Impinj RFID Series Protocol Document

EX10 Series Module Communication Protocol

Ver2024-12-11

Content

1 Introduction....3
2 Overview....3
    2.1 Module Operation Mechanism....3
    2.2 Module Certification Region....5
    2.2 Command Set Structure Classification....6
    2.3 Basic Command Execution Process....7
3 Command Protocol and Data Format....12
    3.1 Common Communication Protocol format....13
    3.2 Extended Command Communication Protocol Format....15
    3.3 Command Construction and Parsing....17
4 Bootloader Command....19
    4.1 Write Flash(0x01)....20
    4.2 Read Flash(0x02)....22
    4.3 Get version(0x03)....24
    4.4 Start APP Firmware(0x04)....27
    4.4Set Baud Rate(0x06)....28
    4.5 Verify APP Firmware(0x08)....28
    4.6 Start Bootloader(0x09)....29
    4.7 Get Current Running Layer(0x0C)....31
    4.8 Get Serial Number(0x10)....33
5 Tag Inventory Command....36
    5.1 Commonly Used Domain Descriptions....38
        5.1.1 Option....38
        5.1.2 Tag Singulation....41
        5.1.3 Metadata Flags....43
        5.1.4 Metadata and Tag EPC....44
        5.1.5 Timeout....46
    5.2 Single Tag Inventory(0x21)....47
    5.3 Synchronous Inventory(0x22)....53
    5.4 Get Tag Buffer(0x29)....62
        5.4.1 IMPINJ FASTID Function....66
    5.5 Clear buffer command (0x2A)....73
    5.6 Asynchronous Inventory....75
        5.6.1 Asynchronous Inventory(0xAA48)....75
        5.6.2 Asynchronous Inventory actively upload data packets....84
        5.6.3 Stop Asynchronous Inventory(0xAA49)....92
        5.6.4 EX Asynchronous Inventory(0xAA58)....93
        5.6.5 Stop EX Asynchronous Inventory (0xAA59)....96

Impinj RFID Series Protocol Document

6 Tag Access Commands......97
    6.1 Write EPCID(0x23)......98
    6.2 Write Memory Bank (0x24)......104
    6.3 Lock Tags (0x25)......111
    6.4 Kill Tags(0x26)......115
    6.5 Read Tags Memory Bank (0x28)......118
    6.6 BlockWrite Tags Memory Bank (0x2D)......123
7 Setting Commands......127
    7.1 Set power/enable antenna ports(0x91)......128
    7.2 Set Protocol: GEN2(0x93)......133
    7.3 Set the frequency hopping table, antenna dwell time, and duty cycle(0x95)......134
    7.4 Set GPOGPO(0x96)......137
    7.5 Set the Current Working Area(0x97)......139
    7.6 Set Standby Low Power Mode(0x98)......141
    7.7 Set Unique Configuration Parameters (0x9A)......142
    7.8 Set Protocol Comfigration Parameters (0x9B)......146
8 Get Commands......149
    8.1 Get antenna port configuration (0x61)......151
    8.2 Get transmit power information (0x62)......156
    8.3 Get the current tag protocol(0x63)......157
    8.4 Get frequency hopping table/antenna dwell time/duty cycle(0x65)......159
    8.5 Get GPI(0x66)......163
    8.6 Get the work area code(0x67)......164
    8.7 Get low power consumption in standby(0x68)......166
    8.8 Get unique configuration(0x6A)......168
    8.9 Get protocol configuration parameters(0x6B)......169
    8.10 Get available tag protocols(0x70)......172
    8.11 Get the available frequency regions(0x71)......174
    8.12 Get module temperature(0x72)......175
9 Command for permanently saving configuration parameters(0xAA40)......176
    9.1 The working antenna and power are enabled by default at power-on......178
        9.1.1 Get the default working antenna and power enabled at power-on......178
        9.1.2 Set the default working antenna and power at power-on......179
    9.2 Default working frequency and frequency hopping time at power-on......182
        9.2.1 Get the default working frequency at power-on......182
        9.2.2 Set the default working frequency at power on......183
    9.3 Default working frequency region at power-on......185
        9.3.1 Get the default working frequency region when powering on......185
        9.3.2 Set the default working frequency region at power-on......185
    9.4 Default is unique when powering on......187
        9.4.1 Get the default unique value when power on......187
        9.4.2 Set the default unique setting at power on......188
    9.5 Default protocol at power on......189
        9.5.1 Get default protocol at power on......189

