, the first two bytes are the high bytes of access password, and the last two bytes are the low bytes. The most-significant bit of a tag 32-bit access password is the most-significant bit in the 1st byte of Pwd (from left to right). Likewise, the least-significant bit of a tag 32-bit access password is the least-significant bit in the 4th (last) byte of Pwd. Access password must be properly provided and will be verified before write operations. If target memory is not password protected, Pwd can be set to all-zero.

MaskMem: 1 byte, mask area indication.

      0x01 – EPC memory;
      0x02 – TID memory;
      0x03 – User memory.

All other values are reserved, reader will return a parameter error status in the response frame if other value is delivered in this field.

MaskAdr: 2 bytes, entry bit address of the mask, the valid range of MaskAdr is 0 ~ 16383.

MaskLen: 1 byte, bit length of mask (unit: bits).

MaskData: mask data. The length of MaskData equals to MaskLen/8. If MaskLen is not a multiple of 8 integer, the length of MaskData is equal to the int[MaskLen/8]+1. Non-specified lower significant figures should be filled up with 0.

NOTE:
When MaskMem, MaskAdr, MaskLen and MaskData are not provided, full EPC number will be used as mask pattern in inventory.

Response frame:

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

8.2.4 Write EPC number

The function of this command is to write EPC number to a tag. During this write EPC operation, only one tag is allowed to be place in the antenna effective area.

Command frame:

Len	Adr	Cmd	Data[]			CRC-16	
			ENum	Pwd	WEPC		
0xXX	0xXX	0x04	0xXX	4 bytes	Variable	LSB	MSB

Parameters definition
ENum: 1 byte, the length of EPC number. The unit of ENum is word, and the length of EPC can be 0, but it should be less than 15 words. Reader will return a parameter error status in the response frame if other value is delivered in this field.

Pwd: 4 bytes, it is the 4 bytes access password of a tag. From left to right, the first two bytes are the high bytes of access password, and the last two bytes are the low bytes. The most-significant bit of a tag 32-bit access password is the most-significant bit in the 1st byte of Pwd (from left to right). Likewise, the least-significant bit of a tag 32-bit access password is the least-significant bit in the 4th (last) byte of Pwd. Access password will only be used for verification if the EPC memory is password protected and the tag access password is non zero. Psw should be set to all-zero or set to the correct access password.

WEPC: the EPC number to be written to tag. The amount of words in WEPC must be identical to the value of ENum. The minimum and maximum length of WEPC is 1 and 15. Reader will return a parameter error status in the response frame if data with inappropriate length is delivered in this field.

Response frame:

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

8.2.5 Kill tag

The function of this command is to kill tags. After the kill operation, the tags will no longer process any command from reader.

Command frame:

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

Parameters of Data[]:

Data[]						
ENum	EPC	Killpwd	MaskMem	MaskAdr	MaskLen	MaskData
0xXX	variable	4 bytes	0xXX	2 bytes	0xXX	variable

Parameters definition
ENum:
0x00 ~ 0x0f – ENum represents the length of EPC number. The unit of ENum is word, and the length of EPC should be less than 15 words. In this situation, parameters MaskMen, MaskAdr, MaskLen, MaskData should all be left empty.
0xff – MaskMem, MaskAdr, MaskLen, MaskData should be provided instead of EPC parameters. Reader will return a parameter error status in the response frame if other value is delivered in this field.

EPC: EPC number of the target tag. Length of the EPC depends on the provided EPC number. The unit of EPC number is word. During communication, the most-significant word and the most-significant byte in a word will be transmitted first. It is essential to provide FULL EPC in this command.

Killpwd: 4 bytes, it is the 4 bytes kill password of a tag. From left to right, the first two bytes are the high bytes of kill password, and the last two bytes are the low bytes. The most-significant bit of a tag 32-bit kill password is the most-significant bit in the 1st byte of Killpwd (from left to right). Likewise, the least-significant bit of a tag 32-bit kill password is the least-significant bit in the 4th (last) byte of Killpwd. In order to kill a tag, the kill password of this tag must be non-zero. It is not possible to kill a tag with zero kill password, hence reader will return a parameter error status in the response frame if all-zero are delivered in this field.

MaskMem: 1 byte, mask area indication.
　　　　0x01 – EPC memory;
　　　　0x02 – TID memory;
　　　　0x03 – User memory.
All other values are reserved, reader will return a parameter error status in the response frame if other value is delivered in this field.

MaskAdr: 2 bytes, entry bit address of the mask, the valid range of MaskAdr is 0 ~ 16383.

MaskLen: 1 byte, bit length of mask (unit: bits).

MaskData: mask data. The length of MaskData equals to MaskLen/8. If MaskLen is not a multiple of 8 integer, the length of MaskData is equal to the int[MaskLen/8]+1. Non-specified lower significant figures should be filled up with 0.

NOTE:
When MaskMem, MaskAdr, MaskLen and MaskData are not provided, full EPC number will be used as mask pattern in inventory.

Response frame

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

8.2.6 Set read/write protection for specific memory

The function of this command is to set the read/write protection status for the following memory
- Reserved memory
  Readable/ writable without protection, permanently readable/ writable, readable/writeable with password protected or permanently unreadable/ un-writable;
- EPC memory /user reserved memory
  Writable without protection, permanently writable, writeable with password protected or permanently un-writable;

EPC memory, user reserved memory and TID memory are permanently readable. Furthermore TID memory is readable only.

Once the protection status of reserved memory is set to permanently readable/ writable or permanently unreadable/ un-writable, the status configuration will not able to accept any future modification. Likewise, if the protection status of EPC memory, user reserved memory or TID memory is set to permanently writable/ un-writable, the status configuration will not able to accept any future modification. Tag will return an error status in the response frame if user attempted to perform future modification.

Access password must be provided to set a specific memory to password protected readable/writable, or change the status from password protected to no protection. Hence, it is essential to ensure access password is already setup for the RFID tag before this operation.

Command frame:

Len	Adr	Cmd	Data[]	CRC-16	
0xXX	0xXX	0x06	——	LSB	MSB

Parameters of Data[]:

Data[]								
ENum	EPC	Select	SetProtect	Pwd	MaskMem	MaskAdr	MaskLen	MaskData
0xXX	variable	0xXX	0xXX	4 bytes	0xXX	2 bytes	0xXX	variable

Parameters definition
ENum:
0x00 ~ 0x0f – ENum represents the length of EPC number. The unit of ENum is word, and the length of EPC should be less than 15 words. In this situation, parameters MaskMen, MaskAdr, MaskLen, MaskData should all be left empty.
0xff – MaskMem, MaskAdr, MaskLen, MaskData should be provided instead of EPC parameters. Reader will return a parameter error status in the response frame if other value is delivered in this field.

EPC: EPC number of the target tag. Length of the EPC depends on the provided EPC number. The unit of EPC number is word. During communication, the most-significant word and the most-significant byte in a word will be transmitted first. It is essential to provide FULL EPC in this command.

Select: 1 byte.
    0x00 – modify kill password read/write protection;
    0x01 – modify access password read/write protection;
    0x02 – modify EPC memory read/write protection;
    0x03 – modify TID memory read/write protection;
    0x04 – modify user memory read/write protection.
All other values are reserved, reader will not execute the command and will return a parameter error status in the response frame if other value is delivered in this field.

SetProtect: 1 byte, the value of SetProtect depends on the value of Select.
- For Select = 0x00 or 0x01, i.e. the kill password or access password protection setting, the value of SetProtect can be the following,
    0x00 – set to readable/ writable without protection;
    0x01 – set to permanently readable/ writable;
    0x02 – set to readable/writeable with password protected;
    0x03 – set to permanently unreadable/ un-writable.
- For Select = 0x02, 0x03, 0x04, i.e. the EPC, TID and user memory protection setting, the value of SetProtect can be the following,
    0x00 – set to writable without protection;
    0x01 – set to permanently writable;
    0x02 – set to writeable with password protected;
    0x03 – set to permanently un-writable.
All other values of Select and SetProtect are reserved, reader will not execute the command and will return a parameter error status in the response frame if other value is delivered in this field.

Pwd: 4 bytes, it is the 4 bytes access password of a tag. From left to right, the first two bytes are the

high bytes of access password, and the last two bytes are the low bytes. The most-significant bit of a tag 32-bit access password is the most-significant bit in the 1st byte of Pwd (from left to right). Likewise, the least-significant bit of a tag 32-bit access password is the least-significant bit in the 4th (last) byte of Pwd. A correct access password must be provided to start the operation.

MaskMem: 1 byte, mask area indication.

> 0x01 – EPC memory;
> 0x02 – TID memory;
> 0x03 – User memory.

All other values are reserved, reader will return a parameter error status in the response frame if other value is delivered in this field.

MaskAdr: 2 bytes, entry bit address of the mask, the valid range of MaskAdr is 0 ~ 16383.

MaskLen: 1 byte, bit length of mask (unit: bits).

MaskData: mask data. The length of MaskData equals to MaskLen/8. If MaskLen is not a multiple of 8 integer, the length of MaskData is equal to the int[MaskLen/8]+1. Non-specified lower significant figures should be filled up with 0.

NOTE:
When MaskMem, MaskAdr, MaskLen and MaskData are not provided, full EPC number will be used as mask pattern in inventory.

Response frame:

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

8.2.7   Block erase

The function of this command is to erase multiple words in reserved, EPC, TID or user memory.

Command frame:

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

Parameters of Data[]:

Data[]									
ENum	EPC	Mem	WordPtr	Num	Pwd	MaskMem	MaskAdr	MaskLen	MaskData
0xXX	variable	0xXX	0xXX	0xXX	4 bytes	0xXX	2 bytes	0xXX	variable

Parameters definition
ENum:
0x00 ~ 0x0f – ENum represents the length of EPC number. The unit of ENum is word, and the

length of EPC should be less than 15 words. In this situation, parameters MaskMen, MaskAdr, MaskLen, MaskData should all be left empty.

0xff – MaskMem, MaskAdr, MaskLen, MaskData should be provided instead of EPC parameters. Reader will return a parameter error status in the response frame if other value is delivered in this field.

EPC: EPC number of the target tag. Length of the EPC depends on the provided EPC number. The unit of EPC number is word. During communication, the most-significant word and the most-significant byte in a word will be transmitted first. It is essential to provide FULL EPC in this command.

Mem: 1 byte, the type of target memory.
>   0x00 – reserved memory
>   0x01 – EPC memory;
>   0x02 – TID memory;
>   0x03 – User memory.

All other values are reserved. Reader will return a parameter error status in the response frame if other value is delivered in this field.

WordPtr: 1 byte, the entry address of target. For instance, 0x01 represents erase operation starts from the 2nd word (the second 16-bit memory area), etc. For EPC memory erase operation, the minimum value of WordPtr should be 0x01. Reader will return a parameter error status in the response frame if inappropriate value is delivered in this field.

Num: 1 byte, the amount of words to be erased in this operation. Erase will start from the addres stated in WordPtr and will erase amount of words stated in Num. 0x00 is not a valid value for this parameter. Reader will return a parameter error status in the response frame if a 0 or a larger than 120 value is delivered in this field.

Pwd: 4 bytes, it is the 4 bytes access password of a tag. From left to right, the first two bytes are the high bytes of access password, and the last two bytes are the low bytes. The most-significant bit of a tag 32-bit access password is the most-significant bit in the 1st byte of Pwd (from left to right). Likewise, the least-significant bit of a tag 32-bit access password is the least-significant bit in the 4th (last) byte of Pwd. Access password will only be used for verification if the associated memory is password protected. Psw should be set to all-zero or set to the correct access password.

MaskMem: 1 byte, mask area indication.
>   0x01 – EPC memory;
>   0x02 – TID memory;
>   0x03 – User memory.

All other values are reserved, reader will return a parameter error status in the response frame if other value is delivered in this field.

MaskAdr: 2 bytes, entry bit address of the mask, the valid range of MaskAdr is 0 ~ 16383.

MaskLen: 1 byte, bit length of mask (unit: bits).

MaskData: mask data. The length of MaskData equals to MaskLen/8. If MaskLen is not a multiple of 8 integer, the length of MaskData is equal to the int[MaskLen/8]+1. Non-specified lower significant figures should be filled up with 0.

NOTE:
When MaskMem, MaskAdr, MaskLen and MaskData are not provided, full EPC number will be used as mask pattern in inventory.

Response frame:

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

8.2.8   Read protection configuration (according to EPC number)

The function of this command is to setup read protection for a tag with particular EPC number; hence the tag will be unreadable by device. Device will not able to inquire EPC number of this tag via inventory operation. This command only valid for **NXP UCODE EPC G2X** tags.

Command frame:

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

Parameters of Data[]:

Data[]						
ENum	EPC	Pwd	MaskMem	MaskAdr	MaskLen	MaskData
0xXX	variable	4 bytes	0xXX	2 bytes	0xXX	variable

Parameters definition
ENum:
0x00 ~ 0x0f – ENum represents the length of EPC number. The unit of ENum is word, and the length of EPC should be less than 15 words. In this situation, parameters MaskMen, MaskAdr, MaskLen, MaskData should all be left empty.
0xff – MaskMem, MaskAdr, MaskLen, MaskData should be provided instead of EPC parameters. Reader will return a parameter error status in the response frame if other value is delivered in this field.

