



Communication Protocol OEM-UHF M6X0

iDTRONIC GmbH
Ludwig-Reichling-Straße 4
67059 Ludwigshafen
Germany/Deutschland

Issue 1.0
– 08 July 2025 –

Phone +49 621 6690094-0
Fax +49 621 6690094-9
E-Mail info@idtronic-rfid.com
Web <https://idtronic-rfid.com/>

Subject to alteration without prior notice.
© Copyright iDTRONIC GmbH 2025
Printed in Germany

Contents

1	Introduction	5
1.1	Host-to-Reader Communication Framework.....	5
1.2	Reader-to-Host Communication Framework.....	5
1.3	Command Classification and Workflow	6
1.4	Special Note	6
1.5	Glossary	7
2	Bootloader Commands	8
2.1	Write Flash (0x01)	8
2.2	Read Flash (0x02)	8
2.3	Verify Firmware (0x08)	9
2.4	Get Version (0x03)	9
2.5	Boot Firmware (0x04)	10
2.6	Set Baud Rate (0x06).....	10
2.7	Boot Bootloader (0x09)	10
2.8	Get Run Phase (0x0C)	11
2.9	Get Serial Number (0x10)	11
3	Tag Inventory Commands	12
3.1	Single Tag Inventory (0x21)	13
3.2	Synchronous Inventory (0x22)	15
3.3	Get Tag Buffer (0x29).....	17
3.4	Asynchronous Inventory (0xAA)	18
3.4.1	Start AsyncInventory (0xAA48)	19
3.4.2	Stop AsyncInventory (0xAA49).....	20
3.4.3	Unrequested Reader-to-Host Commands	20
3.4.4	Remark	20
4	Tag Access Commands	22
4.1	Write Tag Data (0x24)	22
4.2	Write Tag EPC (0x23)	23
4.3	Lock Tag (0x25)	23
4.4	Kill Tag (0x26).....	23
4.5	Read Tag Data (0x28)	24
5	Setting Commands	26
5.1	Set Antenna Ports (0x91)	26
5.2	Set Current Tag Protocol (0x93).....	28
5.3	Set Frequency Hopping (0x95).....	28
5.4	Set GPO (0x96)	28
5.5	Set Current Region (0x97).....	29

5.6	Set Reader Configuration (0x9A)	30
5.7	Set Tag Protocol Configuration (0x9B).....	30
6	Getting Commands	32
6.1	Get Antenna Ports (0x61)	32
6.2	Get Current Tag Protocol (0x63).....	32
6.3	Get Frequency Hopping (0x65)	33
6.4	Get GPI (0x66).....	33
6.5	Get Current Region (0x67)	34
6.6	Get Available Regions (0x71)	34
6.7	Get Reader Configuration (0x6A).....	34
6.8	Get Protocol Configuration (0x6B).....	34
6.9	Get Current Temperature (0x72)	35
7	Status Code	36

1 Introduction

The serial communication between a computer (host) and the reader is based on a synchronized command-response mechanism. Whenever the host sends a message to the reader, it cannot send another message until after it receives a response.

The communication parameters are:

- Baud rate: 9600..921600 bit/s (115200 bit/s is factory default)
- 1 start bit
- 8 data bits
- 1 stop bit
- No parity bit

Note: the total number of bytes of the communication data must not exceed 255.

1.1 Host-to-Reader Communication Framework

Host-to-Reader Communication is based on packets as shown in the diagram below. The reader can only accept one command at a time and commands are executed serially. Hence the host needs to wait for a reader-to-host response before issuing another host-to-reader command packet.

Header	Data Length	Command Code	Data	CRC-16
1 byte, must be 0xFF	1 byte, number of bytes in the data field	1 byte	Data block, high bit in front	2-byte cyclic redundancy code, high bit in front

1.2 Reader-to-Host Communication Framework

The following diagram defines the format of the generic response packet sent from the reader to the host.

Header	Data Length	Command Code	Status Code	Data	CRC-16
1 byte, must be 0xFF	1 byte, number of bytes in the data field	1 byte	2 bytes, 0 means the operation is successful, else error	Data block, high bit in front	2-byte cyclic redundancy code, high bit in front

C Language Example of CRC-16

The return data obtained by calling the function CalcCRC is CRC-16, where the parameter *msgbuf is the communication protocol string data except the CRC-16, and msglen is the total number of bytes except for the CRC-16 bytes.

```

1. #define MSG_CRC_INIT          0xFFFF
2. #define MSG_CCITT_CRC_POLY    0x1021
3.
4. void CRC_calcCrc8(uint16 *crcReg, uint16 poly, uint16 u8Data) {
5.     uint16 i;
6.     uint16 xorFlag;
7.     uint16 bit;
8.     uint16 dcdBitMask = 0x80;
9.
10.    for (i = 0; i < 8; ++i) {
11.        xorFlag = *crcReg & 0x8000;
12.        *crcReg <<= 1;
13.        bit = ((u8Data & dcdBitMask) == dcdBitMask);

```

```

14.         *crcReg |= bit;
15.         if (xorFlag) {
16.             *crcReg = *crcReg ^ poly;
17.         }
18.         dcdBitMask >>= 1;
19.     }
20. }
21.
22. uint16 CalcCRC(uint8 *msgbuf, uint8 msglen) {
23.     uint16 calcCrc = MSG_CRC_INIT;
24.     uint8 i;
25.     for (i = 1; i < msglen; ++i) {
26.         CRC_calcCrc8(&calcCrc, MSG_CCITT_CRC_POLY, msgbuf[i]);
27.     }
28.     return calcCrc;
29. }

```

1.3 Command Classification and Workflow

Command Classification

The commands are divided into four categories according to their functions: Bootloader Commands, Tag Inventory Commands, Tag Access Commands, Setting Commands and Getting Commands.

Command Set Table

Command Set Name	Description
Bootloader Commands	Any command that can be executed while the reader is in the bootloader phase.
Tag Inventory Commands	Commands related to inventory operation.
Tag Access Commands	Commands related to Tag Access operations.
Setting Commands	Used to set configurable values in the firmware of the reader.
Getting Commands	Used to get parameters, options and the working state from the reader.

In addition, some commands can be executed while the reader is in the Bootloader and App Firmware phases.

Command Workflow

The Bootloader is automatically started upon power up. All tag operations of the reader can only be used in the App Firmware layer. Hence you must first execute the Boot Firmware command (0x04) to let the reader enter the App Firmware layer. Afterwards you can execute Setting Commands, Getting Commands, Tag Inventory Commands and Tag Access Commands.

1.4 Special Note

The function and usage of each command will be described in detail in later chapters. When introducing each command, it will follow the following sequence:

1. Command overview
2. Command attribute
3. Host to Reader (format of Data Field)
4. Reader to Host (format of Data Field)
5. Example
6. Remark

For a command without a data field, there is no Host to Reader section. Similarly in the Reader to Host and the Example section.

Integers with multiple bytes are in MSB order.

1.5 Glossary

CRC	Cyclic Redundancy Check
MAC	Message Authentication Code
RFU	Reserved for Future Use

2 Bootloader Commands

The bootloader is automatically started upon power up and allows access to the onboard flash memory along with other commands. The commands described in the following table are all commands that can be executed during the Bootloader phase.

Overview of Bootloader Commands

Command	Command Code	Description
Write Flash	0x01	Write the content of the onboard flash memory, used to update the firmware of the reader
Read Flash	0x02	Read the content of the onboard flash memory
Verify Firmware	0x08	Used to check whether the firmware was written correctly and should not be used for other purposes
Get Version	0x03	Used to get the version information of the reader
Boot Firmware	0x04	Switch the reader to running the APP Firmware layer
Set Baud Rate	0x06	Change the baud rate of the serial port of the reader
Boot Bootloader	0x09	Switch the reader back to running the Bootloader layer
Get Run Phase	0x0C	Get the current run Phase of the reader
Get Serial Number	0x10	Get the serial number of the reader

2.1 Write Flash (0x01)

Bootloader command. Write the content of the onboard flash memory, used to update the firmware of the reader.