9.5.2 Set the default protocol at power on....190
9.6 Whether to run to APP when power on....191
9.6.1 Get whether to run to APP when powered on....191
9.6.2 Set whether to run to APP when powered on....191
9.7 Default baud rate at power on....193
9.7.1 Get the default baud rate at power-on....193
9.7.2 Set the default baud rate at power on....194
9.8 Restore factory default settings....195
9.9 Prepare to upgrade the firmware command....196
10 Other commands....197
10.1 Standing wave detection(0xAA4A)....197
10.2 Multi-label matching filter (0xAA4C)....202
10.3 Private Yichain Temperature Label(0xAA50)....206
10.4 Private iLian light tag (0xAA51)....211
10.5 Configure antenna and power for carrier modulation (0xAA04)....216
10.6 Configure the frequency of carrier modulation(0xAA27)....218
10.7 Transmit carrier wave and modulation(0xAA31)....219
10.8 Set RSSI filter threshold(0xAA5B)....222
10.9Temperature and humidity LED tag(0xAA5A)....225
10.9.1 TAGTYPE=0001：Inno Temperature....227
10.9.2 TAGTYPE=0007：NXP U8/U8M....230
10.9.3 TAGTYPE=0009：SCR409 Temperature....233
10.10 Flip the S2 channel of the tag to side A(0xAA4D)....235
Appendix....237
Appendix 1 Status Code....237
Appendix 2 Regions and Regional Frequency Table....241
Appendix 3 Gen2 Tag Memory Structure....244
Appendix 4 C language example of command CRC....246
Appendix 5 C language example of TagCRC_EPCCRC....247
Appendix 6 SubCRC C language example....248

1 Introduction

Overview

This document designs the serial communication between the control end (host or upper machine) and the EX10 series module (module) based on a request/reply communication mechanism, and specifies the communication data protocol format between the host and the module. The design of both the control end and the module must comply with this protocol.

Impinj RFID Series Protocol Document

Scope

This document applies to EX10 series modules (modules using the IMPINJ E310/E510/E710/E910 RF chips).

Target readers of this document: Developers, API interface developers, system integration developers, and technical support personnel.

Common Terminology

Word/Block，equal to 2 Byte，or 16 bits (the smallest read/write unit defined by the protocol).

Number followed by (2) indicates binary format, e.g., 10000001(2).

Number prefixed with 0x indicates hexadecimal, e.g., 0xFA (unless otherwise specified, all numbers are in hexadecimal).

Instruction/Command refers to the operation code defined by the protocol.

One Frame of Instruction represents a complete set of instruction data.

Document Format Explanation

Blue text indicates important terms,Red text indicates that require extra attention.

Items marked with * are explained in detail in the "Notes" section later in the document.