EPC: EPC number of the target tag. Length of the EPC depends on the provided EPC number. The unit of EPC number is word. During communication, the most-significant word and the most-significant byte in a word will be transmitted first. It is essential to provide FULL EPC in this command.

Pwd: 4 bytes, it is the 4 bytes access password of a tag. From left to right, the first two bytes are the

high bytes of access password, and the last two bytes are the low bytes. The most-significant bit of a tag 32-bit access password is the most-significant bit in the 1st byte of Pwd (from left to right). Likewise, the least-significant bit of a tag 32-bit access password is the least-significant bit in the 4th (last) byte of Pwd. It is not possible to setup the read protection status if the tag has all-zero access password, hence reader will return a parameter error status in the response frame if zeros or incorrect access password are delivered in this field.

MaskMem: 1 byte, mask area indication.

> 0x01 – EPC memory;
> 0x02 – TID memory;
> 0x03 – User memory.

All other values are reserved, reader will return a parameter error status in the response frame if other value is delivered in this field.

MaskAdr: 2 bytes, entry bit address of the mask, the valid range of MaskAdr is 0 ~ 16383.

MaskLen: 1 byte, bit length of mask (unit: bits).

MaskData: mask data. The length of MaskData equals to MaskLen/8. If MaskLen is not a multiple of 8 integer, the length of MaskData is equal to the int[MaskLen/8]+1. Non-specified lower significant figures should be filled up with 0.

NOTE:
When MaskMem, MaskAdr, MaskLen and MaskData are not provided, full EPC number will be used as mask pattern in inventory.

Response frame:

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

8.2.9 Read protection configuration (Without EPC number)

The function of this command is to setup read protection for tags within the effective field. Unlike the pervious command in chapter 8.2.8, this command will perform operation on multiple inquired tags without tag identification. In order to perform operation on multiple tags, it is vital to keep access password consistent on those tags. This command only valid for **NXP UCODE EPC G2X** tags.

Command frame:

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

Parameter definition
Pwd: 4 bytes, it is the 4 bytes access password of a tag. From left to right, the first two bytes are the

high bytes of access password, and the last two bytes are the low bytes. The most-significant bit of a tag 32-bit access password is the most-significant bit in the 1st byte of Pwd (from left to right). Likewise, the least-significant bit of a tag 32-bit access password is the least-significant bit in the 4th (last) byte of Pwd. It is not possible to setup the read protection status if the tag has all-zero access password, hence reader will return a parameter error status in the response frame if zeros or incorrect access password are delivered in this field.

Response frame:

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

8.2.10   Unlock read protection

The function of this command is to unlock read protection of a tag. Only one tag is allowed to be place in the antenna effective area. This command only valid for **NXP UCODE EPC G2X** tags.

Command frame:

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

Parameter definition
Pwd: 4 bytes, it is the 4 bytes access password of a tag. From left to right, the first two bytes are the high bytes of access password, and the last two bytes are the low byte. The most-significant bit of a tag 32-bit access password is the most-significant bit in the 1st byte of Pwd (from left to right). Likewise, the least-significant bit of a tag 32-bit access password is the least-significant bit in the 4th (last) byte of Pwd. It is essential to provide a correct access password in this command, reader will return a parameter error status in the response frame if incorrect access password is delivered in this field.

Response frame:

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

NOTE:
For tags with no read protection function, the default status will be unlocked.

8.2.11   Read protection status check

This command is NOT ABLE TO identify if a specific tag supports the read protection function, the command ONLY inquire the read protection status of the tag. For tags with no read protection function, the default status will be unlocked. Only one tag is allowed to be place in the antenna effective area. This command only valid for **NXP UCODE EPC G2X** tags.

Command frame:

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

Response frame:

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

Parameter definition

ReadPro: 0x00 – read protection is disabled for the tag;

0x01 – read protection is enabled for the tag.

For tags with no read protection function, the default status will be unlocked.

8.2.12 EAS configuration

The function of this command is to modify or reset EAS status. This command only valid for **NXP UCODE EPC G2** tags.

Command frame:

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

Parameters of Data[]:

Data[]							
ENum	EPC	Pwd	EAS	MaskMem	MaskAdr	MaskLen	MaskData
0xXX	variable	4Byte	0xXX	0xXX	2 bytes	0xXX	variable

Parameters definition

ENum:

0x00 ~ 0x0f – ENum represents the length of EPC number. The unit of ENum is word, and the length of EPC should be less than 15 words. In this situation, parameters MaskMen, MaskAdr, MaskLen, MaskData should all be left empty.

0xff – MaskMem, MaskAdr, MaskLen, MaskData should be provided instead of EPC parameters. Reader will return a parameter error status in the response frame if other value is delivered in this field.

EPC: EPC number of the target tag. Length of the EPC depends on the provided EPC number. The unit of EPC number is word. During communication, the most-significant word and the most-significant byte in a word will be transmitted first. It is essential to provide FULL EPC in this command.

Pwd: 4 bytes, it is the 4 bytes access password of a tag. From left to right, the first two bytes are the high bytes of access password, and the last two bytes are the low byte. The most-significant bit of a

tag 32-bit access password is the most-significant bit in the 1st byte of Pwd (from left to right). Likewise, the least-significant bit of a tag 32-bit access password is the least-significant bit in the 4th (last) byte of Pwd. It is not possible to setup EAS if the tag has zero access password, hence reader will return a parameter error status in the response frame if zeros or incorrect access password are delivered in this field.

EAS: 1 byte.
      bit0 = 0, EAS alert is disabled;
      bit0 = 1, EAS alert is enabled.
      bit1 ~ bit7 are reserved, with 0 as default value.
MaskMem: 1 byte, mask area indication.
           0x01 – EPC memory;
           0x02 – TID memory;
           0x03 – User memory.
All other values are reserved, reader will return a parameter error status in the response frame if other value is delivered in this field.

MaskAdr: 2 bytes, entry bit address of the mask, the valid range of MaskAdr is 0 ~ 16383.

MaskLen: 1 byte, bit length of mask (unit: bits).

MaskData: mask data. The length of MaskData equals to MaskLen/8. If MaskLen is not a multiple of 8 integer, the length of MaskData is equal to the int[MaskLen/8]+1. Non-specified lower significant figures should be filled up with 0.

NOTE
When MaskMem, MaskAdr, MaskLen and MaskData are not provided, full EPC number will be used as mask pattern in inventory.

Response frame:

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

8.2.13   EAS alert detection

The function of this command is to detect EAS alert, only valid for **NXP UCODE EPC G2** tags.

Command frame:

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

Response frame:

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

Return "no operatable tag" if EAS alert is not detected.

8.2.14 Single tag inventory

Command frame:

Len	Adr	Cmd	Data[]	CRC-16	
0x04	0xXX	0x0f	——	LSB	MSB

Response frame:

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

Parameters definition

Ant: indicates which antenna had inquired a tag. For example, 0x04 is 0000 0100 in binary, this indicates Antenna 3 had inquired this specific tag. For 0x08, it is 0000 1000 in binary, then it indicates Antenna 4 had inquired tag information.

Num: 0x01 (constant)

EPC ID: inquired tag EPC data. For instance, EPC-1 is the EPC length + EPC number + **RSSI value** of the first tag etc. The RSSI and EPC length values are one byte parameters. The unit of EPC C1 G2 data is word. During communication, the most-significant word and the most-significant byte in a word will be transmitted first.

8.2.15 Write blocks

The function of this command is to write multiple words to reserved memory, EPC, TID and user memory.

Command frame:

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

Parameters of Data[]:

Data[]					
WNum	ENum	EPC	Mem	WordPtr	Wdt
0xXX	0xXX	variable	0xXX	0xXX	variable
Pwd	MaskMem	MaskAdr	MaskLen	MaskData	

4 bytes	0xXX	2 bytes	0xXX	variable

Parameters definition

WNum: the amount of words to be written. Every word contains 2 bytes. The value of WNum must be larger than 0, as well as identical to the actual amount of words to be written. Reader will return a parameter error status in the response frame if a 0 or an incorrect value of WNum is delivered in this field.

ENum:

0x00 ~ 0x0f – ENum represents the length of EPC number. The unit of ENum is word, and the length of EPC should be less than 15 words. In this situation, parameters MaskMen, MaskAdr, MaskLen, MaskData should all be left empty.

0xff – MaskMem, MaskAdr, MaskLen, MaskData should be provided instead of EPC parameters. Reader will return a parameter error status in the response frame if other value is delivered in this field.

EPC: EPC number of the target tag. Length of the EPC depends on the provided EPC number. The unit of EPC number is word. During communication, the most-significant word and the most-significant byte in a word will be transmitted first. It is essential to provide FULL EPC in this command.

Mem: 1 byte, the type of target memory.
  0x00 – reserved memory
  0x01 – EPC memory;
  0x02 – TID memory;
  0x03 – User memory.
All other values are reserved. Reader will return a parameter error status in the response frame if other value is delivered in this field.

WordPtr: 1 byte, the entry address of target.

Wdt: words to be written to tag memory. The amount of words in Wdt must be identical to the value of WNum. The most-significant byte comes first in a word. Words will be written to tag from lower address to higher address according to the order in Data[]. For instance, WordPtr is 0x02, the 1st word in Data[](from left to right) will be written to the address 0x02 in the memory specified by Mem, the 2nd word will then be written to 0x03 etc.

Pwd: 4 bytes, it is the 4 bytes access password of a tag. From left to right, the first two bytes are the high bytes of access password, and the last two bytes are the low bytes. The most-significant bit of a tag 32-bit access password is the most-significant bit in the 1st byte of Pwd (from left to right). Likewise, the least-significant bit of a tag 32-bit access password is the least-significant bit in the 4th (last) byte of Pwd. Access password must be properly provided and will be verified before the write operation. If target memory is not password protected, Pwd can be set to all-zero.

MaskMem: 1 byte, mask area indication.

    0x01 – EPC memory;

    0x02 – TID memory;

    0x03 – User memory.

All other values are reserved, reader will return a parameter error status in the response frame if other value is delivered in this field.

MaskAdr: 2 bytes, entry bit address of the mask, the valid range of MaskAdr is 0 ~ 16383.

MaskLen: 1 byte, bit length of mask (unit: bits).

MaskData: mask data. The length of MaskData equals to MaskLen/8. If MaskLen is not a multiple of 8 integer, the length of MaskData is equal to the int[MaskLen/8]+1. Non-specified lower significant figures should be filled up with 0.

NOTE:

When MaskMem, MaskAdr, MaskLen and MaskData are not provided, full EPC number will be used as mask pattern in inventory.

Response frame:

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

8.2.16   Obtain Monza4QT working parameters

This command is used to obtain the current working parameters of a tag, only valid for **Monza 4QT** tags from **Impinj**.

Command frame:

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

Parameters of Data[]:

ENum	EPC	Pwd	MaskMem	MaskAdr	MaskLen	MaskData
0xXX	variable	4 bytes	0xXX	2 bytes	0xXX	variable

Parameters definition

ENum:

0x00 ~ 0x0f – ENum represents the length of EPC number. The unit of ENum is word, and the length of EPC should be less than 15 words. In this situation, parameters MaskMen, MaskAdr, MaskLen, MaskData should all be left empty.

0xff – MaskMem, MaskAdr, MaskLen, MaskData should be provided instead of EPC parameters. Reader will return a parameter error status in the response frame if other value is delivered in this field.

EPC: EPC number of the target tag. Length of the EPC depends on the provided EPC number. The unit of EPC number is word. During communication, the most-significant word and the most-significant byte in a word will be transmitted first. It is essential to provide FULL EPC in this command.

Pwd: 4 bytes, it is the 4 bytes access password of a tag. From left to right, the first two bytes are the high bytes of access password, and the last two bytes are the low byte. The most-significant bit of a tag 32-bit access password is the most-significant bit in the 1st byte of Pwd (from left to right). Likewise, the least-significant bit of a tag 32-bit access password is the least-significant bit in the 4th (last) byte of Pwd. Access password must be properly provided in the command.

MaskMem: 1 byte, mask area indication.

        0x01 – EPC memory;

        0x02 – TID memory;

        0x03 – User memory.

All other values are reserved, reader will return a parameter error status in the response frame if other value is delivered in this field.

MaskAdr: 2 bytes, entry bit address of the mask, the valid range of MaskAdr is 0 ~ 16383.

MaskLen: 1 byte, bit length of mask (unit: bits).

MaskData: mask data. The length of MaskData equals to MaskLen/8. If MaskLen is not a multiple of 8 integer, the length of MaskData is equal to the int[MaskLen/8]+1. Non-specified lower significant figures should be filled up with 0.

NOTE:

When MaskMem, MaskAdr, MaskLen and MaskData are not provided, full EPC number will be used as mask pattern in inventory.

Response frame:

Len	Adr	reCmd	Status	Data[]		CRC-16	
0x07	0xXX	0x11	0x00	NC	QTcontrol	LSB	MSB
				0x00	1 byte		

Parameter definition

QTcontrol: Working parameters of tag.

bit0: The current mirror page setting.

      0 – private;

      1 – public.

bit1: distance protection setting.

      0 – disabled;

      1 – enabled.

All other values are reserved.

8.2.17 Modify Monza4QT working parameters

The function of this command is to modify the current working parameters of a tag, only valid for **Monza 4QT** tags from **Impinj**.