Host to Reader

Field	Byte Length	Description
FINFLAG	1 byte	0 indicates that there is still data to be written to the flash. 0xFF indicates the last data to be written to flash.
WRITEADDR	4 bytes	The initial address of flashing is 0x00104000. After each successful writing, the next address will be WRITEADDR + WRITELEN*4.
WRITELEN	1 byte	Defines the length of the WRITEDATA in blocks of 4 bytes. The value of WRITELEN is fixed to 32; the actual number of bytes to write is divided by 4 only when the data length of the last write is less than 128 bytes.
WRITEDATA	N bytes	Data to be written, the number of bytes is a multiple of 4.

2.2 Read Flash (0x02)

Bootloader command. Read the content of the onboard flash memory. This command is used as a secondary command for flashing APP firmware and should not be used for other purposes.

Host to Reader

Field	Byte Length	Description
READADDR	4 bytes	The address to read, high byte in front, the lowest address read is 0x00104000.
READLEN	1 byte	0-32, number of bytes read is READLEN*4

Reader to Host

Field	Byte Length	Description
READDATA	N bytes	The read data, length is READLEN*4 bytes

2.3 Verify Firmware (0x08)

Bootloader command. This command is used to check whether the flashing was correct, should not be used for other purposes.

Host to Reader

Field	Byte Length	Description
CHECKADDR	4 bytes	The value is 0x00104000.
CHECKDATALEN	4 bytes	The value is the number of bytes written to the flash using the command 0x01 divided by 4.
CHECKCRC	4 bytes	Calculation method: Use 4 bytes as a unit, and divide all bytes written to the Flash by the 0x01 command into N 4 bytes from the beginning to the end. The highest bytes of the N numbers are added to DATA1. The second highest bytes of the N number are added to DATA2. The second lowest bytes of the N numbers are added to DATA3. The lowest bytes of the N numbers are added to DATA4. DATA1, DATA2, DATA3 and DATA4 are also 32-bit numbers. The lowest 8 bits of DATA1 are the highest byte of CHECKCRC. The lowest 8 bits of DATA2 are the second highest byte of CHECKCRC. The lowest 8 bits of DATA3 are the second lowest byte of CHECKCRC. The lowest 8 bits of DATA4 are the lowest byte of CHECKCRC.

2.4 Get Version (0x03)

Bootloader and Firmware command. The command is used to get the version information of the reader.

Reader to Host

Field	Byte Length	Description
Bootloader Version	4 bytes	The version of the bootloader
Hardware Version	4 bytes	The version of the hardware
Firmware Date	4 bytes	The date of building the firmware
Firmware Version	4 bytes	The version of the firmware
Supported Protocol	4 bytes	The tag protocols supported, currently always 0x00000010

Example

Host to Reader

Header	Data Length	Command Code	CRC-16
FF	00	03	1D 0C

Reader to Host

Header	Data Length	Command Code	Status Code	Bootloader Version
FF	14	03	00 00	13 04 15 00

Hardware Version	Firmware Date	Firmware Version	Supported Protocol	CRC-16
A8 00 00 01	20 13 05 22	13 05 23 00	00 00 00 10	

2.5 Boot Firmware (0x04)

Bootloader and Firmware command. The reader is set to the APP Firmware layer. When the reader is already in the APP Firmware layer, nothing is done, and it returns successfully.

Reader to Host

Field	Byte Length	Description
Bootloader Version	4 bytes	The version of the bootloader
Hardware Version	4 bytes	The version of the hardware
Firmware Date	4 bytes	The date of building the firmware
Firmware Version	4 bytes	The version of the firmware
Supported Protocol	4 bytes	The tag protocols supported, currently always 0x00000010

Example

Host to Reader

Header	Data Length	Command Code	CRC-16
FF	00	04	1D 0B

Reader to Host

Header	Data Length	Command Code	Status Code	Bootloader Version
FF	14	03	00 00	13 04 15 00

Hardware Version	Firmware Date	Firmware Version	Supported Protocol	CRC-16
A8 00 00 01	20 13 05 22	13 05 23 00	00 00 00 10	

2.6 Set Baud Rate (0x06)

Bootloader and Firmware command. The default baud rate of the reader after power-on is 115200 bps. After successfully setting a new baud rate, it is best to have a delay of 10 ms before sending other operation commands to the reader.

Host to Reader

Field	Byte Length	Description
Baud Rate	4 bytes	The baud rate to change to, valid values are: 0x00002580, 0x00004B00, 0x00009600, 0x0000E100, 0x0001C200

Example

Host to Reader

Header	Data Length	Command Code	Baud Rate	CRC-16
FF	00	06	00 01 C2 00	A4 60

2.7 Boot Bootloader (0x09)

Bootloader and Firmware command. If the reader receives this command when currently running in the APP firmware layer, it will change to the bootloader layer. If the reader is currently running in the bootloader layer, nothing will change, and it will return successfully. Wait for 500 ms after successful return before sending another command.

Example

Host to Reader

Header	Data Length	Command Code	CRC-16
FF	00	09	1D 06

2.8 Get Run Phase (0x0C)

Bootloader and Firmware command. Get the current running phase of the reader.

Reader to Host

Field	Byte Length	Description
Program	1 byte	0x11 means bootloader layer; 0x12 means APP Firmware layer

Example

Host to Reader

Header	Data Length	Command Code	CRC-16
FF	00	0C	1D 03

Reader to Host

Header	Data Length	Command Code	Status Code	Program	CRC-16
FF	01	0C	00 00	12	

2.9 Get Serial Number (0x10)

Bootloader and Firmware command. Get the serial number of the reader.

Host to Reader

Field	Byte Length	Description
Option	1 byte	Reserved parameters, currently meaningless
Data Flags	1 byte	Reserved parameters, currently meaningless

Reader to Host

Field	Byte Length	Description
Year	4 bytes	Year of manufacture of this product
Serial Number	8 bytes	The serial number in this batch

Example

Host to Reader

Header	Data Length	Command Code	Option	Data Flags	CRC-16
FF	02	10	00	00	F0 93

Reader to Host

Header	Data Length	Command Code	Status Code	Year	Serial Number	CRC-16
FF	14	10	00 00	02 00 01 03	00 00 00 00 01 02 45 09	

3 Tag Inventory Commands

The reader implements 3 tag inventory modes, which are single tag inventory, synchronous inventory and asynchronous inventory.

- Single Tag Inventory only inventories the tag that first responds to the reader.
- Synchronous Inventory command must specify an execution time for inventory. After the command is sent to the reader, the reader performs the inventory of this time period, then returns the number of tags inventoried and the tag information in the memory of the reader can be retrieved with the Get Tag Buffer (0x29) command.
- Asynchronous Inventory contains a set of commands. The host can start inventory with the Start Asynchronous Inventory command and the reader will immediately reply to the host to tell the host if starting was successful. Then it will remain in the continuous inventory state and once a tag is found, it will be sent to the host immediately.

Command	Command Code	Description
Single Tag Inventory	0x21	Inventory a single tag
Synchronous Inventory	0x22	Inventory multiple tags and store the tags in the memory of the reader
Get Tag Buffer	0x29	Get the information of tags inventoried by Synchronous Inventory
Asynchronous Inventory	0xAA	Contains a set of commands (Start AsyncInventory (0xAA48), Stop AsyncInventory (0xAA49), Unrequested Reader-to-Host Commands)

Tag Singulation

All tag inventory and tag access commands support Tag Singulation/Select. If Tag Singulation is used, only tags that conform to the Tag Singulation rule will be inventoried for the inventory operation; for tag access operations, such as read, write, lock, etc., only one tag that conforms to the Tag Singulation rule will be successfully operated on.

Select-Option Bits

The Tag Singulation/Select feature uses the 0th, 1st, 2nd, 3rd and 5th bit of one byte. These bits are called Select-Option Bits. There is an Option field of one byte in most tag operation commands which contains the Select-Option Bits for the Tag Singulation/Select feature. Other bits of the Option field can be used for other purposes.

Non-Sel-Option Bits

There is an Option field of one byte in most tag operation commands. The Option field bits whose position is not Select-Option Bits are called Non-Sel-Option Bits.

The Tag Singulation/Select function is implemented by the fields in the table below.