References

EPC™ Radio-Frequency Identity Protocols Class-1 Generation-2 UHF RFID

Protocol for Communications at 860 MHz–960 MHz Version 1.2.0

2 Overview

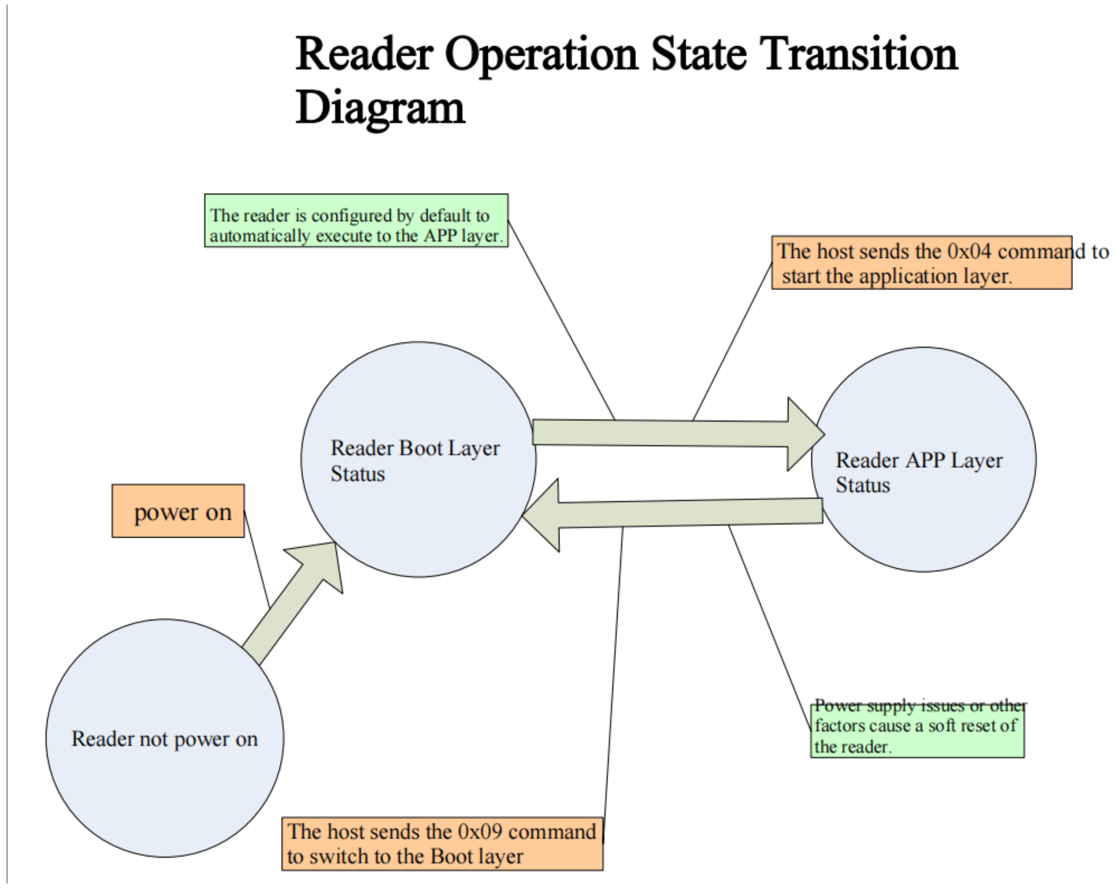
2.1 Module Operation Mechanism

A bare-metal module, when shipped, has the Bootloader layer (BOOT layer, Startup layer) and the App Firmware layer (APP layer, Application layer) firmware programmed. The RFID-related functions can only be used in the APP layer.

After powering on, the module enters the BOOT layer and can execute instructions from the BOOT layer. There are two ways to enter the APP layer:
<1>The host sends the "Start APP command.
<2>Pre-configure "Power-on to APP."

Once in the APP layer, the module can execute instructions from the APP layer. There are three ways to return to the BOOT layer:
<1>If "Power-on to APP" is not configured, the host sends the "Start BOOT command."
<2>The host first sends the "Prepare for Upgrade command," then sends the "Start BOOT command."
<3>If "Power-on to APP" is not configured, and factors such as unstable power supply lead to a reset.

Impinj RFID Series Protocol Document


Reader Operation State Transition Diagram
The reader is configured by default to automatically execute to the APP layer.
The host sends the 0x04 command to start the application layer.
Reader Boot Layer Status
Reader APP Layer Status
power on
Reader not power on
Power supply issues or other factors cause a soft reset of the reader.
The host sends the 0x09 command to switch to the Boot layer

1 The module can only execute the corresponding supported commands in the BOOT or APP layer; otherwise, it will return error code 0101.

2 When the module is in the APP layer and a configuration command (non-permanent) is used, the configuration will be lost (reset to default values) if the module switches to the BOOT layer. The default value can be modified using the permanent save command.

3 If "Power-on to APP" is configured, the module will automatically transition from the BOOT layer to the APP layer after startup.