Command frame:

Len	Adr	Cmd	Data[]	CRC-16	
0xXX	0xXX	0x12	——	LSB	MSB

Parameters of Data[]:

ENum	EPC	QTcontrol1	QTcontrol0	Pwd	MaskMem	MaskAdr	MaskLen	MaskData
0xXX	variable	0x00	0xXX	4 bytes	0xXX	2 bytes	0xXX	variable

Parameter definition

ENum:

0x00 ~ 0x0f – ENum represents the length of EPC number. The unit of ENum is word, and the length of EPC should be less than 15 words. In this situation, parameters MaskMen, MaskAdr, MaskLen, MaskData should all be left empty.

0xff – MaskMem, MaskAdr, MaskLen, MaskData should be provided instead of EPC parameters. Reader will return a parameter error status in the response frame if other value is delivered in this field.

EPC: EPC number of the target tag. Length of the EPC depends on the provided EPC number. The unit of EPC number is word. During communication, the most-significant word and the most-significant byte in a word will be transmitted first. It is essential to provide FULL EPC in this command.

QTcontrol1: 0x00 (Constnat), reserved.

QTcontrol0: working parameters of tag.
bit0: the current mirror page setting.
     0 – private;
     1 – public.
bit1: distance protection setting.
     0 – disabled;
     1 – enabled.
All other values are reserved.

Pwd: 4 bytes, it is the 4 bytes access password of a tag. From left to right, the first two bytes are the high bytes of access password, and the last two bytes are the low bytes. The most-significant bit of a tag 32-bit access password is the most-significant bit in the 1st byte of Pwd (from left to right). Likewise, the least-significant bit of a tag 32-bit access password is the least-significant bit in the 4th (last) byte of Pwd. Access password must be properly provided in the command.

MaskMem: 1 byte, mask area indication.

    0x01 – EPC memory;

    0x02 – TID memory;

    0x03 – User memory.

All other values are reserved, reader will return a parameter error status in the response frame if other value is delivered in this field.

MaskAdr: 2 bytes, entry bit address of the mask, the valid range of MaskAdr is 0 ~ 16383.

MaskLen: 1 byte, bit length of mask (unit: bits).

MaskData: mask data. The length of MaskData equals to MaskLen/8. If MaskLen is not a multiple of 8 integer, the length of MaskData is equal to the int[MaskLen/8]+1. Non-specified lower significant figures should be filled up with 0.

NOTE:

When MaskMem, MaskAdr, MaskLen and MaskData are not provided, full EPC number will be used as mask pattern in inventory.

Response frame:

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

8.2.18   Extended data reading with assigned mask

The function of this command is to read data from reserved memory, EPC memory, TID memory, user memory of tag. Read operation starts from a defined address, and the unit of data is word.

Command frame:

Len	Adr	Cmd	Data[]	CRC-16	
0xXX	0xXX	0x15	——	LSB	MSB

Parameters of Data[]:

Data[]									
ENum	EPC	Mem	WordPtr	Num	Pwd	MaskMem	MaskAdr	MaskLen	MaskData
0xXX	variable	0xXX	2 bytes	0xXX	4 bytes	0xXX	2 bytes	0xXX	Variable

Parameters definition

ENum:

0x00 ~ 0x0f – ENum represents the length of EPC number. The unit of ENum is word, and the length of EPC should be less than 15 words. In this situation, parameters MaskMen, MaskAdr, MaskLen, MaskData should all be left empty.

0xff – MaskMem, MaskAdr, MaskLen, MaskData should be provided instead of EPC parameters. Reader will return a parameter error status in the response frame if other value is delivered in

this field.

EPC: EPC number of the target tag. Length of the EPC depends on the provided EPC number. The unit of EPC number is word. During communication, the most-significant word and the most-significant byte in a word will be transmitted first. It is essential to provide FULL EPC in this command.

Mem: 1 byte, the type of target memory.
  0x00 – reserved memory
  0x01 – EPC memory;
  0x02 – TID memory;
  0x03 – User memory.
All other values are reserved. Reader will return a parameter error status in the response frame if other value is delivered in this field.

WordPtr: 2 bytes, the address of target entry. For instance, 0x0000 represent the read operation starts from 1st word (the first 16-bit memory area), 0x0001 represents operation starts from the second word, etc.

Num: 1 byte, the amount of words to be read in this operation, hence 0x00 is not a valid value for this parameter. Furthermore the value of Num should not exceed 120, i.e. the maximum reading amount is 120 words. Reader will return a parameter error status in the response frame if a 0 or a larger than 120 value is delivered in this field.

Pwd: 4 bytes, it is the 4 bytes access password of a tag. From left to right, the first two bytes are the high bytes of access password, and the last two bytes are the low byte. The most-significant bit of a tag 32-bit access password is the most-significant bit in the 1st byte of Pwd (from left to right). Likewise, the least-significant bit of a tag 32-bit access password is the least-significant bit in the 4th (last) byte of Pwd. Access password will only be used for verification during reserved memory reading operation, the associated target is password protected and the tag access password is non zero. Psw should be set to all-zero or set to the correct access password.

MaskMem: 1 byte, mask area indication.
  0x01 – EPC memory;
  0x02 – TID memory;
  0x03 – User memory.
All other values are reserved, reader will return a parameter error status in the response frame if other value is delivered in this field.

MaskAdr: 2 bytes, entry bit address of the mask, the valid range of MaskAdr is 0 ~ 16383.

MaskLen: 1 byte, bit length of mask (unit: bits).

MaskData: mask data. The length of MaskData equals to MaskLen/8. If MaskLen is not a multiple of 8 integer, the length of MaskData is equal to the int[MaskLen/8]+1. Non-specified lower significant figures should be filled up with 0.

NOTE:

When MaskMem, MaskAdr, MaskLen and MaskData are not provided, full EPC number will be used as mask pattern in inventory.

Response frame:

Len	Adr	reCmd	Status	Data[]	CRC-16	
0xXX	0xXX	0x15	0x00	Word1，Word2,…	LSB	MSB

Parameter definition

Word1, Word2...: the unit of this field is word. Every word contains 2 bytes, most-significant byte first. Word1 is the 1st word from the starting address and the 2nd word is Word 2 etc.

8.2.19 Extended data reading with assigned mask

The function of this command is to write multiple words to reserved memory, TID memory or user memory in one communication cycle.

Command frame:

Len	Adr	Cmd	Data[]	CRC-16	
0xXX	0xXX	0x16	——	LSB	MSB

Parameters of Data[]:

Data[]					
WNum	ENum	EPC	Mem	WordPtr	Wdt
0xXX	0xXX	variable	0xXX	2 bytes	variable
Pwd	MaskMem	MaskAdr	MaskLen	MaskData	
4 bytes	0xXX	2 bytes	0xXX	variable	

Parameter definition

WNum: the amount of words to be written. Every word contains 2 bytes. The value of WNum must be larger than 0 and less or equal to 32, as well as identical to the actual amount of words to be written. Reader will return a parameter error status in the response frame if a 0 or an incorrect value of WNum is delivered in this field.

ENum:

0x00 ~ 0x0f – ENum represents the length of EPC number. The unit of ENum is word, and the length of EPC should be less than 15 words. In this situation, parameters MaskMen, MaskAdr, MaskLen, MaskData should all be left empty.

0xff – MaskMem, MaskAdr, MaskLen, MaskData should be provided instead of EPC parameters. Reader will return a parameter error status in the response frame if other value is delivered in this field.

EPC: EPC number of the target tag. Length of the EPC depends on the provided EPC number. The

unit of EPC number is word. During communication, the most-significant word and the most-significant byte in a word will be transmitted first. It is essential to provide FULL EPC in this command.

MaskMem: 1 byte, mask area indication.
        0x01 – EPC memory;
        0x02 – TID memory;
        0x03 – User memory.
All other values are reserved, reader will return a parameter error status in the response frame if other value is delivered in this field.

WordPtr: 1 byte, the entry address of target.

Wdt: words to be written to tag memory. The amount of words in Wdt must be identical to the value of WNum. The most-significant byte comes first in a word. Words will be written to tag from lower address to higher address according to the order in Data[]. For instance, WordPtr is 0x02, the 1st word in Data[](from left to right) will be written to the address 0x02 in the memory specified by Mem, the 2nd word will then be written to 0x03 etc.

Pwd: 4 bytes, it is the 4 bytes access password of a tag. From left to right, the first two bytes are the high bytes of access password, and the last two bytes are the low byte. The most-significant bit of a tag 32-bit access password is the most-significant bit in the 1st byte of Pwd (from left to right). Likewise, the least-significant bit of a tag 32-bit access password is the least-significant bit in the 4th (last) byte of Pwd. Access password must be properly provided and will be verified before the write operation. If target memory is not password protected, Pwd can be set to all zero.

MaskMem: 1 byte, mask area indication.
        0x01 – EPC memory;
        0x02 – TID memory;
        0x03 – User memory.
All other values are reserved, reader will return a parameter error status in the response frame if other value is delivered in this field.

MaskAdr: 2 bytes, entry bit address of the mask, the valid range of MaskAdr is 0 ~ 16383.

MaskLen: 1 byte, bit length of mask (unit: bits).

MaskData: mask data. The length of MaskData equals to MaskLen/8. If MaskLen is not a multiple of 8 integer, the length of MaskData is equal to the int[MaskLen/8]+1. Non-specified lower significant figures should be filled up with 0.

NOTE:
When MaskMem, MaskAdr, MaskLen and MaskData are not provided, full EPC number will be used as mask pattern in inventory.

Command frame:

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

8.2.20 Inventory with memory buffer

Inventory command is used for inquiring/identifying RFID tags, and stored the inquired tag data into reader memory buffer.

The main distinction between Inventory with or without memory buffer (refer to Chapter 8.2.1) is by using the internal memory buffer, reader can continuously inquired tags during the inventory time. At the end of every inventory time, reader will report the total amount of tags stored in the memory buffer (a tag being accessed multiple times will also increase the amount) as well as the amount of tags inquired in the current inventory. User can access data from the memory buffer via obtain tag data, obtain tag amount or clear memory buffer commands.

Default inventory time is 2s, it can be modified by using reader customised command, "Modify reader inventory time"(refer to Chapter 8.4.4) or perform temporary configuration via optional parameter in the inventory. The valid range of inventory time is from 3*100ms to 255*100ms (the actual responding time may slightly larger than the setting value and this difference will varies from 0 up to 75ms).

NOTE
- An unreasonable short inventory time setting may causes tag inventory failure.
- Buffer will be cleared if an "inventory without memory buffer" command is delivered from host.

Command frame:

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

Parameters of Data[]:

Data[]							
QValue	Session	MaskMem	MaskAdr	MaskLen	MaskData	AdrTID	LenTID
0xXX	0xXX	0xXX	2 bytes	0xXX	variable	0xXX	0xXX

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

Parameters definition

QValue: 1 byte, the original Q-value of the EPC tag inventory, the setting of Q-value should follow the rule: $2^Q \approx$ total amount of tags within the effective field. The range of Q-value is 0 ~ 15, if other value is delivered in this field, reader will return a parameter error status in the response frame.

Session: 1 byte, the Session-value of the EPC tag inventory.

        0x00 – apply S0 as Session value;

        0x01 – apply S1 as Session value;

        0x02 – apply S2 as Session value;

        0x03 – apply S3 as Session value;

        0xff – apply reader smart configuration (only valid in EPC inventory).

All other values are reserved, reader will return a parameter error status in the response frame if other value is delivered in this field.

MaskMem: 1 byte, mask area indication.

        0x01 – EPC memory;

        0x02 – TID memory;

        0x03 – User memory.

All other values are reserved, reader will return a parameter error status in the response frame if other value is delivered in this field.

MaskAdr: 2 bytes, entry bit address of the mask, the valid range of MaskAdr is 0 ~ 16383.

MaskLen: 1 byte, bit length of mask (unit: bits).

MaskData: mask data. The length of MaskData equals to MaskLen/8. If MaskLen is not a multiple of 8 integer, the length of MaskData is equal to the int[MaskLen/8]+1. Non-specified lower significant figures should be filled up with 0.

AdrTID: initial word address of inventory TID memory. If command delivered this parameter and LenTID at the same frame, the mode of inventory should be TID, not EPC.

LenTID: data length for TID inventory operation, the valid range of LenTID is 0 ~ 15.
All other values are reserved, and reader will return a parameter error status in the response frame if other value is delivered in this field. If command delivered this parameter and AdrTID, the mode of inventory should be TID, not EPC.

Target (optional parameter): 1 byte, the Target value of EPC tag inventory.

            0x00 – apply A as Target value;

            0x01 – apply B as Target value.

All other values are reserved, reader will return a parameter error status in the response frame if other value is delivered in this field.

Ant (optional parameter): 1 byte, antenna selection for the current inventory.

            0x80 – antenna 1;

            0x81 – antenna 2;

            0x82 – antenna 3;

            0x83 – antenna 4.

ScanTime (optional parameter): 1 byte, the inventory time configuration for the current inventory. Reader will set the maximum operation time as ScanTime*100ms.

NOTE:

1. When MaskMem, MaskAdr, MaskLen and MaskData are not provided, no mask pattern will be involved in inventory

2. Target, Ant and ScanTime are optional parameters, all three parameters must be delivered in one command frame. Reader will apply default setting for these parameters, until all three parameters setting are being properly deliver from host, the new settings will then become effective for following inventory.

Response frame:

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

Parameter definition

BufferCount: 2 bytes, the total amount of tag stored in the memory buffer, tags with identical EPC/TID data will be treated as one tag. BufferCount is the sum of tag amount from multiple inventories, until the memory buffer is being cleared.