Field	Values	Description
Select-Option Bits	0x00	Select functionality is disabled. The first tag found will be the tag operated on. No other Tag Singulation field should be specified. Note: When Select is disabled, commands do not support an access password. Use Option=0x05 to send a password without Select Content.
	0x01	Select on the value of the EPC. Require all fields except the Select Address field.
	0x02	Select on contents of the TID memory bank (Gen2 bank 0x02). Requires all fields.
	0x03	Select on contents of the User memory bank (Gen2 bank 0x03). Requires all fields.

	0x04	Select on contents of the EPC memory bank (Gen2 bank 0x01). Requires all fields.
	0x05	Use this option when you need to specify an access password for operation on locked data but don't want to perform a Select. When this option is used, do not pass the Select Content field.
	0x08	Sets Invert Flag. This results in tags NOT matching the specified Tag Singulation Fields will be returned.
	0x20	Changes Select Data Length to 2 bytes, allowing Select Data to be greater than 255 bits.
Select Content	N bytes	Detailed rules for data matching of Tag Singulation/Select.

Select Content

Field	Byte Length	Description
Select Address	4 bytes	The offset in bits within the memory bank. Note: Addresses are always zero-based.
Select Data Length	1 byte	The length of the data (Select Data) to be compared, in bits.
Select Data	N bytes	The data to be compared against.

Example

The following EPC IDs (first 3 bits) are in the field: 0xAAAA (101), 0xCCCC (110), 0x4444 (010) and 0x3000 (001).

Select Option = 0x04 (EPC MemBank)

Select Data Length = 0x01 (1 bit)

Select Data = 0x80

Select Data Address = 0x00000022 (third bit in the EPC ID)

In this case, the third bit of the EPC ID is matched against the first bit of the Select Data value, 1. This would result in the following IDs being returned: 0xAAAA and 0x3000.

Timeout

All tag operation commands have the field timeout (except Asynchronous Inventory). This field specifies the maximum time in milliseconds spent executing the command. If the command completes the operation before this timeout, the reader will reply earlier. The maximum timeout is 65535 ms (0xFFFF).

3.1 Single Tag Inventory (0x21)

Firmware command. This command is to inventory a tag EPC within a specified time.

Host to Reader

Field	Byte Length	Description
Timeout	2 bytes	
Option	1 byte	If Select-Option Bits = 0, the first archived tag is returned; if it is another value, the first tag that matches the selection filter condition is returned. When the 4th bit of this field is 0, only the EPC is returned.
Metadata Flags	2 bytes	This field only exists if bit4 of the Option field is set to 1, otherwise this field does not exist. The field tells the reader what metadata to return.
Select Content	N bytes	The Select Content of Tag Singulation. This field only exists if Tag Singulation is enabled, otherwise this field does not exist.

Metadata Flags

Set multiple bits to 1 to return related data or set all related bits to 1 to return all relevant tag parameters. The content of each bit defined by Metadata Flags is as follow:

Value of Flags	Description
0x0000	No related tag metadata returned. Only tag EPC returned (including tag CRC).
0x0001	Bit0 is set; the number of times the tag archived during the inventory time will be returned.
0x0002	Bit1 is set; the RSSI signal value of the tag will be returned.
0x0004	Bit2 is set; the antenna ID used for archiving the tag will be returned.
0x0008	Bit3 is set; the frequency value used when the tag is archived will be returned.
0x0010	Bit4 is set; the time value when the tag is archived will be returned.
0x0020	Bit5 is set; the RFU reserved value will be returned.
0x0040	Bit6 is set; the tag protocol value currently used by the reader will be returned.
0x0080	Bit7 is set; the data length will be returned (value is 0x0000 in single tag reading command 0x21)

Reader to Host

There are two different data field formats depending on whether the host-to-reader command contains the Metadata Flags field. The first one is Get Tag EPC, when there is no Metadata Flags field in the host-to-reader command. The other is Get Tag EPC and Meta Data.

Get Tag EPC

Field	Byte Length	Description
Option	1 byte	Same as the Option field in the host-to-reader command
EPC	M bytes	The EPC of the tag
TagCRC	2 bytes	The tag CRC in the EPC bank

Get Tag EPC and Meta Data

Field	Byte Length	Description
Option	1 byte	Same as the Option field in the host-to-reader command
Metadata Flags	2 bytes	Same as the Metadata Flags field in the host-to-reader command
Read Count	1 byte	The number of times the tag has been inventoried if the flag was set
RSSI	1 byte	The signal strength in dbm, signed char byte, if the flag was set
Antenna ID	1 byte	Antenna ID from which the tag is inventoried, if flag was set
Frequency	3 bytes	The frequency from which the tag is inventoried in kHz, if the flag was set
Timestamp	4 bytes	The time elapsed from the issuance of an inventory order to the acquisition of this tag in milliseconds, if the flag was set
RFU	2 bytes	Reserved data, if the flag was set
Protocol ID	1 byte	Tag protocol (0x05 means GEN2), if the flag was set
Tag Data Length	2 bytes	Tag data length (value is 0x0000 in single tag reading 0x21), if the flag was set
EPC ID	N bytes	Tag EPC
Tag CRC	2 bytes	Tag CRC

Example

Get Tag EPC (only EPC returned): the following example uses the tag filter function in 1000 ms to inventory tags. Select Option = 0x03 (user bank), Select Address is 32th bit and Select Data is 0x1234.

Host to Reader: FF 0A 21 03 E8 03 00 00 00 20 10 12 E5 AC

Reader to Host: FF M+3 21 00 00 03 Mbytes Tag CRC

Example

Get the antenna ID and the reader system time information while getting the EPC. Metadata Flags = 0x14.

Host to Reader: FF 05 21 01 E8 10 00 14 2F 6D

Reader to Host: FF 16 21 00 00 10 00 14 01 00 BB 5F 04 01 23 45 67 89 AB CD EF 01 23 45 67 E6 C8

3.2 Synchronous Inventory (0x22)

Firmware command. The difference between this command and the Single Tag Inventory command (0x21), is that this command inventories all the tags in the RF field during the set time and returns the number of tags until the timeout expires. After the command is sent, send the Get Tag Buffer (0x29) command to get the tag information. The tag buffer stores up to 299 tags. When 299 tags are accumulated in the tag buffer, the inventory is stopped, and the result is returned.

Host to Reader

Field	Byte Length	Description
Option	1 byte	Non-Sel-Option Bits must all be 0
Search Flags	2 bytes	Currently only bit2 is valid, other settings are 0. When bit2 =1, the inventory embedding command is used, else it is not used
Timeout	2 bytes	Inventory time in milliseconds
Access Password	4 bytes	Access password. If the tag is locked and the embedded command requires a password, send the correct access password, else the password is 0x00000000
Select Content	N bytes	Select Content in Tag Singulation. This field does not exist if the Select Option does not have the Tag Singulation feature enabled
Embedded Command Content	N bytes	The Synchronous Inventory command can be embedded with other tag operation commands. Currently only embedded 0x28 commands are supported. When bit2 of the Search Flags field is 0, this field does not exist

Note: The data sorting in the command is Option first, followed by Search Flags, Timeout, Access Password and Select Content, which is a little different from the typical matching filter format. In addition, only when Select-Option Bits = 0, Access Password must be removed from the command string along with the Select Content field. When Select-Option Bits = 0x05, there is only the Access Password and no Select Content. Select Address of Select Content does not exist when Select-Option Bits = 1.