2.2 Module Certification Region

The module certification region refers to the UHF parameters of the module that comply with the regulations of a specific region.

For example, if the certification region is China, the module will comply with the UHF standards of mainland China.

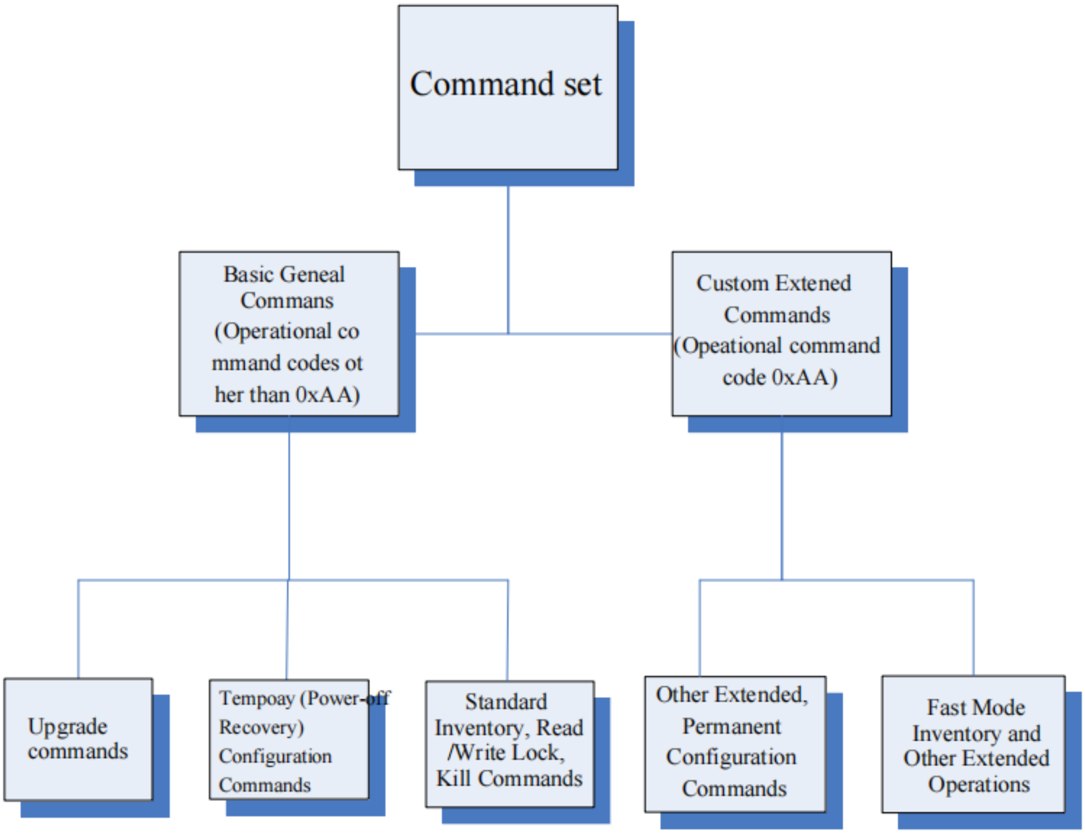
Different certification regions may result in differences in the module's firmware functionality.

	China Certification Region	Other Certification Region
Complies with Regional Standards	China (Default)	Specified certification region frequency band
Default Operating Frequency	NA	Specified certification region frequency band
Configurable Operating Frequency	China，NA， CE_LOW，Open frequency	Specified certification region frequency band
Can be tuned to a fixed frequency or select frequency band?	Yes	CE can be fixed frequency, others not supported
Can use carrier modulation for frequency tuning?	Yes	Yes
Can use EX series dedicated fast mode inventory command (0xAA58)?	Yes	CE，INDIA，RUSSIA，PHILIPPINES，JAPAN(all) ，ISRAEL supports， other regions do not support.
Supports Yilian LED Tag Function?	Yes	No
Supports CC33 Custom Function?	Yes	Only support CMD=0x01，Does not support CMD=0x02 and 0x03。