TagNum: 2 bytes, the amount of tag inquired in the current inventory, a tag being accessed multiple times will also increase the amount.

8.2.21   Mix inventory

Inventory command is used for inquire RFID tags with corresponding protocol within the effective field, and obtain specific tag information once the tag EPC number is inquired.

According to different circumstances, user can modify the setting of maximum operation time (inventory time). Reader will return a inventory result within the pre-defined inventory time. If the reader fails to complete inventory processes for all the tags in the effective field within the predefined inventory time, reader will not perform further inventory after inventory time is exceed. Reader will report all the already inquired tags, as well as the current (uncompleted) inventory status to host. Reader will then wait for the next command from host.

Default inventory time is 2s, it can be modified by using reader customised command "modify reader inventory time" (refer to chapter 8.4.4). The valid range of inventory time is from 3*100ms to 255*100ms (the actual responding time may slightly larger than the setting value and this difference will varies from 0 up to 75ms).
Note: an unreasonable short inventory time setting may cause tag inventory failure.

NOTE:

An unreasonable short inventory time setting may cause tag inventory failure.

Command frame:

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

Parameters of Data[]:

Data[]					
QValue	Session	MaskMem	MaskAdr	MaskLen	MaskData
0xXX	0xXX	0xXX	2 bytes	0xXX	variable

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

Parameters definition

QValue: 1 byte.

bit7: Statistic data packet flag.

    0 – After inventory，DO NOT deliver statistic data packet of inventory process;

    1 – After inventory，deliver statistic data packet of inventory process

bit6 ~ bit0: the original Q-value of the EPC tag inventory, the setting of Q-value should follow the rule: $2^Q \approx$ total amount of tags within the effective field. The range of Q-value is 0 ~ 15, if other value is delivered in this field, reader will return a parameter error status in the response frame.

Session: 1 byte, the Session-value of the EPC tag inventory.

    0x00 – apply S0 as Session value;

    0x01 – apply S1 as Session value;

    0x02 – apply S2 as Session value;

    0x03 – apply S3 as Session value;

    0xff – apply reader smart configuration (only valid in EPC inventory).

All other values are reserved, reader will return a parameter error status in the response frame if other value is delivered in this field.

MaskMem: 1 byte, mask area indication.

    0x01 – EPC memory;

    0x02 – TID memory;

    0x03 – User memory.

All other values are reserved, reader will return a parameter error status in the response frame if other value is delivered in this field.

MaskAdr: 2 bytes, entry bit address of the mask, the valid range of MaskAdr is 0 ~ 16383.

MaskLen: 1 byte, bit length of mask (unit: bits).

MaskData: mask data. The length of MaskData equals to MaskLen/8. If MaskLen is not a multiple of 8 integer, the length of MaskData is equal to the int[MaskLen/8]+1. Non-specified lower significant figures should be filled up with 0.

ReadMem: 1 byte, the type of target memory.

        0x00 – reserved memory;

        0x01 – EPC memory;

        0x02 – TID memory;

        0x03 – user memory.

All other values are reserved, reader will return a parameter error status in the response frame if other value is delivered in this field.

ReadAdr: 2 bytes, the entry address of target, most-significant byte first. For instance, 0x0000 represent the read operation starts from 1st word (the first 16-bit memory area), 0x0001 represents operation starts from the 2nd word, etc.

ReadLen: 1 byte, the amount of words to be read in this operation, the minimum length is 1 word and the maximum is 120 words. 0x00 is not a valid value for this parameter; furthermore the value of Num should not exceed 120. Reader will return a parameter error status in the response frame if a 0 or a larger than 120 value is delivered in this field.

Pwd: 4 bytes, it is the 4 bytes access password of a tag. From left to right, the first two bytes are the high bytes of access password, and the last two bytes are the low bytes. The most-significant bit of a tag 32-bit access password is the most-significant bit in the 1st byte of Pwd (from left to right). Likewise, the least-significant bit of a tag 32-bit access password is the least-significant bit in the 4th (last) byte of Pwd. Access password will only be used for verification during reserved memory reading operation, when the associated target memory is password protected and the tag access password is non-zero. Otherwise Psw should be set to all zero or set to the correct access password.

Target (optional parameter): 1 byte, the Target value of EPC tag inventory.

        0x00 – apply A as Target value;

        0x01 – apply B as Target value.

All other values are reserved, reader will return a parameter error status in the response frame if other value is delivered in this field.

Ant (optional parameter): 1 byte, antenna selection for the current inventory.

        0x80 – antenna 1;

        0x81 – antenna 2;

        0x82 – antenna 3;

        0x83 – antenna 4.

ScanTime (optional parameter): 1 byte, the inventory time configuration for the current inventory. Reader will set the maximum operation time as ScanTime*100ms.

NOTE:

1. When MaskMem, MaskAdr, MaskLen and MaskData are not provided, no mask pattern will be

involved in inventory

2. Target, Ant and ScanTime are optional parameters, all three parameters must be delivered in one command frame. Reader will apply default setting for these parameters, until all three parameters setting are being properly deliver from host, the new settings will then become effective for following inventory.

(1) Response status is 0x26, the response should be as following:

Len	Adr	reCmd	Status	Data[]			CRC-16	
				Ant	ReadRate	TotalCount		
0xXX	0xXX	0x19	0xXX	0xXX	2 bytes	4 bytes	LSB	MSB

Parameters definition
Status: the status of response, detail description is shown in the following table

Status	Description
0x26	After inventory, deliver statistic data of the current inventory process

Ant: indicates which antenna had inquired a tag. For example, 0x04 is 0000 0100 in binary, this indicates Antenna 3 had inquired this specific tag. For 0x08, it is 0000 1000 in binary, then it indicates Antenna 4 had inquired tag information.

ReadRate: tag identification rate for the current inventory (time of successful identification / sec), a tag being indentified multiple times will also increase the time of successful identification.

TotalCount: the total amount of tag detected in the current inventory, a tag being accessed multiple times will also increase the total amount.

(2) Response status is not 0x26, the response should be as following:

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

Parameters definition
Status: the status of response, detail description is shown in the following table

Status	Description
0x01	Operation completed, reader will report all inquired tags information to host
0x02	Inventory timeout, operation is aborted. reader will report all the already inquired tags to host
0x03	Reader is not able to response all the data in a single frame, further data will be transmitted in the following frames.

0x04	Reader only completed parts of the inventory but run out of memory space due to the amount of tags. Reader will report all the already inquired tags as well as this status value to host.
0xF8	Antenna error detected, the current antenna might be disconnected.

Ant: indicates which antenna had inquired a tag. For example, 0x04 is 0000 0100 in binary, this indicates Antenna 3 had inquired this specific tag. For 0x08, it is 0000 1000 in binary, then it indicates Antenna 4 had inquired tag information.

Num: the amount of tag information data packets included in this response.

Data Packet: inquired tag data, Packet-1 is data of the 1st packet, Packet-2 is data of the 2nd packet etc. The format of a typical packet is shown below:

Packet			
PacketParam	Len	Data	RSSI
0xXX	0xXX	variable	0xXX

Parameters data packet:
PacketParam: 1 byte, parameters of this packet.
bit7: the type indicator of this data packet.

    0 – this data packet contains tag EPC number;

    1 – this data packet contains inquired tag data (the EPC number of this tag is delivered in the last data packet).

bit6 ~ bit0: the serial number of the data packet. The range of the serial number is 0 ~ 127. At the beginning of ever mix inventory, the packet serial number will restart from 0, and increase for ever uploaded data packet. Once serial number reaches the maximum value 127, it will recount again from 0.

Len: 1 byte, the length of data in this packet.

Data: the EPC number or the inquired data from a specific area of a tag. The unit of **EPC C1 G2** tag data is word. During communication, the most-significant word and the most-significant byte in a word will be transmitted first.

RSSI: 1 byte, the reader signal strength at the time when the tag is inquired.

NOTE:
Data packet will be uploaded according to EPC inquired order. For every tag, reader will firstly upload the tag EPC in the initial data packet, further tag data will be uploaded in the second data packet. These two packets will have sequential serial number.

In the case when reader fails to read data of a tag after uploaded the EPC packet, reader will not upload any tag data packet. Reader will continue to inquire the next tag and restart the normal mix inventory process.

8.2.22 Inventory with EPC number

The function of this command is to inquire tag with specific EPC. Reader will only response data from the tag with corresponding EPC. All other tags with different EPC will be ignored.

Command frame:

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

Parameters of Data[]:

Data[]			
MatchType	MatchLen	MatchOffset	EPCData
0xXX	2 bytes	2 bytes	variable

Parameter definition
MatchType: EPC number matching type.

    0 – inquire tag with corresponding EPC;
    1 – inquire all other tags with different EPC.

All other values are reserved, reader will return a parameter error status in the response frame if other value is delivered in this field.

MatchLen: 2 bytes, most-significant byte first, the bit length of the defined EPC number. The range of MatchLen is 1 ~ 196 bits.

MatchOffset: 2 bytes, most-significant byte first. The entry address of the defined EPC (unit: bits). The range of MatchOffset is 0 ~ 495 bits.
NOTE:
The sum of **MatchLen** and **MatchOffset** should not exceed 496 bits**.** Reader will return a parameter error status in the response frame if incorrect value is delivered in this field.

EPCData: the defined EPC number data. The length of EPCData equals to MatchLen/8. If MatchLen is not a multiple of 8 integer, the length of EPCData is equal to the int[MatchLen /8]+1. Non-specified lower significant figures should be filled up with 0.

Response frame:

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

Parameters definition
Status: the status of response, detail description is shown in the following table

Status	Description
0x01	Operation completed, reader will report all inquired tags information to host
0x02	Inventory timeout, operation is aborted. reader will report all the already inquired tags to host
0x03	Reader is not able to response all the data in a single frame, further data will be transmitted in the following frames.
0xF8	Antenna error detected, the current antenna might be disconnected.

Ant: indicates which antenna had inquired a tag. For example, 0x04 is 0000 0100 in binary, this indicates Antenna 3 had inquired this specific tag. For 0x08, it is 0000 1000 in binary, then it indicates Antenna 4 had inquired tag information.

Num：the amount of tag EPC included in this response.

EPC ID: inquired EPC/TID data. For instance, EPC-1 is the EPC/TID length + EPC number/TID data + **RSSI value** of the first tag etc. The RSSI and EPC length values are one byte parameters. The unit of EPC C1 G2 data is word. During communication, the most-significant word and the most-significant byte in a word will be transmitted first.

8.2.23   QT inventory

This command is used to inquiry the private EPC number of a Monza4QT tag with public mirroring. The command seeks RFID tags with corresponding protocol. In order to process further operation on a new tag with unknown EPC, user should firstly obtain tag EPC number by using inventory command.

According to different circumstances, user can modify the setting of maximum operation time (inventory time). Reader will return an inventory result within the predefined inventory time. If the reader fails to complete inventory processes for all the tags in the effective field within the predefined inventory time, reader will not perform further inventory after inventory time is exceed. Reader will report all the already inquired tags, as well as the current (uncompleted) inventory status to host. Reader will then wait for the next command from host.

Default inventory time is 1s, it can be modified by using reader customised command "modify reader inventory time" (refer to chapter 8.4.4). The valid range of inventory time is from 3*100ms to 255*100ms (the actual responding time may slightly larger than the setting value and this difference will varies from 0 up to 75ms).

Note: an unreasonable short inventory time setting may cause tag inventory failure.

Command frame:

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

Parameters of Data[]:

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

Parameters definition

QValue: 1 byte.

bit7: Statistic data packet flag.

    0 – After inventory，DO NOT deliver statistic data packet of inventory process;

    1 – After inventory，deliver statistic data packet of inventory process

bit6 ~ bit0: the original Q-value of the EPC tag inventory, the setting of Q-value should follow the rule: $2^Q \approx$ total amount of tags within the effective field. The range of Q-value is 0 ~ 15, if other value is delivered in this field, reader will return a parameter error status in the response frame.

Session: 1 byte, the Session-value of the EPC tag inventory.

        0x00 – apply S0 as Session value;

        0x01 – apply S1 as Session value;

        0x02 – apply S2 as Session value;

        0x03 – apply S3 as Session value;

        0xff – apply reader smart configuration (only valid in EPC inventory).

All other values are reserved, reader will return a parameter error status in the response frame if other value is delivered in this field.

Target (optional parameter): 1 byte, the Target value of EPC tag inventory.

                0x00 – apply A as Target value;

                0x01 – apply B as Target value.

All other values are reserved, reader will return a parameter error status in the response frame if other value is delivered in this field.

Ant (optional parameter): 1 byte, antenna selection for the current inventory.

                0x80 – antenna 1;

                0x81 – antenna 2;

                0x82 – antenna 3;

                0x83 – antenna 4.

All other values are reserved, and reader will return a parameter error status in the response frame if other value is delivered in this field.

ScanTime (optional parameter): 1 byte, the inventory time configuration for the current inventory. Reader will set the maximum operation time as ScanTime*100ms.

NOTE:

1. Target, Ant and ScanTime are optional parameters, all three parameters must be delivered in one command frame. Reader will apply default setting for these parameter, until all three parameters

setting are being properly deliver from host, the new settings will then become effective for following inventory.