Embedded Command Content

Field	Byte Length	Description
Embedded Command Count	1 byte	The number of embedded commands; must be 1.
Embedded Command Length	1 byte	The length of the data field of the embedded command in bytes.
Embedded Command Opcode	1 byte	Embedded command code. Now only 0x28 command is supported.
Embedded Values	N bytes	Data field of embedded command

Reader to Host

Field	Byte Length	Description
Option	1 byte	Same as in the host-to-reader command
Search Flags	2 bytes	Same as in the host-to-reader command. If the number of archived tags is greater than 255, bit4 of Search Flags will be set to 1

Tags Found	1 byte	Number of archived tags, if the number of archived tags is greater than 255, tags found is 4 bytes
Embedded Command Result	N bytes	If the embedded command is not used, this field does not exist

Embedded Command Result

Field	Byte Length	Description
Embedded Command Count	1 byte	The number of embedded commands, must be 1.
Embedded Command Opcode	1 byte	Same as in the host-to-reader command.
Operations Succeeded	2 bytes	The number of times the embedded command operation succeeded. Since the same tag may be operated multiple times during the inventory time, the number of successful operations here can only be used as a reference.
Operations Failed	2 bytes	The number of times the embedded command operation failed. Since the same tag may be operated multiple times during the inventory time, the number of operation failures here can only be used as a reference.
Embedded Command Data Returned	N bytes	The data returned by the embedded command operated successfully (If the operation of command 0x28 is successful, it will return the data read by the tag first operated successfully. If it is unsuccessful, there is no such field.)

Note: When the inventory embedded command 0x28 is successfully executed, the command 0x29 can be used to get the archived tag information stored. When the embedded command 0x28 is archived, the length of the read tag memory is up to 32 bytes. The format of the embedded command 0x28 refers to the command 0x28. The operation flow of the inventory embedding command 0x28 is to perform command 0x28 on the tag after inventory each time, and the EPC of the tag will be saved regardless of whether the operation of the command 0x28 is successful or not.

Example

Enable matching filter for inventory and the matching area is EPC. Access Password = 0x00000000

Host to Reader: FF 0F 22 04 00 00 03 E8 00 00 00 00 00 00 78 08 66 DE C0

Reader to Host: FF 04 22 00 00 04 00 00 02 B7 6E

If the number of archived tags is more than 255, the length of Tag Found is 4 bytes and the bit4 of Search Flags is set to 1. If 257 tags are archived, the returned command is as follows: FF 07 22 00 00 04 00 10 00 00 01 01 CRC

Example

Do not enable matching filter function.

Host to Reader: FF 05 22 00 00 00 00 C8 CRC

Reader to Host: FF 04 22 00 00 00 00 00 00 CRC

Example

Without matching filter, the embedded command 0x28 reads 32 words of data starting at address 0 of the USER area.

Host to Reader: FF 11 22 00 00 04 03 E8 01 09 28 00 00 00 03 00 00 00 00 20 CRC

Reader to Host: FF 4A 22 00 00 00 00 04 24 01 28 00 1C 00 29 00 00 ... 00 00 CRC

Example

With matching filter, the matching area is 8 bits starting from the start address 0x00 of the TID area, the matching value is 0xE2 and the inventory embedded command 0x28 reads the 2 words starting from the start word address 0x02 of the RESERVED area, that is, read access password. With access password = 0x22221111.

Host to Reader: FF 1B 22 02 00 04 03 E8 22 22 11 11 00 00 00 00 08 E2 01 09 28 00 00 00 00 00 00 02 02 CRC

Reader to Host: FF 0E 22 00 00 02 00 04 1C 01 28 00 01 00 2F 22 22 11 11 CRC

3.3 Get Tag Buffer (0x29)

Firmware command. This command is used to get the information of tags inventoried by Synchronous Inventory (0x22). The information that can be retrieved includes the EPC of tags and their related meta data.

Host to Reader

Field	Byte Length	Description
Metadata Flags	2 bytes	The meaning is the same as in the 0x21 command
Option	1 byte	0x00 means to retrieve information if tags that has not yet been retrieved. 0x01 means to retrieve the tag information got by the previous 0x29 command.

Reader to Host

Field	Byte Length	Description
Metadata Flags	2 bytes	The meaning is the same as in the host-to-reader command
Option	1 byte	The meaning is the same as in the host-to-reader command
Tag Count	1 byte	The number of tags contained in the returned information
Tag Information	N bytes	The information of each tag is packaged as a data block of Tag EPC and Meta Data. The number of these data blocks is Tag Count. The format of Tag EPC and Meta Data is defined as follow

Get Tag EPC and Meta Data

Field	Byte Length	Description
Read Count	1 byte	The number of times the tag has been inventoried
RSSI	1 byte	The signal strength in dbm, signed char byte
Antenna ID	1 byte	Antenna ID from which the tag is inventoried
Frequency	3 bytes	The frequency from which the tag is inventoried in kHz
Timestamp	4 bytes	The time elapsed from the issuance of an inventory order to the acquisition of this tag in milliseconds
RFU	2 bytes	Reserved data, if the flag was set
Protocol ID	1 byte	Tag protocol (0x05 means GEN2)
Tag Data Length	2 bytes	Bank data length of the tag. The bit length of the tag memory data read when command 0x28 is embedded. If the command 0x28 is not embedded or the operation of 0x28 fails, the value is 0x0000
Tag Data	N bytes	Tag bank data, the length is Tag Data Length/8
EPC Length	2 bytes	The bit length of the EPC, including PC and CRC
PC Word	2 bytes	PC value in EPC bank
EPC ID	N bytes	Tag EPC
Tag CRC	2 bytes	Tag CRC

Example

Get tags with the metadata Read Count, Antenna ID and Timestamp (-> 0x0015).

Host to Reader: FF 03 29 00 15 00 97 55

Reader to Host: FF 34 29 00 00 00 15 00 02 22 01 02 50 CE F6 00 80 31 C1 **11 11 22 22 33 33 44 44 55 55 66 66**
 FB 15 0E 01 04 1D 3D 3C 00 80 30 00 **05 00 00 00 00 00 00 00 00 00 23 54** 4A C8 CRC

The marked bytes are the two **EPCs**.

Example

Get all the tag meta data except the Protocol ID (-> 0x00BF).

Host to Reader: FF 03 29 00 BF 00 4B 22

Reader to Host: FF 4A 29 00 00 00 BF 00 02 07 E3 01 0E 22 2A 00 00 8D 8F 00 00 00 00 00 60 20 00 **11 11 22 22 33 33 44 44** C2 41 07 D0 01 0E 22 2A 00 00 8D 87 00 00 00 00 00 D0 58 00 **11 11 22 22 33 33 44 44 55 55 66 66 77 77 88 88 99 99 00 00 AA AA** 96 86 CRC

Example

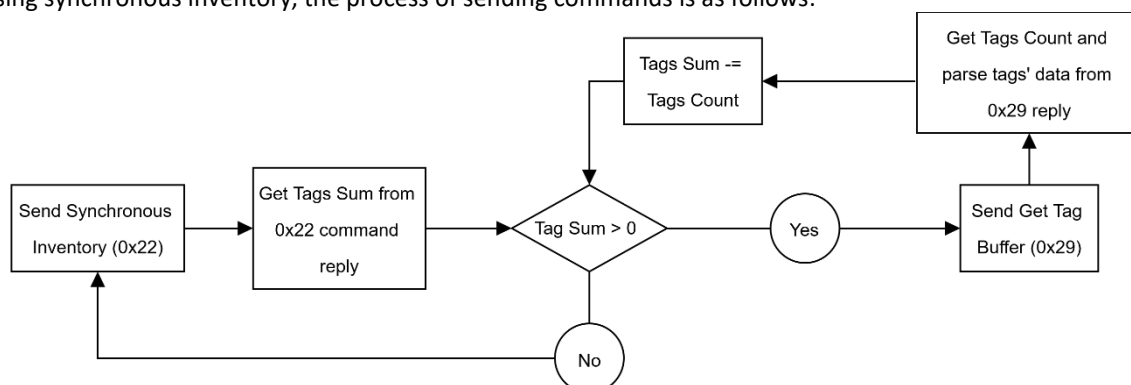
The command 0x22 embeds the command 0x28, reads the first 2 words of address 0 in TID bank and get all the tag meta data except the Protocol ID (-> 0x00BF).