2.2 Command Set Structure Classification

The command set has a large number of commands. Based on the functionality and format design of the commands, the basic structure of the command set is as shown

Command Set Structure


Command set
Basic Geneal Commans (Operational co mmand codes ot her than 0xAA)
Custom Extened Commands (Opeational command code 0xAA)
Upgrade commands
Tempoay (Power-off Recovery) Configuration Commands
Standard Inventory, Read /Write Lock, Kill Commands
Other Extended, Permanent Configuration Commands
Fast Mode Inventory and Other Extended Operations

The document will subsequently introduce seven categories of functional commands: Bootloader command, Tag inventory command, Tag access command, Setting command , Retrieval Commands, Permanent Save Configuration, and Other Functional Commands.

Command set overview

Command set	Description
Bootloader command	Any command that can be executed during the module's Bootloader phase is referred to as a Bootloade command.
Tag inventory command	Commands related to inventory operations, where inventory refers to the action of specifying one or more antennas to poll and read the EPC ID of one or more tags.
Tag access command	Commands related to tag access operations, which refer to memory operations on a single tag using a single antenna
Setting command	Set Related Commands
Retrieval Commands	Retrieve Related Commands
Permanent Save Configuration	These are extended commands used to permanently save configuration parameters.
Other Functional Commands	Special Function Commands

2.3 Basic Command Execution Process

The necessary steps for the module from powering on to performing basic read/write operations are as follows:

1 Start and Enter APP Firmware Layer (If the "Run to APP layer on power-up" function is configured, this step can be skipped.)

2 Enable Antenna Ports (Required for multi-port modules; single-port modules can skip this step.)

Optionally configure settings such as "Antenna Power, Frequency Band, Session, Target, Q, RF_mode, Unique Additional Data," etc.

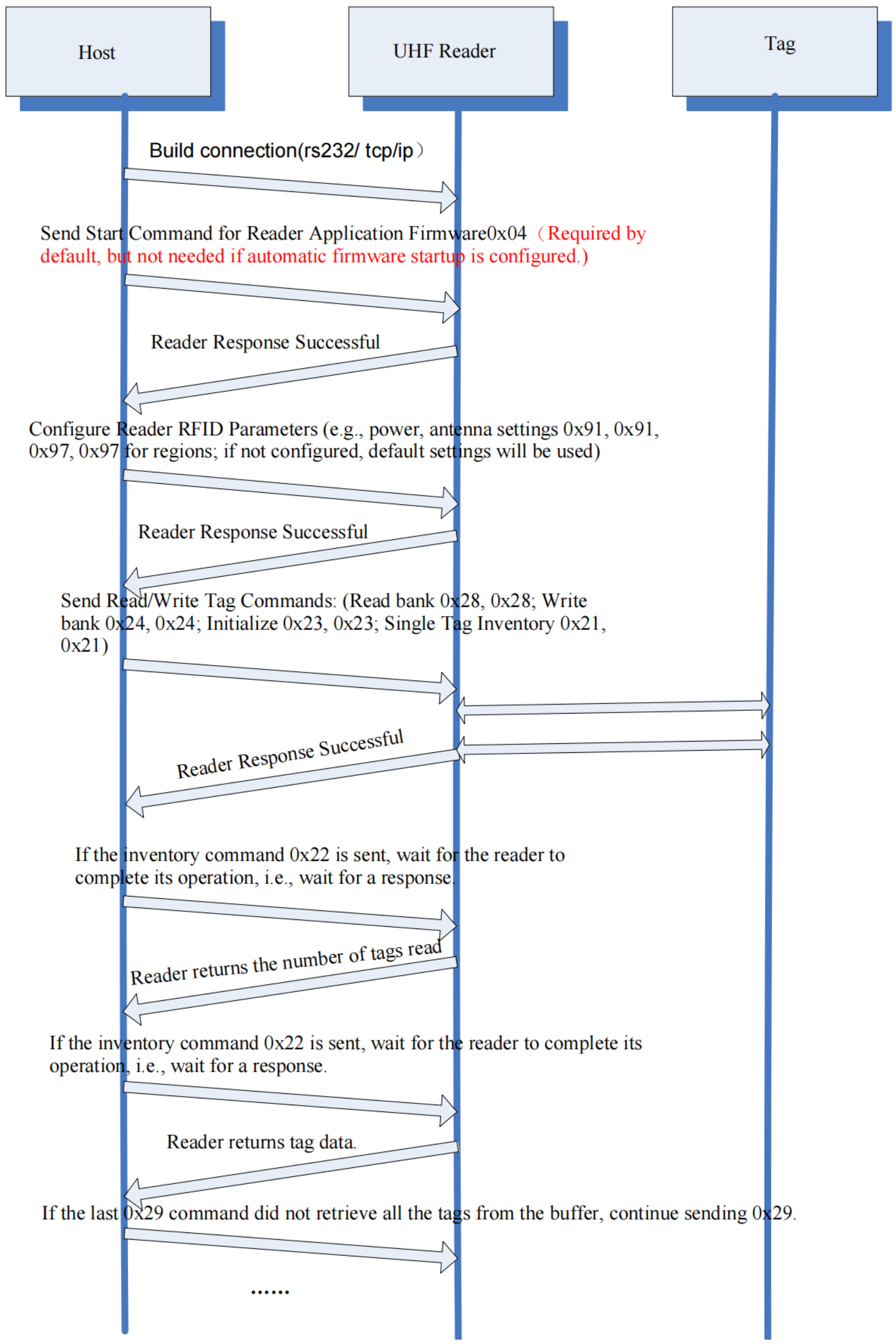
3 Execute Inventory, Read Tag, Write Tag, Lock Tag as Needed.