(1) Response status is 0x26, the response should be as following:

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

Parameters definition

Status: the status of response, detail description is shown in the following table,

Status	Description
0x26	After inventory, deliver statistic data of the last inventory process

Ant: indicates which antenna had inquired a tag. For example, 0x04 is 0000 0100 in binary, this indicates Antenna 3 had inquired this specific tag. For 0x08, it is 0000 1000 in binary, then it indicates Antenna 4 had inquired tag information.

ReadRate: tag identification rate for the current inventory (time of successful identification / sec), a tag being indentified multiple times will also increase the time of successful identification.

TotalCount: the total amount of tag detected in the current inventory, a tag being accessed multiple times will also increase the total amount.

(2) Response status is not 0x26, the response should be as following:

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

Parameters definition

Status: the status of response, detail description is shown in the following table,

Status	Description
0x01	operation completed, reader will report all inquired tags information to host
0x02	inventory timeout, operation is aborted. reader will report all the already inquired tags to host
0x03	reader is not able to response all the data in a single frame, further data will be transmitted in the following frames.
0x04	reader only completed parts of the inventory but run out of memory space due to the amount of tags. Reader will report all the already inquired tags as well as this status value to host.

Ant: indicates which antenna had inquired a tag. For example, 0x04 is 0000 0100 in binary, this indicates Antenna 3 had inquired this specific tag. For 0x08, it is 0000 1000 in binary, then it indicates Antenna 4 had inquired tag information.

Num: the amount of EPC/TID included in this response.

EPC ID: inquired EPC/TID data. For instance, EPC-1 is the EPC/TID length + EPC number/TID data + **RSSI value** of the first tag etc. The RSSI and EPC length values are one byte parameters. The unit of EPC C1 G2 data is word. During communication, the most-significant word and the most-significant byte in a word will be transmitted first.

8.3   18000-6B Commands

8.3.1   Single tag inventory

The function of this command is to inquire a single tag. If multiple tags are placed within the effective field, reader may fail to inquire any tag.

Command frame:

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

Response frame:

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

Parameters definition

Ant: indicates which antenna had inquired a tag. For example, 0x04 is 0000 0100 in binary, this indicates Antenna 3 had inquired this specific tag. For 0x08, it is 0000 1000 in binary, then it indicates Antenna 4 had inquired tag information.

ID: 10 bytes, the 1st byte is the length of UID, 0x08. The 2nd ~ 9th byte is the tag UID number, least-significant byte first. The 10th byte is RSSI.

8.3.2   Inquire tags according specified condition

The function of this command is to inquire tags according to specified condition.

Command frame:

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

Parameters definition

Condition: the condition for inventory;

0x00 – equal to the reference;
0x01 – no equal to the reference;
0x02 – larger than the reference
0x03 – smaller than the reference

Address: address of the comparing data

Mask: mask, specify the data for comparison.

Word_data: the value of reference. Every bit in mask is corresponds to a byte in Word_data. The most-significant bit (bit7) corresponds to the 1st byte in Word_data (from left to right). Consequently, the least- significant bit (bit0) corresponds to the last byte in Word_data (from left to right). Word_data is the reference data for comparison with data in tag starts from the location stated in Address. The 1st byte of Word_data will be compare with the data store in Address, the last byte of Word_data will be compare with the data store in Address+7. Set the byte corresponding bit of Mask to 1, reader will perform comparison on that particular byte. Set the bit to 0, no comparison will be performed on that particular byte.

Response frame:

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

Parameters definition

Status: the status of response, detail description is shown in the following table

Status	Description
0x15	Operation completed, reader will report all inquired tags information to host.
0x16	Inventory timeout, operation is aborted. Reader will report all the already inquired tags to host.
0x17	Reader is not able to response all the data in a single frame, further data will be transmitted in the following frames.
0x18	Reader only completed parts of the inventory but run out of memory space due to the amount of tags. Reader will report all the already inquired tags as well as this status value to host..
0xF8	Antenna error detected, the current antenna might be disconnected.

Ant: indicates which antenna had inquired a tag. For example, 0x04 is 0000 0100 in binary, this indicates Antenna 3 had inquired this specific tag. For 0x08, it is 0000 1000 in binary, then it indicates Antenna 4 had inquired tag information.

Num: the amount of UID included in this response.

Data[]: UID of the tag. The length of every UID data block is 10 bytes. The 1st byte is the length value of UID number, i.e. 0x08. The 2nd ~ 9th bytes are the tag UID number, least-significant byte first. The 10th byte is the RSSI value. For Num = 0, i.e. no UID data is provided, Data[] is empty.

8.3.3 Reader data

The function of this command is to read multiple bytes from a specific address.

Command frame:

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

Parameters definition
Address: the entry address of target. The valid value range of Address is 0 ~ 223. Reader will return a parameter error status in the response frame if incorrect address is delivered.

Num: the amount of words will be read in this operation. The valid value range of Num is 1 ~ 32. If the sum of Address and Num is larger than 224, Num is equal to 0 or larger than 32, return a parameter error status in the response frame.

ID: the ID of the target tag, 8 bytes, least significant byte first.

Response frame:

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

Parameter definition
Data: inquired data from tag, least-significant byte first.

8.3.4 Write data

The function of this command is to write multiple bytes to a specific tag.

Command frame:

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

Parameter definition
Address: 1 byte, the address of the target byte. The range of address is 8 ~ 223. Reader will return a parameter error status in the response frame if other value is delivered in this field.

ID: 8 bytes, the ID number of the target tag, the least-significant byte first.

Wdata: the data to be written to the tag. The length of Wdata should not exceed 32 bytes. The most-significant byte will be written to the lowest byte from entry stated in Address. If the length of Wdata is 0 (no data) or exceed 32, reader will return a parameter error status in the response frame. Besides, if the sum of Address and Wdata exceeds 224, reader will also return parameter error.

Response frame:

Len	Adr	reCmd	Status	Data[]	CRC-16	
0x05	0xXX	0x53	0x00	——	LSB	MSB

8.3.5   Obtain lock status

The function of this command is to obtain the lock status of a specific byte.

Command frame:

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

Parameters definition
Address: 1 byte, the address of the target byte. The range of address is 0 ~ 223. Reader will return a parameter error status in the response frame if other value is delivered in this field.

ID: 8 bytes, the ID number of the target tag. The least-significant byte should be transmitted first.

Response frame:

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

Parameter definition
LockState: 0x00: the byte is unlocked;
          0x01: the byte is locked.

8.3.6   Lock byte

The function of this command is to lock a specific byte in a tag.

Command frame:

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

Parameters definition
Address: 1 bytes, the address of the target byte. the range of address is 8 ~ 223. Reader will return a parameter error status in the response frame if other value is delivered in this field.

ID: 8 bytes, the ID number of the target tag. The least-significant byte should be transmitted first.

Response frame:

Len	Adr	reCmd	Status	Data[]	CRC-16

| 0x05 | 0xXX | 0x55 | 0x00 | —— | LSB | MSB |

8.4 Reader customised commands

8.4.1 Obtain reader information

The function of this command is to obtain reader information, including reader address, firmware version, reader model code, supported protocols, working frequency band, RF power, inventory time, buzzer status, GPIO for notification etc.

Command frame:

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

Response frame:

Len	Adr	reCmd	Status	Data[]	CRC-16	
0x11	0xXX	0x21	0x00	Version，Type，Tr_Type，dmaxfre，dminfre，Power，Scntm，Ant，BeepEn，OutputRep，CheckAnt	LSB	MSB

Parameters of Data[]:

Parameters	Length (bytes)	Description
Version	2	Firmware version, the high byte states the main version number and the low byte states the subversion number.
Type	1	Reader model code, 0x8B is RRU2881ADV.
Tr_Type	1	Supported prototypes. bit1 = 1: supports 18000-6C. bit0 = 1: supports 18000-6B. All other bits are reserved.
dmaxfre	1	bit7 ~ bit6: frequency band configuration; bit5 ~ bit0: maximum frequency point.
Dminfre	1	bit7 ~ bit6: frequency band configuration; bit5 ~ bit0: minimum frequency point.
Power	1	Output RF power, range from 0 to 30.
Scntm	1	Inventory time. Reader will respond the inventory command delivered from host within this specific inventory time.
Ant	1	Antenna configuration.
BeepEn	1	Buzzer status information.
OutputRep	1	GPIO status for notification

CheckAnt	1	Antenna check configuration 0: antenna check off; 1: antenna check on.

Frequency band configuration table

MaxFre(bit7)	MaxFre(bit6)	MinFre(bit7)	MinFre(bit6)	FreqBand
0	0	0	0	Reserved
0	0	0	1	Chinese band2
0	0	1	0	US band
0	0	1	1	Korean band
0	1	0	0	EU band
0	1	0	1	Reserved
0	1	1	0	Ukraine band
0	1	1	1	Peru band
1	0	0	0	Chinese band1
1	1	0	0	US band3
...	...	...	...	...
1	1	1	1	Reserved

8.4.2 Modify working frequency

The function of this command is to select frequency band, modify maximum and minimum frequency points.

Command frame:

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

Parameters definition
MaxFre: 1 byte.
bit7 ~ bit6: frequency band configuration;
bit5 ~ bit0: maximum frequency point.

MinFre: 1 byte.
bit7 ~ bit6: frequency band configuration;
bit5 ~ bit0: minimum frequency point.

NOTE:
Maximum frequency point must be larger or equal the minimum frequency point. Reader will return a parameter error status in the response frame if other value is delivered in this field.

Frequency band configuration table

MaxFre(bit7)	MaxFre(bit6)	MinFre(bit7)	MinFre(bit6)	FreqBand
0	0	0	0	Reserved
0	0	0	1	Chinese band2
0	0	1	0	US band
0	0	1	1	Korean band
0	1	0	0	EU band
0	1	0	1	Reserved
0	1	1	0	Ukraine band
0	1	1	1	Peru band
1	0	0	0	Chinese band1
1	1	0	0	US band3
...	...	...	...	...
1	1	1	1	Reserved

Response frame:

Len	Adr	reCmd	Status	Data[]	CRC-16	
0x05	0xXX	0x22	0x00	——	LSB	MSB

Formulae for different frequency bands:

Chinese band2: $Fs = 920.125 + N * 0.25$ (MHz) where $N \in [0, 19]$.

US band: $Fs = 902.75 + N * 0.5$ (MHz) where $N \in [0,49]$.

Korean band: $Fs = 917.1 + N * 0.2$ (MHz) where $N \in [0, 31]$.

EU band: $Fs = 865.1 + N*0.2$ (MHz) where $N \in [0, 14]$.

Ukraine band: $Fs = 868.0 + N*0.1$ (MHz) where $N \in [0, 6]$.

Peru band: $Fs = 916.2 + N*0.9$ (MHz) where $N \in [0, 11]$.

US band3: $Fs = 902 + N * 0.5$ (MHz) where $N \in [0,52]$.

Chinese band1: $Fs = 840.125 + N * 0.25$ (MHz) where $N \in [0, 19]$.

8.4.3   Modify reader address

Command frame:

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

Parameter definition

Adr: new address setting of reader. 0xFF is not a valid address, reader will return a parameter error status in the response frame if 0xFF is delivered in this field.

Response frame:

Len	Adr	reCmd	Status	Data[]	CRC-16

0x05	0xXX	0x24	0x00	——	LSB	MSB

NOTE:

Reader will response this command with the ORIGINAL address.

8.4.4 Modify reader inventory time

Command frame:

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

Parameter definition

Scantime: inventory time. Reader will modify the maximum response time according to user defined value (3*100ms ~ 255*100ms), and reader will apply this new setting for future inventories. Default setting of Scantime is 0x14 (corresponding to 20*100ms). Valid setting of Scantime is 0x03 ~ 0xff (corresponding to 3*100ms ~ 255*100ms).

NOTE: the actual responding time may slightly larger than the setting value and this difference will varies from 0 up to 75ms. If user delivers 0x00 to 0x02 as Scantime value in the command, reader will reset to inventory time setting to default value 0x14 (corresponding to 20*100ms).

Response frame:

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

8.4.5 Modify serial baud rate

The function of this command is to modify baud rate for the serial port.

Command frame:

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

Parameters definition

baudrate: the new baud rate setting, options of baudrate is 0/1/2/5/6 (refer to the following table for proper baud rate), all other values are reserved.

baudrate configuration table

baudrate value	Actual baud rate
0	9600bps
1	19200 bps
2	38400 bps

| 5 | 57600 bps (default) |
| 6 | 115200 bps |

Response frame:

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

NOTE:

Response will be delivered using the ORITINAL baud rate setting. The new baud rate setting will take effect in the NEXT COMMUNICATION.

8.4.6 Modify RF power

The function of this command is to modify the RF power of reader. The valid value of this parameter is 0 ~ 30. For setting of 30, the output power is approximately 1W.

Command frame:

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

Parameter definition

Pwr: the RF power parameter.

Response frame:

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

8.4.7 Buzzer/LED control

The function of this command is to control the TAG LED and buzzer to perform specific actions.

Command frame:

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

Parameters definition

ActiveT: TAG LED and buzzer switch ON time (ActiveT*50ms). The range of ActiveT is 0 ~ 255. Default setting is 0.

SilentT: TAG LED and buzzer switch OFF time (SilentT *50ms). The range of SilentT is 0 ~ 255. Default setting is 0.

Times: TAG LED and buzzer action time, the range of Times is 0 ~ 255. Default setting is 0.