Host to Reader: FF 03 29 00 BF 00 4B 22

Reader to Host: FF 6E 29 00 00 00 BF 00 03 08 D7 01 0D F7 32 00 00 71 9B 00 00 00 20 E2 00 34 12 00 80 30 00 **E2 00 81 81 81 16 02 40 08 20 C7 4C 7E 4C** 08 D5 01 0D F7 32 00 00 71 B5 00 00 00 20 E2 00 60 04 00 D0 58 00 **11 11 22 22 33 33 44 44 55 55 66 66 77 77 88 88 99 99 00 00 AA AA** 96 86 07 D4 01 0D F7 32 00 00 71 8D 00 00 00 20 E2 00 60 04 00 20 00 00 E2 F0 CRC

Remark

Using synchronous inventory, the process of sending commands is as follows:



3.4 Asynchronous Inventory (0xAA)

Firmware command. This inventory mode uses asynchronous mode, the command of starting inventory will return immediately after starting of inventory, the reader is in a continuous inventory state and once the tag is read, it is actively sent to the host. In this way, the inventory performance of the reader is optimal, and applications with higher inventory performance requirements should use this asynchronous inventory.

The asynchronous Inventory includes a set of commands. The command code of all these commands is 0xAA. Different command functions are encapsulated in the Data field. So different commands of asynchronous Inventory use different subcommand codes.

Host to Reader

Field	Byte Length	Description
Subcommand Marker	10 bytes	Always "Moduletech", this field is a string represented by ASCII code
Subcommand Code	2 bytes	Different commands of the asynchronous inventory use different subcommand codes

Subcommand Data	N bytes	Different commands of the asynchronous inventory have different subcommand data
SubCRC	1 byte	The lower 8 bits of the result of adding all data starting from Subcommand Code to the end of Subcommand Data
Terminator	1 byte	Always 0xBB

Reader to Host

Field	Byte Length	Description
Subcommand Marker	10 bytes	Always "Moduletech", this field is a string represented by ASCII code
Subcommand Code	2 bytes	Different commands of the asynchronous inventory use different subcommand codes
Subcommand Data	N bytes	Different commands of the asynchronous inventory have different subcommand data

3.4.1 Start AsyncInventory (0xAA48)

Start the asynchronous inventory.

Host to Reader

Field	Byte Length	Description
Metadata Flags	2 bytes	Same meaning as in the 0x22 command
Option	1 byte	Same meaning as in the 0x22 command
Search Flags	2 bytes	Same meaning as in the 0x22 command. Some bits of this field are used for some other special purpose as explained below
Access Password	4 bytes	Same meaning as in the 0x22 command
Select Content	N bytes	Same meaning as in the 0x22 command
Embedded Command Content	N bytes	Same meaning as in the 0x22 command

Other Special Purpose of Search Flags

The lower 4 bits of the high byte of Search Flags indicate the proportion of time spent resting (carrier and power amplifier turned off to reduce the temperature and avoid overloading the device) during the inventory process. and the value ranges from 0 to 15. If the value is 0-9 the proportion is the value * 5%. If the value is 10-15 the proportion is 50%.

The highest bit of Search Flags indicates whether the reader sends heartbeat packet to the host computer at intervals in asynchronous inventory mode. 1 indicates yes and 0 indicates no. When it is enabled, the reader sends a frame of heartbeat packet to the host computer every 15 seconds. If the asynchronous inventory stops, the reader won't send heartbeat packet.

The second highest bit of Search Flags indicates whether stop the inventory when the enabled antenna determines that new tag can't be read after a period of time and send the reply of "Stop AsyncInventory command" to the host. (This function is used when only one antenna is enabled at a time.) When using the asynchronous inventory mode this feature is often used to extend the single antenna port of the reader to multiple antenna ports externally.

Reader to Host

When the inventory successfully starts or encounters an exception, the reader will immediately reply to the host. There is no Subcommand Data field in the reader-to-host command.

Example

Start asynchronous inventory without Tag Singulation/Select and Embedded Command Content. Metadata Flags is 0x00BF, that means to ask the reader to send all the metadata with tag EPC except for the Protocol ID.

Host to Reader: FF 13 AA 4D 6F 64 75 6C 65 74 65 63 68 AA 48 00 BF 00 80 03 34 BB 29 0F

Reader to Host: FF 0C AA 00 00 4D 6F 64 75 6C 65 74 65 63 68 AA 48 0F 23

Example

Start asynchronous inventory with Tag Singulation/Select and Embedded Command Content. Metadata Flags is 0x00BF.

Host to Reader: FF 2A AA 4D 6F 64 75 6C 65 74 65 63 68 AA 48 00 BF 02 80 07 00 00 00 00 00 00 20 0C E2 00 01 09 28 00 00 02 00 00 00 02 7E BB D0 91

3.4.2 Stop AsyncInventory (0xAA49)

Stop the asynchronous inventory. There is no Subcommand Data field in host-to-reader command and reader-to-host command.

Example

Host to Reader: FF 0E AA 4D 6F 64 75 6C 65 74 65 63 68 AA 49 F3 BB 03 91

Reader to Host: FF 0C AA 00 00 4D 6F 64 75 6C 65 74 65 63 68 AA 49 0F 22

3.4.3 Unrequested Reader-to-Host Commands

When the reader is in the process of asynchronous inventory, there are three commands that the reader may actively send to the host. The commands that are sent without a request are called packet.

Tag Information Packet

As the tag is inventoried, the tag EPC and its metadata information are immediately packaged into a tag information packet and sent to the host. Each tag information packet contains only one tag information. The format of Tag Information Packet fully complies with the Reader-to-Host Communication Framework.

Data Field

Field	Byte Length	Description
Metadata Flags	2 bytes	Same meaning as in the 0x22 command
Tag EPC and Meta Data	N bytes	Same meaning as in the 0x29 command

Heartbeat Packet

When the reader enables the heartbeat function in the command of Start AsyncInventory, the reader will periodically send the heartbeat packet. The format of the heartbeat packet fully complies with the Reader-to-Host Communication Framework.

Data Field

Field	Byte Length	Description
Heartbeat Marker	4 bytes	Always "XTSJ", represented by ASCII code
Search Flags	N bytes	Same meaning as in the 0x29 command
State Data		

3.4.4 Remark

If the reader receives commands (including Start Asynchronous Inventory command) other than Stop AsyncInventory command during asynchronous inventory process, it exits asynchronous inventory and returns an unsuccessful answer of the invalid command. The error status code is 0xAA49.

If the reader encounters an exception during asynchronous inventory process, it exits asynchronous inventory and returns with an error status code.

If the reader is not in an asynchronous inventory process and receives the Stop AsyncInventory command, it returns successful execution.

4 Tag Access Commands

Tag access operations include operations such as reading, writing, locking and killing operation, as shown in the table below.

Command	Command Code	Description
Write Tag Data	0x23	Write data to the specified address in the specified tag memory
Write Tag EPC	0x24	Update the tag EPC
Lock Tag	0x25	Lock or unlock the specified memory areas
Kill Tag	0x26	Destroy tag
Read Tag Data	0x28	Read the contents of the tag storage area

4.1 Write Tag Data (0x24)

Firmware command. This command is to write data to the specified address in the tag bank. The first tag in response to the reader will be written.

Host to Reader

Field	Byte Length	Description
Timeout	2 bytes	
Option	1 byte	Same meaning as in the 0x22 command. Non-Sel-Option Bits must be 0.
Write Address	4 bytes	Starting address to write. Word address (16 bits) starting from 0.
Write MemBank	1 byte	0x00 = Reserved bank, 0x01 = EPC bank, 0x02 = TID bank, 0x03 = USER bank
Access Password	4 bytes	Access password. If the memory bank is not locked, the access password is 0x00000000, else the correct password must be given
Select Content	N bytes	
Write Data	N bytes	Data to write, the data length must be a multiple of 2 bytes. It is only possible to write up to 32 words at a time (64 bytes)

Example

Disable matching filter function. Write 0xAAAABBBBCCCCDDDD to the start address 1 of the USER area.