Note:

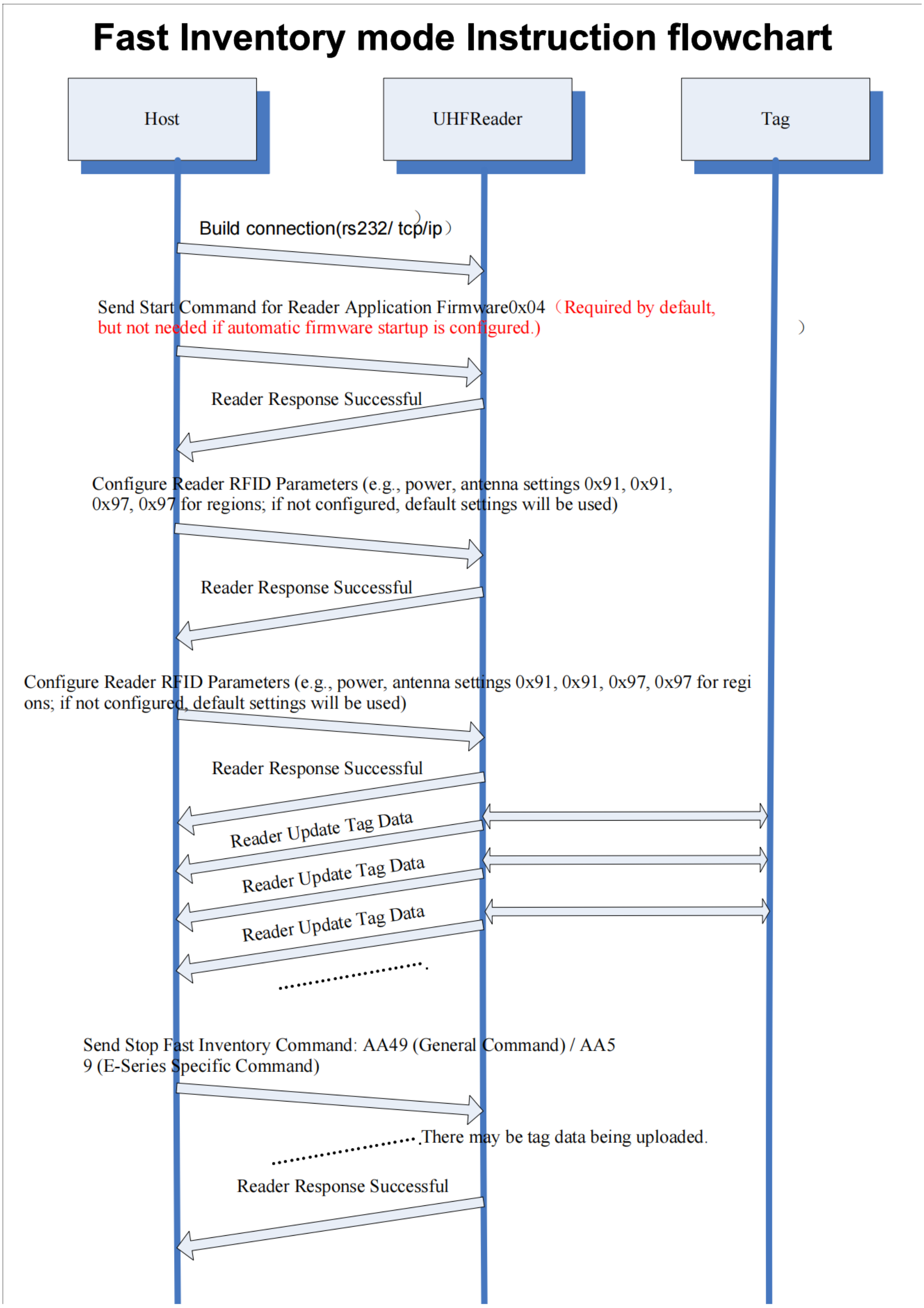
If there is a logical order of operations, the steps must be followed in sequence. For example, when setting the frequency point, the first step is to ensure that the target frequency is within the frequency table of the current operating region. Operations such as modifying locked areas, temporarily locking, or killing tags must be performed when the password is non-zero.