Response frame:

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

8.4.8   Modify reader working mode

The function of this command is to switch reader working mode. Reader supports 3 different modes: answer mode, auto mode (including trigger mode) and real time inventory mode.

In auto mode, reader will accept commands from host, but reader will only execute the reader customised commands. If reader receives other commands from host, reader will response 0xFE as status in the response field and will not execute the command.

For real time inventory mode, reader will only response to 3 commands:
1. obtain reader information (refer to Chapter 8.4.1);
2. modify reader working mode(refer to Chapter 8.4.8)
3. obtain auto-mode parameters(refer to Chapter 8.4.9)

Command frame:

Len	Adr	Cmd	Data[]	CRC-16	
			Read_mode		
0x05	0xXX	0x35	0xXX	LSB	MSB

Parameters definition
Read_mode: working mode selection, refer to the following table

bit2	bit1	bit0	Working mode
0	0	0	Answer mode
0	0	1	Auto mode
0	1	0	Trigger mode(low level active)
0	1	1	Trigger mode(high level active)
1	1	0	Real time inventory mode

All other bit are reserved, defaults values are 0.

Response frame:

Len	Adr	reCmd	Status	Data[]	CRC-16	
0x05	0xXX	0x35	0x00	——	LSB	MSB

Output format in Auto mode
1. Tag inventory:

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

Parameters of Data[]:

Data[]				
DiscTime	LastTime	Count	Ant	EPC-ID
4 bytes	4 bytes	2 bytes	0xXX	variable

Parameters definition

DiscTime: the timestamp of the first tag detection.

DiscTime					
Year	Month	Date	Hour	Minute	Second
bit31 ~ bit26	bit25 ~ bit22	bit21 ~ bit17	bit16 ~ bit12	bit11 ~ bit6	bit5 ~ bit0

Year – 6 bits, valid range is 0 ~ 63, i.e. 2000 ~ 2063.

Month – 4 bits, valid range is 1 ~ 12.

Date – 5 bits, valid range is 1 ~ 31.

Hour – 5 bits, valid range is 0 ~ 23.

Minute – 6 bits valid range is 0 ~ 59.

Second – 6 bits, valid range is 0 ~ 59.

LastTime: the timestamp of the last tag detection.

LastTime					
Year	Month	Date	Hour	Minute	Second
bit31 ~ bit26	bit25 ~ bit22	bit21 ~ bit17	bit16 ~ bit12	bit11 ~ bit6	bit5 ~ bit0

Year – 6 bits, valid range is 0 ~ 63, i.e. 2000 ~ 2063.

Month – 4 bits, valid range is 1 ~ 12.

Date – 5 bits, valid range is 1 ~ 31.

Hour – 5 bits, valid range is 0 ~ 23.

Minute – 6 bits valid range is 0 ~ 59.

Second – 6 bits, valid range is 0 ~ 59.

Count: the total detected times for a particular tag between DiscTime and LastTime.

Ant: indicates which antenna had inquired the tag. For example, 0x05 is 0101 in binary, this indicates Antenna 3 and Antenna 1.

EPC-ID: the 1st byte represents the length of EPC/UID number. EPC/UID number data starts from the second byte.

2. EAS check:

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

Close relay for 100ms, once EAS is detected.

Output format in real time inventory mode:

Once reader is set to real time inventory mode, reader will perform auto inventory according to predefined configuration.

If a tag is inquired and the tag matches the predefined condition, reader will automatically upload data in the following format:

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

Status: the status of response, detail description is shown in the following table

Status	Description
0x00	Detected appropriate tag, reader will also report the detected tag data.
0x28	No appropriate tag detected within the heartbeat packet time interval, reader will upload heartbeat packet.

(1) Response status is 0x00, parameters of Data[] are shown as below,

Data[]			
Ant	Len	EPC/TID	RSSI
0xXX	0xXX	N bytes	0xXX

Parameters definition
Ant: indicates which antenna had inquired the tag. For example, 0x05 is 0101 in binary, this indicates Antenna 3 and Antenna 1.

Len: 1 byte, the byte length of the EPC/TID.

EPC/TID: EPC number/TID data of tag, the length of data should identical with Len. The unit of EPC C1 G2 data is word. Every tag EPC number or TID data is the most-significant word and the most-significant byte in a word first.

RSSI: 1 byte, the reader signal strength at the time when the tag is inquired.

(2) Response status is 0x28, parameters of Data[] are shown as below

Data[]		
PacketNo	AntStatus	TotalCount
4 bytes	4 bytes	4 bytes

Parameters definition
PacketNo: heartbeat serial number. 4 bytes, most-significant byte first.
Serial number will increase for ever heartbeat packet uploading operation. If heartbeat serial number exceeds the maximum 4 bytes value, the serial number will recount again from 0.

AntStatus: the current status of 4 antennas, queued from 1 to 4 according to byte order.

0x00 – target antenna is idle, not a effective inventory antenna

0x01 – target antenna is working properly;

0x02 – target antenna is disconnected.

All other values are reserved.

TotalCount: the total amount of tag inquired since the beginning of the current auto-inventory. A tag being indentified multiple times will also increase the value of TotalCount. 4 bytes, with most-significant byte first. If total amount of inquired tag exceeds maximum 4 bytes value, TotalCount will recount again from 0.

8.4.9   Obtain auto-mode parameters

The function of this command is to obtain the parameters of auto-mode.

Command frame:

Len	Adr	Cmd	Data[]	CRC-16	
0x04	0xXX	0x36	——	LSB	MSB

Response frame:

Len	Adr	reCmd	Status	Data[]	CRC-16	
0x32	0xXX	0x36	0x00	Read_mode, Accuracy, RepCondition, RepPauseTime, ReadPauseTim, TagProtocol, MaskMem, MaskAdr, MaskLen, MaskData, TriggerTime, AdrTID, LenTID	LSB	MSB

Parameter definition

Read_mode: 1 byte, working mode information

Accuracy: 1 byte, the accuracy parameter of EAS check in auto-mode.

RepCondition, **RepPauseTime**: 1 byte respectively, the parameter of reader answering form in auto-mode.

ReadPauseTim: 1 byte, time break between two inventories.

TagProtocol: 1 byte, tag type for auto-mode inventory.

MaskMem, MaskAdr, MaskLen, MaskData: mask condition for G2 tag inventory in auto-mode. MaskMem and MaskLen are 1 byte long respectively. MaskAdr is 2 bytes long, most-significant byte first. MaskData has constant length of 32 bytes, fill the over MaskLen value content with zero.

TriggerTime: 1 byte, the effective trigger time in trigger mode.

AdrTID: 1 byte, initial word address for TID memory read operation.

LenTID: 1 byte, data length for the TID read operation.

8.4.10   Modify EAS check accuracy and notification configuration

The function of this command is to modify the accuracy of EAS check in auto-mode.

Command frame:

Len	Adr	Cmd	Data[]	CRC-16	
			Accuracy		
0x05	0xXX	0x37	0xXX	LSB	MSB

Parameter definition
Accuracy:
bit7: 1 – close relay for 100ms once EAS is detected in auto-mode;
     0 – relay remains in current state.
bit6 ~ bit0: the valid range is 0 ~ 8, lower value represent higher sensitivity but lower accuracy.
          Default setting is 8, i.e. highest accuracy and lowest sensitivity.

Response frame:

Len	Adr	reCmd	Status	Data[]	CRC-16	
0x05	0xXX	0x37	0x00	——	LSB	MSB

8.4.11   Modify mask configuration

The function of this command is to modify G2 tag inventory condition in **auto-mode**.

Command frame:

Len	Adr	Cmd	Data[]				CRC-16	
			MaskMem	MaskAdr	MaskLen	MaskData		
0xXX	0xXX	0x3b	0xXX	2Bytes	0xXX	variable	LSB	MSB

Parameters definition
MaskMem: 1 byte, mask area indication.
          0x01 – EPC memory;
          0x02 – TID memory;
          0x03 – User memory.
All other values are reserved, reader will return a parameter error status in the response frame if other value is delivered in this field.

MaskAdr: 2 bytes, entry bit address of the mask, the valid range of MaskAdr is 0 ~ 16383.

MaskLen: 1 byte, bit length of mask (unit: bits).

MaskData: mask data. The length of MaskData equals to MaskLen/8. If MaskLen is not a multiple of 8 integer, the length of MaskData is equal to the int[MaskLen/8]+1. Non-specified lower significant figures should be filled up with 0.

Response frame:

Len	Adr	reCmd	Status	Data[]	CRC-16	
0x05	0xXX	0x3b	0x00	——	LSB	MSB

8.4.12 Modify answering form configuration

The function of this command is to modify reader answering form in **auto-mode**.

Command frame:

Len	Adr	Cmd	Data[]		CRC-16	
			RepCondition	RepPauseTime		
0x06	0xXX	0x3c	0xXX	0xXX	LSB	MSB

Parameters definition

RepCondition: options for answering form in auto-mode.

        0x00 – notify upon command, reader will only produce tag information report upon notification command reception;

        0x01 – notify over time, reader will produce tag information report in every RepPauseTime time interval;

        0x02 – notify upon new tag, reader will produce tag information report and store the information once a new tag is inquired;

        0x03 – notify upon tag information removal, reader will produce tag information report upon tag information deletion due to lack of memory.

        0x04 – notify upon tag information changes, reader will produce tag information report upon tag information adding or removal in the memory.

All other values are reserved, reader will return a parameter error status in the response frame if other value is delivered in this field.

RepPauseTime: the time break between two tag information reports, in notify over time form. The range of RepPauseTime is (0 ~ 255)*1s.

Response frame:

Len	Adr	reCmd	Status	Data[]	CRC-16	
0x05	0xXX	0x3c	0x00	——	LSB	MSB

8.4.13 Modify inventory time break

The function of this command is to modify the reader inventory time break in auto-mode.

Command frame:

Len	Adr	Cmd	Data[]	CRC-16	
			ReadPauseTim		
0x05	0xXX	0x3d	0xXX	LSB	MSB

Parameter definition

ReadPauseTim: time break between two inventories, refer to the following table for corresponding time of different values.

ReadPauseTim	Time
0x00	10ms
0x01	20ms
0x02	30ms
0x03	50ms
0x04	100ms

Response frame:

Len	Adr	reCmd	Status	Data[]	CRC-16	
0x05	0xXX	0x3d	0x00	——	LSB	MSB

8.4.14 Modify inventory tag type

The function of this command is to modify the inventory tag type in auto-mode.

Command frame:

Len	Adr	Cmd	Data[]	CRC-16	
			TagProtocol		
0x05	0xXX	0x3e	0xXX	LSB	MSB

Parameter definition
TagProtocol:
bit7: tag protocol type.

　　0 – set inventory on G2(18000-6C) tag.

　　　　for TagProtocol = 0x00, only inquired EPC of G2 tags.

　　　　for TagProtocol = 0x02, only detects EAS.

　　　　for TagProtocal = 0x10, only inquired TID of G2 tags.

　　1 –

for TagProtocol = 0x80, set inventory on 18000-6B tag.
All other value reserved.

Response frame:

Len	Adr	reCmd	Status	Data[]	CRC-16	
0x05	0xXX	0x3e	0x00	——	LSB	MSB

8.4.15 Setup antenna multiplexing

The function of this command is to modify reader antenna configuration.

Command frame:

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

Parameter definition
Ant: antenna configuration information. 1 antenna is the minimum requirement for operation.
bit0: antenna 1 configuration bit.
    0 – disable antenna 1;
    1 – enable antenna 1.
bit1: antenna 2 configuration bit.
    0 – disable antenna 2;
    1 – enable antenna 2.
bit2: antenna 3 configuration bit.
    0 – disable antenna 3;
    1 – enable antenna 3.
bit3: antenna 4 configuration bit.
    0 – disable antenna 4;
    1 – enable antenna 4.
bit4 ~ bit6: reserved, default value is 0.
bit7: configuration preservation status.
    0 – configuration preserved during reader power off;
    1 – configuration not preserved.

Response frame:

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

8.4.16 Enable/disable buzzer

The function of this command is enable/disable buzzer.

Command frame:

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

Parameter definition
BeepEn: buzzer working mode selection.
bit0: 0 – disable buzzer;
    1 – enable buzzer, the buzzer will beep on every success tag operation.
bit1 ~ bit7 are reserved, default value is 0.

Response frame:

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

8.4.17 Adjust Real time clock

The function of this command is to adjust real time clock.

Command frame:

Len	Adr	Cmd	Data[]						CRC-16	
			Year	Month	Date	Hour	Minute	Second		
0x0a	0xXX	0x41	0xXX	0xXX	0xXX	0xXX	0xXX	0xXX	LSB	MSB

Parameters definition
Year – 6 bits, valid range is 0 ~ 63, i.e. 2000 ~ 2063.
Month – 4 bits, valid range is 1 ~ 12.
Date – 5 bits, valid range is 1 ~ 31.
Hour – 5 bits, valid range is 0 ~ 23.
Minute – 6 bits valid range is 0 ~ 59.
Second – 6 bits, valid range is 0 ~ 59.
NOTE: the corresponding time of this parameter must be after the most recently saved tag information timestamp, reader will return a parameter error status in the response frame if incorrect value is delivered in this field.

Response frame:

Len	Adr	reCmd	Status	Data[]	CRC-16	
0x05	0xXX	0x41	0x00	——	LSB	MSB

8.4.18 Obtain current time from real time clock

The function of this command is to obtain the current time from the reader real time clock.