Host to Reader: FF 10 24 03 E8 00 00 00 00 01 03 AA AA BB BB CC CC DD DD C7 B3

Example

Disable matching filter function and write 0xAAAABBBBCCCCDDDD to Reserved area

Host to Reader: FF 10 24 03 E8 00 00 00 00 00 00 AA AA BB BB CC CC DD DD 58 E2

Example

Enable matching filter function. Write MemBank=0x00, Write Address=0x00000000,

Write Data=0xAAAABBBBCCCCDDDD, Access Password=0xCCCCDDDD, Select MemBank=EPC bank,

Select Address(bits)=0x00000020, Select Data Length(bits)=0x0C, Select Data=0x1110

Host to Reader: FF 1B 24 03 E8 04 00 00 00 00 00 CC CC DD DD 00 00 00 20 0C 11 10 AA AA BB BB CC CC DD DD 26 AA

Remark

- When Option=0x05, there is only the access password, no Select Content field.
- When Option=0x00 or 0x01, unnecessary subfields in the Select Content field should not appear in the command (e.g. access password).

4.2 Write Tag EPC (0x23)

Firmware command. Update the tag EPC command. The difference to the 0x24 command is that it automatically changes the value of the bit indicating the EPC length in the PC according to the data length written by the user. The command writes the EPC ID to the address beginning with 0x20 (bits) in the EPC area.

Host to Reader

Field	Byte Length	Description
Timeout	2 bytes	
Option	1 byte	Same meaning as in the 0x22 command. Non-Sel-Option Bits must be 0.
RFU	1 byte	Exists only if Option=0x00, must be 0x00 then.
Access Password	4 bytes	Access password. If the memory bank is not locked, the access password is 0x00000000, else the correct password must be given
Select Content	N bytes	
Tag EPC ID	N bytes	The EPC code to write, up to 496-bit (depending on tag)

Example

Disable matching filter function.

Host to Reader: FF 0C 23 03 E8 00 00 11 11 22 22 33 33 44 44 63 2C

Example

Enable matching filter. The matching filter area is EPC area, the matching address is 0x00000020 (bits), the matching data length is 0x08 bits, the matching data is 0x11 and the matching is inverted, meaning it will respond to tags that don't have 0x11 as the first 8 bits in the EPC area.

Host to Reader: FF 19 23 03 E8 0C 00 00 00 00 00 00 20 08 11 11 11 22 22 33 33 44 44 55 55 66 66 57 3E

4.3 Lock Tag (0x25)

Firmware command. This command is to lock or unlock specified memory areas.

Host to Reader

Field	Byte Length	Description
Timeout	2 bytes	
Option	1 byte	Same meaning as in the 0x22 command. Non-Sel-Option Bits must be 0. Option=0x05 cannot be used here
Access Password	4 bytes	Access password
Mask Bits	2 bytes	The Mask Bits are specified in the Class-1 Generation-2 UHF RFID specification
Action Bits	2 bytes	The Action Bits are specified in the Class-1 Generation-2 UHF RFID specification
Select Content	N bytes	

Example

EPC ID = 0x111122223333444455556666, access password = 0x11223344, enable matching filter and lock the EPC bank.

Host to Reader: FF 18 25 03 E8 01 11 22 33 44 00 20 00 20 60 11 11 22 22 33 33 44 44 55 55 66 66 9E 7A

4.4 Kill Tag (0x26)

Firmware command.

Host to Reader

Field	Byte Length	Description
Timeout	2 bytes	
Option	1 byte	Same meaning as in the 0x22 command. Non-Sel-Option Bits must be 0. Option=0x05 cannot be used here
Kill Password	4 bytes	Kill password of a tag
RFU	1 byte	Must be 0x00
Select Content	N bytes	

Example

Disable matching filter function. Kill password = 0x11223344

Host to Reader: FF 08 26 03 E8 00 11 22 33 44 00 91 16

Example

Use matching filter and the filter bank is USER.

Host to Reader: FF 10 26 03 E8 03 11 22 33 44 00 00 00 00 18 11 11 22 BF 40

4.5 Read Tag Data (0x28)

Firmware command. Read the contents of the tag storage area.

Host to Reader

Field	Byte Length	Description
Timeout	2 bytes	
Option	1 byte	If the 4th bit is 1, the command has the Metadata Flags field, else it doesn't.
Metadata Flags	2 bytes	This field only exists if the 4th bit of the Option field is 1
Read MemBank	1 byte	Memory area: 0x00 = Reserved bank, 0x01 = EPC bank, 0x02 = TID bank, 0x03 = User bank
Read Address	4 bytes	Read start address (word address, 16 bits), starting from 0
Word Count	1 byte	Number of blocks to read, maximum of 96 words at a time
Access Password	4 bytes	Access password is 0x00000000 if the memory area is not locked, else the correct password must be provided
Select Content	N bytes	

Reader to Host

Field	Byte Length	Description
Timeout	2 bytes	
Metadata Flags	2 bytes	If the host-to-reader command contains this field, the response also contains it, else not
Read Count	1 byte	The number of times the tag has been inventoried
RSSI	1 byte	The signal strength in dbm, signed char byte
Antenna ID	1 byte	Antenna ID from which the tag is inventoried
Frequency	3 bytes	The frequency from which the tag is inventoried in kHz
Timestamp	4 bytes	The time elapsed from the issuance of an inventory order to the acquisition of this tag in milliseconds
RFU	2 bytes	Reserved data, if the flag was set
Protocol ID	1 byte	Tag protocol (0x05 means GEN2)
Tag Data Length	2 bytes	Always 0x0000

Data Read	N bytes	The data read
-----------	---------	---------------

Example

Disable the match filter function and read the 2 words starting with word address 1 in the TID area.

Host to Reader: FF 09 28 03 E8 00 02 00 00 00 01 02 C1 F3

Reader to Host: FF 05 28 00 00 00 60 04 01 35 13 04

Example

Enable the matching filter function, read the 3 words starting with word address 1 in the TID area, password=0x00000000, the matching area is TID, the starting address is 0x10, the matching length is 4 bits and the matching data is 0x60.

Host to Reader: FF 13 28 03 E8 02 02 00 00 00 01 03 00 00 00 00 00 00 10 04 60 7C 91

Reader to Host: FF 07 28 00 00 02 60 04 01 35 F8 69 6C 29

Example

Read tag data with metadata flags antenna ID and timestamp.

Host to Reader: FF 15 28 03 E8 14 00 14 00 00 00 00 02 02 00 00 00 00 00 00 78 08 34 9C 0E

Reader to Host: FF 0C 28 00 00 14 00 14 02 00 00 00 15 12 34 56 78 CRC

5 Setting Commands

The Set commands are used to set configurable values in the firmware. Since the values are not stored in flash, these values are reset to the default values whenever the application firmware is restarted.

Command	Command Code	Description
Set Antenna Ports	0x91	Configure the antenna ports for tag access or inventory operation and tx power
Set Current Tag Protocol	0x93	Set the tag protocol for operations
Set Frequency Hopping	0x95	Set the frequency hopping table and regulatory hopping time
Set GPO	0x96	Set and get the status of GPO pins
Set Current Region	0x97	Set the current region of the reader
Set Reader Configuration	0x9A	Set configuration options of the reader
Set Tag Protocol Configuration	0x9B	Set protocol-specific configuration parameters

5.1 Set Antenna Ports (0x91)

Firmware command. This command uses the concept of a logical antenna number. The logical antenna number of a reader is the same as the physical antenna port number of a reader which is marked with a number on the reader. The antenna is classified into antennas used for reception and antennas used for transmission. The logical antenna number of antennas used for reception is called RX Logical Antenna Number. The logical antenna number of antennas used for transmission is called TX Logical Antenna Number.

This reader uses transceiver integrated antenna mode, that is, when a physical antenna port of the reader works, it uses this port to send and receive signals.

There are multiple formats for Set Antenna Ports command.

Host to Reader

This format is used to set the antenna for tag access operations; every kind of tag access operation can only specify one antenna for the operation.

Field	Byte Length	Description
Option	1 byte	Always 0x00
TX Logical Antenna Number	1 byte	
RX Logical Antenna Number	1 byte	

Set Antennas for Tag Inventory Option

The Tag inventory operation can use one or multiple antennas.

Field	Byte Length	Description
Option	1 byte	Always 0x02
TX, RX Logical Antenna Number pairs	M*2 bytes	M 2-byte TX, RX Logical Antenna Number pairs, after multiple Logical Antennas are set, the order of switching antennas of tag inventory is the same as the order of TX, RX Logical Antenna Number pairs in the command

Set the Power of Antennas

Set the transmission power of the antenna ports.