As shown in Figure 3, this is the process flow for standard mode inventory, read, write, lock, kill, and other operations.

Normal Inventory mode Instruction flowchart

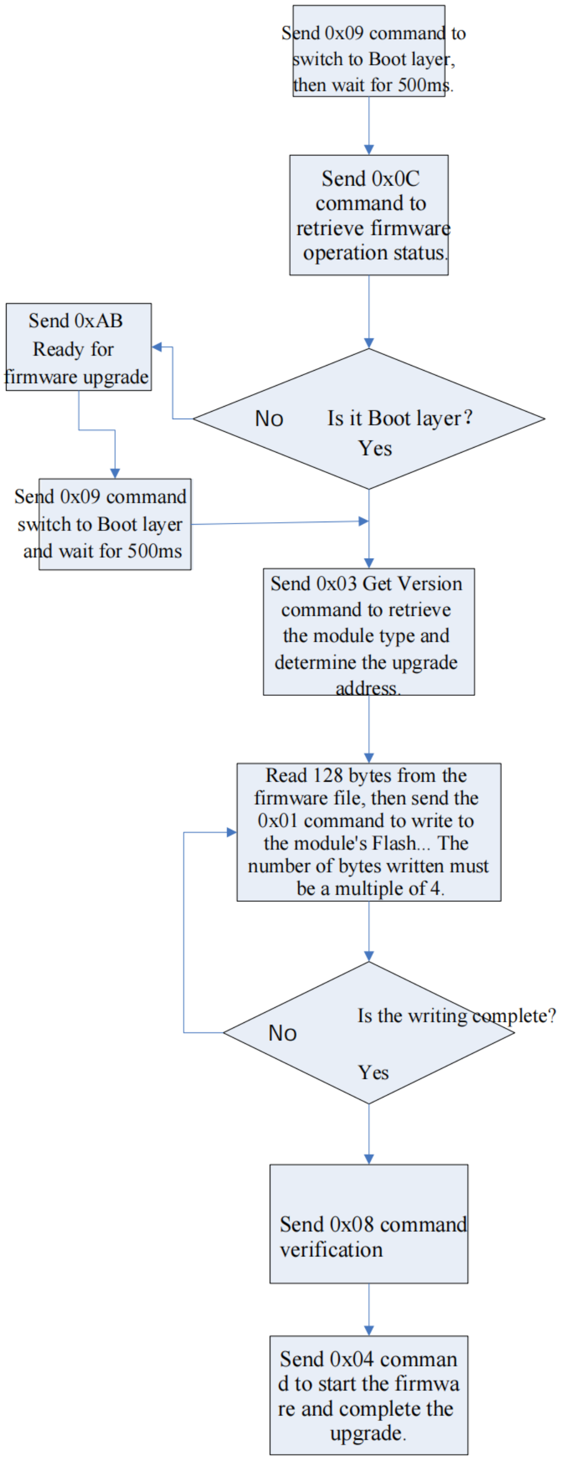

Host
UHF Reader
Tag
Build connection(rs232/ tcp/ip）
Send Start Command for Reader Application Firmware0x04 （Required by default, but not needed if automatic firmware startup is configured.）
Reader Response Successful
Configure Reader RFID Parameters (e.g., power, antenna settings 0x91, 0x91, 0x97, 0x97 for regions; if not configured, default settings will be used)
Reader Response Successful
Send Read/Write Tag Commands: (Read bank 0x28, 0x28; Write bank 0x24, 0x24; Initialize 0x23, 0x23; Single Tag Inventory 0x21, 0x21)
Reader Response Successful
If the inventory command 0x22 is sent, wait for the reader to complete its operation, i.e., wait for a response.
Reader returns the number of tags read
If the inventory command 0x22 is sent, wait for the reader to complete its operation, i.e., wait for a response.
Reader returns tag data.
If the last 0x29 command did not retrieve all the tags from the buffer, continue sending 0x29.
……

The following diagram shows the command flow for fast mode inventory.


Fast Inventory mode Instruction flowchart
Host
UHFReader
Tag
Build connection(rs232/ tcp/ip）
Send Start Command for Reader Application Firmware0x04（Required by default, but not needed if automatic firmware startup is configured.)
Reader Response Successful
Configure Reader RFID Parameters (e.g., power, antenna settings 0x91, 0x91, 0x97, 0x97 for regions; if not configured, default settings will be used)
Reader Response Successful
Configure Reader RFID Parameters (e.g., power, antenna settings 0x91, 0x91, 0x97, 0x97 for regi ons; if not configured, default settings will be used)
Reader Response Successful
Reader Update Tag Data