Command frame:

Len	Adr	Cmd	Data[]	CRC-16	
0x04	0xXX	0x42	——	LSB	MSB

Response frame:

Len	Adr	reCmd	Status	Data[]						CRC-16	
				Year	Month	Date	Hour	Minute	Second		
0x0b	0xXX	0x42	0x00	0xXX	0xXX	0xXX	0xXX	0xXX	0xXX	LSB	MSB

8.4.19   Obtain tag information from reader memory

The function of this command is to obtain all the tag information stored in reader memory.

Command frame:

Len	Adr	Cmd	Data[]	CRC-16	
0x04	0xXX	0x43	——	LSB	MSB

Response frame:

Len	Adr	reCmd	Status	Data[]	CRC-16	
0xXX	0xXX	0x43	0xXX	——	LSB	MSB

Parameters definition

Status: 0x00 – these is no data in Data[], and this response frame is the end of the series.

0x03 – there is data in Data[], and further data will delivered in the following frames.

Parameters of Data[]:

Data[]				
DiscTime	LastTime	Count	Ant	EPC-ID
4 bytes	4 bytes	2 bytes	0xXX	variable

Parameter definition

DiscTime: 4 bytes, the timestamp of the first tag detection.

DiscTime					
Year	Month	Date	Hour	Minute	Second
bit31 ~ bit26	bit25 ~ bit22	bit21 ~ bit17	bit16 ~ bit12	bit11 ~ bit6	bit5 ~ bit0

Year – 6 bits, valid range is 0 ~ 63, i.e. 2000 ~ 2063.

Month – 4 bits, valid range is 1 ~ 12.

Date – 5 bits, valid range is 1 ~ 31.
Hour – 5 bits, valid range is 0 ~ 23.
Minute – 6 bits valid range is 0 ~ 59.
Second – 6 bits, valid range is 0 ~ 59.

LastTime: the timestamp of the last tag detection.

LastTime					
Year	Month	Date	Hour	Minute	Second
bit31 ~ bit26	bit25 ~ bit22	bit21 ~ bit17	bit16 ~ bit12	bit11 ~ bit6	bit5 ~ bit0

Year – 6 bits, valid range is 0 ~ 63, i.e. 2000 ~ 2063.
Month – 4 bits, valid range is 1 ~ 12.
Date – 5 bits, valid range is 1 ~ 31.
Hour – 5 bits, valid range is 0 ~ 23.
Minute – 6 bits valid range is 0 ~ 59.
Second – 6 bits, valid range is 0 ~ 59.

Count: 2 bytes, the total detected times for a particular tag between DiscTime and LastTime.

Ant: 1 byte, indicates which antenna had inquired the tag. For example, 0x05 is 0101 in binary, this indicates Antenna 3 and Antenna 1.

EPC-ID: the 1st byte represents the length of EPC/UID number. EPC/UID number data starts from the 2nc byte.

8.4.20 Clear reader memory buffer

The function of this command is to clear all the stored tag information from the reader memory.

Command frame:

Len	Adr	Cmd	Data[]	CRC-16	
0x04	0xXX	0x44	——	LSB	MSB

Response frame:

Len	Adr	reCmd	Status	Data[]	CRC-16	
0x05	0xXX	0x44	0x00	——	LSB	MSB

8.4.21 Relay control

The function of this command is to control the state of the built-in relay.

Command frame:

Len	Adr	Cmd	Data[] RelayTime	CRC-16	
0x05	0xXX	0x45	0xXX	LSB	MSB

Parameter definition

RelayTime: configuration of the relay pickup time, the valid range of the parameter is 1 ~ 255, corresponds to (1 ~ 255)*50ms

Response frame:

Len	Adr	reCmd	Status	Data[]	CRC-16	
0x05	0xXX	0x45	0x00	——	LSB	MSB

8.4.22 GPIO control

The function of this command is to control the output of GPIO. The default output is high TTL level.

Command frame:

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

Parameter definition

OutputPin: the output state of GPIO (pin Out1 to Out4). Bit0 ~ bit3 control the Out1 to Out4 respectively. Bit4 ~ bit7 are reserved.

Response frame:

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

8.4.23 Obtain GPIO state

The function of this command is to obtain the input and output states of GPIO

Command frame:

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

Response frame:

Len	Adr	reCmd	Status	Data[] OutputPin	CRC-16	

| 0x06 | 0xXX | 0x47 | 0x00 | 0xXX | LSB | MSB |

Parameter definition

OutputPin: the input and output states of GPIO. Bit0 ~ bit3 represent IN1 to IN4 and bit4 ~ bit7 represent Out1 to Out4 respectively.

8.4.24   Notification pulse configuration

The function is to enable or disable a 2ms low level notification pulse on the associated port for every tag detection.

Command frame:

Len	Adr	Cmd	Data[] OutputRep	CRC-16	
0x05	0xXX	0x48	0xXX	LSB	MSB

Parameters definition

OutputRep:

bit0: associated with antenna 1 and Out1 pin.

    1 – Out1 will output a 2ms low level notification pulse for every tag detection from antenna 1;

    0 – disable notification signal.

bit1: associated with antenna 2 and Out2 pin.

    1 – Out2 will output a 2ms low level notification pulse for every tag detection from antenna 2;

    0 – disable notification signal.

bit2: associated with antenna 3 and Out3 pin.

    1 – Out3 will output a 2ms low level notification pulse for every tag detection from antenna 3;

    0 – disable notification signal.

bit3: associated with antenna 4 and Out4 pin.

    1 – Out4 will output a 2ms low level notification pulse for every tag detection from antenna 4;

    0 – disable notification signal.

All other values are reserved, default is 0.

Response frame:

Len	Adr	reCmd	Status	Data[]	CRC-16	
0x05	0xXX	0x48	0x00	——	LSB	MSB

Note: Default TTL level of the associated ports should be high, otherwise pulse will not be generated

8.4.25   Modify delay configuration in trigger-mode

The function of this command is to modify the trigger delay configuration for trigger-mode

Command frame:

Len	Adr	Cmd	Data[]		CRC-16	
			TriggerTime			
0x05	0xXX	0x49	0xXX		LSB	MSB

Parameter definition

TriggerTime: configuration of the trigger delay, the valid range of the parameter is 0 ~ 255, corresponds to (0 ~ 255)*1s. Default value of TriggerTime is 0.

Response frame:

Len	Adr	reCmd	Status	Data[]	CRC-16	
0x05	0xXX	0x49	0x00	——	LSB	MSB

8.4.26 Modify configuration for TID inventory

The function of this command is to modify the parameters for TID inventory in auto-mode.

Command frame:

Len	Adr	Cmd	Data[]		CRC-16	
			AdrTID	LenTID		
0x06	0xXX	0x4a	0xXX	0xXX	LSB	MSB

Parameters definition

AdrTID: initial word address of TID memory inventory.

LenTID: data length for TID inventory operation, the valid range of LenTID 0 ~ 15. All other values are reserved, and reader will return a parameter error status in the response frame if other value is delivered in this field.

Response frame:

Len	Adr	reCmd	Status	Data[]	CRC-16	
0x05	0xXX	0x4a	0x00	——	LSB	MSB

8.4.27 Obtain the reader unique serial number

The function of this command is to obtain the unique serial number of a reader.

Command frame:

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

Response frame:

Len	Adr	reCmd	Status	Data[]	CRC-16	

0x09	0xXX	0x4c	0x00	SeriaNo		
				4 bytes	LSB	MSB

Parameter definition
SeriaNo: 4 bytes, the unique serial number of the reader.

8.4.28 Switch network mode of reader

The function of this command is to switch the reader network mode between AT-mode and transparent-mode. Reader will reset the network to transparent-mode on every start-up. User can switch the network mode via delivering this command to reader. In AT-mode, user can modify network parameters via serial communication. The network mode will switch back to transparent-mode once AT-mode is exited. Power off reader and restart the reader again will also exit AT-mode.

Command frame:

Len	Adr	Cmd	Data[]	CRC-16	
			ATMode		
0x05	0xXX	0x4d	0xXX	LSB	MSB

Parameter definition
ATMode: network mode selection.
   0x01 – enter AT-mode
   0x00 – exit AT-mode.

Response frame:

Len	Adr	reCmd	Status	Data[]	CRC-16	
0x05	0xXX	0x4d	0x00	——	LSB	MSB

8.4.29 Network AT transparent command

When network mode is set to AT-mode, user is able to control the network module via AT commands. By using the transparent command, user can define the sent data，the reception and operation timeout configuration.

Command frame:

Len	Adr	Cmd	Data[]		CRC-16	
			TimeOut	ATCmd		
0x05+n	0xXX	0x4e	0xXX	N bytes	LSB	MSB

Parameters definition
TimeOut: Timeout setting for the current command. The valid range of the parameter is 1 ~ 255, corresponds to (1~255)*10ms.

ATCmd: Data to network module

Response frame:

Len	Adr	reCmd	Status	Data[]	CRC-16	
				ATRsp		
0x05+n	0xXX	0x4e	0x00	N bytes	LSB	MSB

Parameters definition
ATRsp: the inquired data from a successful operation. If any failure occurred during the operation, reader will return all the already inquired data after the timeout period is exceed.

8.4.30 Modify tag customised function

The function of this command is to launch the customised utilities of some particular tags, to achieve specific tag function.

Command frame:

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

Parameter definition
InlayType: the type of tag, the valid value of this parameter is 0 ~ 254.
0 – the default value of this parameter, represent tag type is not specified.
1 – launch the Peek function of Monza4QT tag (the status of tag will temporary change from public to private). Launching this function will make affection on the data reading/writing, block writing, protection word writing and EPC number writing operation.

Response frame:

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

Parameter definition
InlayType: the type of tag, the valid value of this parameter is 0 ~ 254.

8.4.31 Enable antenna check

The function of this command is to enable/disable the antenna check during tag reading/writing operation.

Command frame:

Len	Adr	Cmd	Data[]	CRC-16	
			CheckAnt		

| 0x05 | 0xXX | 0x66 | 0xXX | LSB | MSB |

Parameter definition

CheckAnt: 1 byte, antenna check switch.

0x00 – disable antenna check;

0x01 – enable antenna check.

All other values are reserved, reader will return a parameter error status in the response frame if other value is delivered in this field.

Response frame:

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

8.4.32 Modify maximum EPC/TID length configuration for memory buffer

The function of this command is to modify the maximum EPC/TID length for inventory with memory buffer. This modification will clear all the tag data previously stored in the memory buffer.

Command frame:

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

Parameter definition

SaveLen: 1 byte, the maximum EPC/TID length.

0 – 128bit length, i.e. 16 bytes. The maximum storable tag amount is 528 for this setting;

1 – 496bit length, i.e. 62 bytes. The maximum storable tag amount is 160 for this setting.

Response frame:

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

8.4.33 Load the maximum EPC/TID length configuration

The function of this command is to load the configuration of maximum EPC/TID length for reader memory buffer

Command frame:

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

Response frame:

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

Parameter definition

SaveLen: 1 byte, the maximum EPC/TID length.

           0 – 128bit length, i.e. 16 bytes;

           1 – 496bit length, i.e. 62 bytes.

8.4.34   Obtain data from memory buffer

The function of this command is to obtain all the tag information from reader memory. This command will not cause affection on the status of the stored data. Data can be access multiple times. On the other hand, the tag inventory command (refer to Chapter 8.2.1) will clear all the data from memory buffer.

Command frame:

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

Response frame:

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

Parameters definition

Status: the status of response, detail description is shown in the following table

Status	Description
0x01	operation completed, reader will report all inquired tags information to host
0x03	reader is not able to response all the data in a single frame, further data will be transmitted in the following frames.

Num: 1 byte, the amount of EPC/TID included in this response.

EPC Data: tag EPC/TID data stored in the memory buffer.

EPC-n				
Ant	Len	EPC/TID	RSSI	Count
0xXX	0xXX	N bytes	0xXX	0xXX

Ant: indicates which antenna had inquired the tag. For example, 0x05 is 0101 in binary, this indicates Antenna 3 and Antenna 1.

Len: 1 byte, the byte length of the EPC/TID.

EPC/TID: EPC number/TID data of tag, the length of data should identical with Len. Every tag EPC number or TID data is the most-significant word and the most-significant byte in a word first.

RSSI: 1 byte, the reader signal strength at the time when the tag is inquired.

Count: the total detected times for a particular tag.

   0xFF – total detection time is larger or equal to 255.

8.4.35 Clear memory buffer

The function of this command is to clear all the stored tag data from the memory buffer.

Command frame:

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

Response frame:

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

8.4.36 Obtain the total tag amount from memory buffer

The function of this command is to obtain the total tag amount stored in memory buffer.

Command frame:

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

Response frame:

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

Parameters definition

Count: 2 bytes, the total amount of tag stored in the memory buffer, most-significant byte first.

8.4.37 Modify parameters of real time inventory mode

The function of this command is to modify the real time inventory associated parameters.

Command frame:

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

Parameters of Data[]:

Data[]

TagProtocol	ReadPauseTime	FliterTime	QValue	Session
0xXX	0xXX	0xXX	0xXX	0xXX

Data[]					
MaskMem	MaskAdr	MaskLen	MaskData	AdrTID	LenTID
0xXX	2 bytes	0xXX	variable	0xXX	0xXX

Parameters definition

TagProtocol: 1 byte, tag type definition for real time inventory.