Field	Byte Length	Description
Option	1 byte	Always 0x03
TX Logical Antenna Power Configuration	M*5 bytes	M TX Logical Antenna Power Configurations

TX Logical Antenna Power Configuration

Field	Byte Length	Description
TX Logical Antenna Number	1 byte	
Read Power	2 bytes	Transmission power of reading related operations, unit is 0.01 dbm but only has a precision of 1 dbm
Write Power	2 bytes	Transmission power of writing related operations, unit is 0.01 dbm but only has a precision of 1 dbm

Set the Power and Settling Time of antennas

Set the transmission power of the antenna ports.

Field	Byte Length	Description
Option	1 byte	Always 0x04
TX Logical Antenna Power and Settling Time Configuration	M*7 bytes	M TX Logical Antenna Power and Settling Time Configurations

TX Logical Antenna Power and Settling Time Configuration

Field	Byte Length	Description
TX Logical Antenna Number	1 byte	
Read Power	2 bytes	Transmission power of reading related operations, unit is 0.01 dbm but only has a precision of 1 dbm
Write Power	2 bytes	Transmission power of writing related operations, unit is 0.01 dbm but only has a precision of 1 dbm
Settling Time	2 bytes	The settling time, in microseconds, to be used when this antenna is active

Example

Set the Antenna 1 for Tag Access Operations (Option=0x00).

Host to Reader: FF 03 91 00 01 01 62 87

Example

Set Antennas 1 and 4 for Tag Inventory Operation (Option=0x02).

Host to Reader: FF 05 91 02 01 01 04 04 2B C6

Remark

Antenna port 1 is enabled by default when the reader is powered on. The default initial transmission power (read/write) of all antennas may not be the maximum power output value.

The values of Read Power and Write Power can be set differently. Each antenna can also have different read/write power values.

5.2 Set Current Tag Protocol (0x93)

Firmware command. Set the tag protocol for operations. Currently the readers only support Gen2 protocol. The Gen2 protocol is used by default when the reader is powered on.

Host to Reader

Field	Byte Length	Description
Current Protocol	2 bytes	Must be 0x0005 (Gen2 protocol)

Example

Host to Reader: FF 02 93 00 05 51 7D

5.3 Set Frequency Hopping (0x95)

Firmware command. The Set Frequency Hopping command sets the frequency hopping table of reader and, optionally, the regulatory hopping time, to use when hopping. Each frequency is encoded as a 32-bit value in kHz. The maximum number of frequencies which can be set is 50. The set-table frequencies of a certain work region can refer to Region Frequencies Table described in Set Current Region section. This command has two formats for setting the frequency hopping table and regulatory hopping time.

Host to Reader

Set Frequency Hopping Table

Field	Byte Length	Description
Frequencies	M*4 bytes	M frequencies, each frequency is 4 bytes length

Set Regulatory Hopping Time: This format is reserved for future use and does not work currently. The reader uses 400 ms frequency hopping time by default.

Field	Byte Length	Description
Option	1 byte	Must be 0x01
Hop time	4 bytes	Frequency hopping time in milliseconds

Example

Set Frequency Hopping Table with 3 frequencies: 915250 kHz, 903250 kHz and 926750 kHz.

Host to Reader: FF 0C 95 00 0D F7 32 00 0D C8 52 00 0E 24 1E E5 24

5.4 Set GPO (0x96)

Firmware command. This command has two formats for setting GPO and getting GPO status.

Host to Reader

Set GPO

Field	Byte Length	Description
GPO Number and Status pairs	M*2 bytes	M GPO number and status pairs, each pair is 2 bytes

Get GPO: No data field

Reader to Host

When getting GPO status, the format of the data field is as follows:

Field	Byte Length	Description
Status of GPO pins	N bytes	The status of all the GPO pins of the reader in numerical order

Example

Set GPO.

Host to Reader: FF 04 96 01 01 02 00 2F 68

Example

Get GPO status. (device in example has 3 outputs)

Reader to Host: FF 03 96 00 00 01 00 01 EE 3A

5.5 Set Current Region (0x97)

Firmware command.

Host to Reader

Field	Byte Length	Description
Region Code	1 byte	Refer to the Region Code Table below

Region Code Table

Region Name	Region Code
North America (902-928)	0x01
China 1 (920-925)	0x06
European (865-867)	0x08
China 2 (840-845)	0x0A
Full Frequency Band (840-960)	0xFF

Example

Set region to Europe.

Host to Reader: FF 01 97 08 CRC

Remark

The hop table of different regions can only contain certain specific frequencies in the table below except Full Frequency Band. So the Set Frequency Hopping command can only select the frequencies which belong to the region which the reader is working on. The Full Frequency Band can use any frequency in the range 840-960 MHz. The frequencies in the Region Frequencies Table are the default hop table for each region after using the Set Current Region command.

Region Frequencies Table

Region Name	Frequencies (kHz)
North America (902-928)	915750, 915250, 903250, 926750, 926250, 904250, 927250, 920250, 919250, 909250, 918750, 917750, 905250, 904750, 925250, 921750, 914750, 906750, 913750, 922250, 911250, 911750, 903750, 908750, 905750, 912250, 906250, 917250, 914250, 907250, 918250, 916250, 910250, 910750, 907750, 924750, 909750, 919750, 916750, 913250, 923750, 908250, 925750, 912750, 924250, 921250, 920750, 922750, 902750, 923250

China 1 (920-925)	921375, 922625, 920875, 923625, 921125, 920625, 923125, 921625, 922125, 923875, 921875, 922875, 924125, 923375, 924375, 922375
European (865-867)	865700, 866300, 866900, 867500
China 2 (840-845)	841375, 842625, 840875, 843625, 841125, 840625, 843125, 841625, 842125, 843875, 841875, 842875, 844125, 843375, 844375, 842375
Full Frequency Band (840-960)	840000, 850000, 860000, 870000, 880000, 890000, 900000, 910000, 920000, 930000, 940000, 950000, 960000

5.6 Set Reader Configuration (0x9A)

Firmware command. This command is used to set several configuration options of the reader.

Host to Reader

Field	Byte Length	Description
Option	1 byte	Must be 0x01
Key	1 byte	Indicates a configuration item
Value	1 byte	The value of a configuration item

Key Value Description Table

Key	Value	Description
0x00: Use Antenna Port as Unique Identifier of Tag Buffer Entry	0x00	Antenna port is a unique characteristic (default)
	0x01	Antenna port is ignored for Tag Buffer Entries
0x06: Record the highest RSSI	0x00	The RSSI Tag metadata value is the value for the read tag for each buffer entry (default)
	0x01	The RSSI Tag metadata value will be the highest value recorded during the Read Tag Multiple search operation (0x22)
0x08: Tag Data as Unique Identifier	0x00	Tag Data is a unique characteristic of a Tag Buffer Entry
	0x01	Tag Data is ignored for Tag Buffer Entry uniqueness (default)

Example

Set to use Antenna Port as unique identifier of Tag Buffer Entry.

Host to Reader: FF 03 9A 01 00 01 AF 5C

5.7 Set Tag Protocol Configuration (0x9B)

Firmware command. The command is used to set protocol-specific configuration parameters.

Host to Reader

Field	Byte Length	Description
Protocol Value	1 byte	Must be 0x05 (Gen2 protocol)
Parameter	1 byte	Indicates a parameter of the protocol
Option	1 byte	An option of a parameter, not for all parameters
Value	1 byte	Value of a parameter with an option, not for all parameters

Protocol Parameter Option Table

Parameter	Option	Value
0x00: Session used for tag inventory	No such field	0x00: Session 0 (default)
		0x01: Session 1
		0x02: Session 2

		0x03: Session 3
0x01: Target used for tag inventory	0x01: Static target	0x00: Target A (default)
		0x01: Target B
	0x00: Dynamic target	0x00: Start Inventory from A and transfer to B until no tag is found. (Only for 0x22 command)
		0x01: Start Inventory from B and transfer to A until no tag is found. (Only for 0x22 command)
0x02: Miller coding options (RFU)	No such field	0x01: M = 2
		0x02: M = 4 (default)
		0x03: M = 8
0x12: Q-Value	0x00: Dynamic Q (default)	No such field
	0x01: Static Q	0x00 – 0x0F (1 byte, Q value)

Example

Set to Session 1 for inventory.