        0 – EPC C1G2 (ISO18000-6C) tags.

        1 – ISO18000-6B tags. Configurations of the following parameters will be ignored for 6B, QValue, Session, MaskMem, MaskAdr, MaskLen, MaskData, AdrTID, LenTID.

All other values are reserved, reader will return a parameter error status in the response frame if other value is delivered in this field.

ReadPauseTime: 1 byte, time break between 2 real time inventories.

        0x00 – 10ms;

        0x01 – 20ms;

        0x02 – 30ms;

        0x03 – 50ms;

        0x04 – 100ms.

All other values are reserved, reader will return a parameter error status in the response frame if other value is delivered in this field.

FliterTime: 1 byte, tag filtering time. The valid value of this parameter is 0 ~ 255, corresponds to (0 ~ 255)*1s. In real time inventory, if reader detects a particular tag for more than 1 time, reader will only upload tag information of this tag once within the pre-defined filtering time. For FliterTime = 0, disable tag filtering function.

QValue: 1 byte, the original Q-value of the EPC tag inventory, the setting of Q-value should follow the rule: $2^Q \approx$ total amount of tags within the effective field. The range of Q-value is 0 ~ 15, if other value is delivered in this field, reader will return a parameter error status in the response frame.

Session: 1 byte, the Session-value of the EPC tag inventory.

        0x00 – apply S0 as Session value;

        0x01 – apply S1 as Session value;

        0x02 – apply S2 as Session value;

        0x03 – apply S3 as Session value;

        0xff – apply reader smart configuration (only valid in EPC inventory).

All other values are reserved, reader will return a parameter error status in the response frame if other value is delivered in this field.

MaskMem: 1 byte, mask area indication.

0x01 – EPC memory;

0x02 – TID memory;

0x03 – User memory.

All other values are reserved, reader will return a parameter error status in the response frame if other value is delivered in this field.

MaskAdr: 2 bytes, entry bit address of the mask, the valid range of MaskAdr is 0 ~ 16383.

MaskLen: 1 byte, bit length of mask(unit: bits).

MaskData: mask data. the length of MaskData equals to MaskLen/8. If MaskLen is not a multiple of 8 integer, the length of MaskData is equal to the int[MaskLen/8]+1. Non-specified lower significant figures should be filled up with 0.

AdrTID：initial word address of inventory TID memory. If command delivered this parameter and LenTID, the mode of inventory should be TID, not EPC.

LenTID: data length for TID inventory operation, the valid range is 0 ~ 15. All other values are reserved, and reader will return a parameter error status in the response frame if other value is delivered in this field. If command delivered this parameter and AdrTID, the mode of inventory should be TID, not EPC.

NOTE:

1. When MaskMem, MaskAdr, MaskLen and MaskData are not provided, no mask pattern will be involved in inventory

2. In real time inventory mode, reader will apply the predefined antenna and inventory time parameters for inventory.

Response frame:

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

8.4.38   Load real time inventory mode parameters

The function of this command is to load the parameters of real time inventory

Command frame:

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

Response frame:

Len	Adr	reCmd	Status	Data[]	CRC-16	
0xXX	0xXX	0x77	0x00	ReadMode,TagProtocol,	LSB	MSB

				ReadPauseTime, FliterTime, QValue, Session, MaskMem, MaskAdr, MaskLen, MaskData, AdrTID, LenTID		

Parameters definition

ReadMode: 1 byte, the current working mode of reader.

TagProtocol: 1 byte, tag type definition of real time inventory.

ReadPauseTime: 1 byte, time break between 2 real time inventories.

FliterTime: 1 byte, tag filtering time of real time inventory.

QValue: 1 byte, the original Q-value of real time mode for EPC inventory.

Session: 1 byte, the Session-value of real time mode for EPC inventory.

MaskMem, MaskAdr, MaskLen, MaskData: mask condition for **EPC C1G2** tag inventory in real time mode. MaskMem and MaskLen are 1 byte long respectively. MaskAdr is 2 bytes long, most-significant byte first. MaskData has constant length of 32 bytes, fill the over MaskLen value content with zero.

AdrTID: initial word address of TID memory inventory.

LenTID: data length for TID inventory operation.

8.4.39   Load/modify heartbeat packet time break of real time inventory

The function of this command is to modify the heartbeat packet upload time break for real time inventory mode. For HeartBeatTime = 0, disable heartbeat packet delivery.

Command frame:

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

Parameter definition
HeartBeatTime: time break between 2 heartbeat packets deliveries
bit7: action on heartbeat time break configuration
    0 – load heartbeat time break configuration;
    1 – modify heartbeat time break configuration.
bit6 ~ bit0: heartbeat time break configuration
For bit7 = 0, bit6 ~ bit0 will be ignored.
For bit7 = 1, bit6 ~ bit0 is the configuration of time break between 2 heartbeat packets deliveries
For HeartBeatTime = 0, disable heartbeat packet delivery.

Response frame:

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

Parameter definition

HeartBeatTime: the current configuration of heartbeat packet time break.

bit7: reserved, default value is 0.

bit6 ~ bit0: the current configuration of heartbeat packet time break. The valid value of this parameter is 0 ~ 127, corresponds to (0 ~ 127)*30s.

NOTE:

Reader will only deliver heartbeat packet if no tag is detected for a consecutive period (longer than the heartbeat time break)

8.4.40 Modify RF power configuration separately for write operations

The function of this command is to modify RF power for write operations. The default value of the power parameter is 0x00. The setting of this parameter will be preserved even reader power is down.

Command frame:

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

Parameter definition

WritePower: configuration of the power.

bit7: enable/disable separate RF power configuration for write operation.

  0 – disable separate RF power configuration, power will be identical for both read and write commands.

  1 – enable separate RF power configuration. The valid value of RF power is 0~30, for setting of 30, the output power is approximately 1W.

Response frame:

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

The separate RF power will take effect for the following commands,

EPC C1G2 (ISO18000-6C) commands

- write data command;
- write EPC number command;
- Extended data writing command with assigned mask;
- block erase command;

- block writing command.

ISO18000-6B command

- write data command

8.4.41 Load the RF power configuration of write operations

The function of this command is to load the predefined separate RF power configuration of write operation.

Command frame:

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

Response frame:

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

Parameter definition

WritePower: configuration of the power.

bit7: configuration of sseparate RF power configuration for write operation.

    0 – disabled separate RF power configuration, power will be identical for both read and write commands.

    1 – enabled separate RF power configuration. The valid value of RF power is 0~30, for setting of 30, the output power is approximately 1W.

8.4.42 Modify or load maximum write retry time configuration

The function of this command is to modify or load the maximum write retry time configuration. For tag writing and associated commands, if failure occurred, reader will reattempt the operation until success or reach the maximum write retry time. Default value of the retry time is 3. The setting of this parameter will be preserved even reader power is down.

Command frame:

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

Parameter definition

RetryTimes: action on maximum write retry time configuration

bit7: load/modify maximum write retry time configuration

    0 – load maximum write retry time;

    1 – modify maximum write retry time;

bit6 ~ bit3: reserved.

bit2 ~ bit0: maximum write retry time

For bit7 = 0, bit6 ~ bit0 will be ignored.

For bit7 = 1, bit2 ~ bit0 is the configuration of maximum retry time. The range of this parameter is 0 ~ 7.

Response frame:

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

Parameter definition

RetryTimes: value of maximum write retry time

bit7 ~ bit3: reserved, default value is 0.

bit2 ~ bit0: maximum write retry time setting. The valid range of RetryTimes is 0 ~ 7.

The retry time counter will take effect for the following command,

EPC C1G2 (ISO18000-6C) commands

- write data command;
- write EPC number command;
- Extended data writing command with assigned mask;
- block erase command;
- block writing command.

ISO18000-6B command

- write data command

8.4.43   Modify auto-mode inventory parameters

The function of this command is to modify the parameters of auto-mode inventory. Values of these parameters are not valid in answering-mode, for answering-mode parameters modification, refer to Chapter 8.2.1.

Command frame:

Len	Adr	Cmd	Data[]		CRC-16	
			QValue	Session		
0x06	0xXX	0x81	0xXX	0xXX	LSB	MSB

Parameters definition

QValue: 1 byte, the original Q-value of the EPC tag inventory, the setting of Q-value should follow the rule: $2^Q \approx$ total amount of tags within the effective field. The range of Q-value is 0 ~ 15, if other value is delivered in this field, reader will return a parameter error status in the response frame.

Session: 1 byte, the Session-value of the EPC tag inventory.

        0x00 – apply S0 as Session value;

0x01 – apply S1 as Session value;

0x02 – apply S2 as Session value;

0x03 – apply S3 as Session value;

0xff – apply reader smart configuration (only valid in EPC inventory).

All other values are reserved, reader will return a parameter error status in the response frame if other value is delivered in this field.

Response frame:

Len	Adr	reCmd	Status	Data[]	CRC-16	
0x05	0xXX	0x81	0x00	——	LSB	MSB

8.4.44 Obtain auto-mode inventory parameters

The function of this command is to obtain the parameters of auto-mode inventory. These parameters only valid in auto mode.

Command frame:

Len	Adr	Cmd	Data[]	CRC-16	
0x04	0xXX	0x82	——	LSB	MSB

Response frame:

Len	Adr	reCmd	Status	Data[]	CRC-16	
0x07	0xXX	0x82	0x00	QValue , Session	LSB	MSB

Parameters definition

QValue: the original Q-value of the EPC tag inventory, the range of Q-value is 0 ~ 15,

Session: 1 byte, the Session-value of the EPC tag inventory.

0x00 – apply S0 as Session value;

0x01 – apply S1 as Session value;

0x02 – apply S2 as Session value;

0x03 – apply S3 as Session value;

0xff – apply reader smart configuration (only valid in EPC inventory).

8.4.45 Obtain R2000 module firmware version

The function of this command is to obtain reader internal R2000 module firmware version.

Command frame:

Len	Adr	Cmd	Data[]	CRC-16	
0x04	0xXX	0x83	——	LSB	MSB

Response frame:

Len	Adr	reCmd	Status	Data[]	CRC-16	
0x07	0xXX	0x83	0x00	Version (2 bytes)	LSB	MSB

Parameter definition
Version: 2 bytes, the high byte states the main version number and the low byte states the subversion number.

8.4.46 Update internal ROM

The function of this command is to set the internal ROM to update mode. Reader will enter update mode immediately after the response delivery. To exit the update mode, turn the power of reader off, then restart the reader again after a few second.

Command frame:

Len	Adr	Cmd	Data[]	CRC-16	
0x04	0xXX	0x84	——	LSB	MSB

Response frame:

Len	Adr	reCmd	Status	Data[]	CRC-16	
0x05	0xXX	0x84	0x00	——	LSB	MSB

8.4.47 Modify or load Antenna return loss threshold configuration

The function of this command is to modify or load the return loss threshold for antenna check. The default return loss threshold is -6dB. The setting of this parameter will be preserved even reader power is down.

Command frame:

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

Parameter definition
ReturnLoss: action on the Return loss configuration.
bit7: load/modify return loss flag.
    0 – load the current return loss configuration;
    1 – modify return loss configuration.
bit6 ~ bit0: return loss configuration
For bit7 = 0, bit6 ~ bit0 will be ignored.
For bit7 = 1, bit6 ~ bit0 is the desired return loss configuration. The range of return loss is 0 ~ 20, according to 0dB ~ 20dB.
Other values are reserved, reader will return a parameter error status in the response frame if other

value is delivered in this field.

Response frame:

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

Parameter definition

ReturnLoss: current return loss configuration.

bit7: reserved, default setting is 0.

bit6 ~ bit0: the current antenna return loss threshold. The range is 0 ~ 20.

8.4.48　Modify or load DRM configuration

The function of this command is to modify or load DRM switch mode. Setting of these parameters will lost during power off. DRM will be reset to off state on every reader start-up.

Command frame:

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

Parameter definition

DRMMode: action on DRM configuration.

bit7: load/modify DRM flag.

　　0 – load the current DRM configuration;

　　1 – modify DRM configuration.

bit6 ~ bit0: DRM configuration

For bit7 = 0, bit6 ~ bit0 will be ignored.

For bit7 = 1, bit6 ~ bit0 is the desired DRM configuration.

　　　　0 – Switch OFF DRM;

　　　　1 – Switch ON DRM.

Other values are reserved, reader will return a parameter error status in the response frame if other value is delivered in this field.

Response frame:

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

Parameter definition

DRMMode: action on DRM configuration.

bit7: reserved, the default setting is 0.

bit6 ~ bit0: current DRM configuration

0 –DRM is switch OFF;

1 – DRM is switch ON.

8.4.49 Measure antenna return loss

The function of this command is to measure antenna return loss on specific frequency point.

Command frame:

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

Parameters definition

TestFreq: target frequency point for the return loss measurement. The unit of TestFreq is KHz, most-significant byte first. A valid frequency point must be a multiple of either 125KHz or 100KHz. Reader will return a parameter error status in the response frame if other value is delivered in this field.

Ant: 1 byte, target antenna for this measurement

    0 – antenna 1;

    1 – antenna 2;

    2 – antenna 3;

    3 – antenna 4.

Other values are reserved, reader will return a parameter error status in the response frame if other value is delivered in this field.

Response frame:

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

Parameter definition

ReturnLoss: result of the return loss measurement, the unit of ReturnLoss is dB.