Host to Reader: FF 03 9B 05 00 01 DC E9

Example

Set to static Q for inventory (Q=3).

Host to Reader: FF 04 9B 05 12 01 03 80 AC

Example

Set to target B for inventory.

Host to Reader: FF 04 9B 05 01 01 01 A2 FC

6 Getting Commands

The Get commands listed in the table below are used to get parameters, options and working state from the reader.

Command	Command Code	Description
Get Antenna Ports	0x61	Get the configuration of the antenna ports for tag access or inventory operations and tx power, etc
Get Current Tag Protocol	0x63	Get the tag protocol for operations
Get Frequency Hopping	0x65	Get the frequency hopping table and regulatory hopping time
Get GPI	0x66	Get the status of GPI pins
Get Current Region	0x67	Get the current region of the reader
Get Available Regions	0x71	Get the available regions supported by the reader
Get Reader Configuration	0x6A	Get configuration options of the reader
Get Tag Protocol Configuration	0x6B	Get protocol-specific configuration parameters
Get Current Temperature	0x72	Get the current temperature of the reader

6.1 Get Antenna Ports (0x61)

Firmware command. This command returns the current antenna configuration including which antennas are set to transmit and receive, and which ports have antennas attached. There are multiple formats for the command.

Host to Reader

Field	Byte Length	Description
Option	1 byte	Refer to the table below

Value of Option	Description
0x00	If the antenna for Tag Access Operations was set using the 0x91 command before, this command returns the antenna port set. If the 0x91 command was not used to set the antenna for tag access operations, the lowest logic antenna number will be returned.
0x02	Get the logical antennas for inventory
0x03	Get reading and writing transmission power of all logical antenna ports
0x04	Get reading and writing transmission power and antenna setting time for all logical antenna ports
0x05	Get the connection status of all logical antenna ports

Example

Get the Antenna for Tag Access Operations.

Host to Reader: FF 01 61 00 BD BD

Reader to Host: FF 02 61 00 00 03 03 4C 20

6.2 Get Current Tag Protocol (0x63)

Firmware command. Get the tag protocol for operations. Currently the reader only supports GEN2 protocol.

Reader to Host

Field	Byte Length	Description
Current Protocol	2 bytes	Always 0x05 (GEN2 protocol)

Example

Reader to Host: FF 02 63 00 00 00 05 21 46

6.3 Get Frequency Hopping (0x65)

Firmware command. This command is used to get the information of frequency hopping and frequency hopping time. The command has two formats for getting the frequency hopping table and regulatory hopping time.

Host to Reader

Get Frequency Hopping Table: There is no data in the host-to-reader command.

Get Regulatory Hopping Time:

Field	Byte Length	Description
Option	1 byte	Must be 0x01

Reader to Host

Get Frequency Hopping Table

Field	Byte Length	Description
frequencies	M*4 bytes	M frequencies, each frequency is 4 bytes long

Get Regulatory Hopping Time

Field	Byte Length	Description
Option	1 byte	Must be 0x01
Hop time	4 bytes	Frequency hopping time in milliseconds

Example

Get Frequency Hopping Table.

Reader to Host: FF 0C 65 00 00 00 0D F9 26 00 0D C8 52 00 0E 24 1E 2C B5

Example

Get Regulatory Hopping Time.

Host to Reader: FF 01 65 01 B9 BC

Reader to Host: FF 05 65 00 00 01 00 00 01 90 4B 6C

6.4 Get GPI (0x66)

Firmware command. This command gets the status of all GPI pins of the reader.

Reader to Host

Field	Byte Length	Description
Status of GPI pins	N bytes	The status of all the GPI pins of the reader in numerical order

Example

Device in example has 4 GPI pins.

Reader to Host: FF 04 66 00 00 00 01 00 01 F3 E6

6.5 Get Current Region (0x67)

Firmware command.

Reader to Host

Field	Byte Length	Description
Region Code	1 byte	Refer to the Region Code Table in section 5.5.

Example

Reader to Host: FF 01 67 00 00 01 B4 80

6.6 Get Available Regions (0x71)

Firmware command.

Reader to Host

Field	Byte Length	Description
Region Codes	N bytes	N Region Codes, each Region Code is one byte, refer to the Region Code Table in section 5.5.

Example

Reader to Host: FF 02 71 00 00 01 06 0D 46

6.7 Get Reader Configuration (0x6A)

Firmware command. The command is used to get several configuration options on the reader.

Reader to Host

Field	Byte Length	Description
Option	1 byte	Must be 0x01
Key	1 byte	Indicates a configuration item, refer to the Key Value Description Table in section 5.6.
Value	1 byte	The value of a configuration item, refer to the Key Value Description Table in section 5.6.

Example

Reader to Host: FF 03 6A 00 00 01 00 01 3E 45

6.8 Get Protocol Configuration (0x6B)

Firmware command. This command is used to get protocol-specific configuration parameters.

Host to Reader

Field	Byte Length	Description
Protocol Value	1 byte	Must be 0x05 (GEN2 protocol)
Parameter	1 byte	Indicates a parameter of the protocol, refer to the Protocol Parameter Option Table in section 5.7.

Reader to Host

Field	Byte Length	Description
Protocol Value	1 byte	Must be 0x05 (GEN2 protocol)

Parameter	1 byte	Indicates a parameter of the protocol, refer to the Protocol Parameter Option Table in section 5.7.
Option	1 byte	An option of the parameter, not for all parameters, refer to the Protocol Parameter Option Table in section 5.7.
Value	1 byte	The value of the parameter, not for all parameters, refer to the Protocol Parameter Option Table in section 5.7.

Example

Get session configuration for inventory.

Host to Reader: FF 02 6B 05 00 3A 6F

Reader to Host: FF 03 6B 00 00 05 00 00 08 74

Example

Get target configuration for inventory.

Host to Reader: FF 02 6B 05 01 3A 6E

Reader to Host: FF 04 6B 00 00 05 01 01 00 2C 68

6.9 Get Current Temperature (0x72)

Firmware command. The maximum operating temperature of the reader is about 85 °C and the reader will report an error when the temperature exceeds this value.

Reader to Host

Field	Byte Length	Description
Temperature	1 byte	The current temperature of the reader

Example

Reader to Host: FF 01 72 00 00 27 48 20

7 Status Code

The following table describes the detailed meaning of each status code.

Status Code	Description
0x0000	The operation was successful
0x0100	The actual length of the data is different from the value of the length byte
0x0101	Unavailable command
0x0105	Unavailable parameter value
0x010A	Unavailable baud rate
0x010B	Unavailable region selection
0x0200	App Firmware layer program CRC is incorrect
0x0302	Flash undefined error, flash writing failed
0x0400	No tag found
0x0402	Protocol unavailable
0x040A	General tag error (reading/writing lock, kill command)
0x040B	Length of reading memory out of limit (only 96 words can be read at a time)
0x040C	Unavailable kill password
0x0420	GEN2 protocol error
0x0423	Memory overrun bad PC
0x0424	Mem locked
0x042B	Insufficient power
0x042F	Non-specific error
0x0430	Unknown error
0x0500	Unavailable frequency value
0x0504	Temperature overrun
0x0505	High return loss
0x7F00	Unknown error, serious error
0xFF01	Error occurs in initializing timer, reading/writing Flash function, GPIO configuration function
0xFF02	OEM initialization failed
0xFF03	Reader command interface function initialization failed
0xFF04	MAC register reading/writing function initialization failed
0xFF05	MAC register initialization failed
0xFF06	R2000 and ARM7 communication interface initialization failed
0xFF07	R2000 and ARM7 communication detection failed
0xFF08	R2000 and ARM7 communication detection failed
0xFF09	GPIO configuration error
0xFF0A	R2000 chip register initialization failed
0xFF0B	EPC protocol function interface initialization failed
0xFF0C	OEM mapping MAC register initialization failed
0xFF0D	Serial port initialization failed
0xFF0E	APP main handler interface error