Reader Update Tag Data
Reader Update Tag Data
Send Stop Fast Inventory Command: AA49 (General Command) / AA5 9 (E-Series Specific Command)
There may be tag data being uploaded.
Reader Response Successful

As following is figure of command flow for firmware upgrade.

Firmware Upgrade Command Flow Diagram


Send 0x09 command to switch to Boot layer, then wait for 500ms.
Send 0x0C command to retrieve firmware operation status.
Is it Boot layer?
No
Yes
Send 0xAB Ready for firmware upgrade
Send 0x09 command switch to Boot layer and wait for 500ms
Send 0x03 Get Version command to retrieve the module type and determine the upgrade address.
Read 128 bytes from the firmware file, then send the 0x01 command to write to the module's Flash... The number of bytes written must be a multiple of 4.
Is the writing complete?
No
Yes
Send 0x08 command verification
Send 0x04 comman d to start the firmwa re and complete the upgrade.

3 Command Protocol and Data Format

The module operates in passive mode, with all tasks initiated by commands sent from the host. After execution, the operation result is returned. The command communication follows these regulations:

(1) The host and the module follow one-send-one receive principle, each time the host sends a message to the module, it should not send the next command until the reply is received.

(2)The length of a frame of communication data (either sent or received command) must not exceed 255 Bytes.

(3)Multi-Byte integers in the command use MSB (Most Significant Byte) first, i.e., big-endian mode: the high-order Byte is stored at the lower address (high Byte first), and the low-order Byte is stored at the higher address. The highest bit in a Byte is the first bit, and the lowest bit is BIT0.

(4)After the host computer sends any command, the timeout for waiting for a response from the module is set to 5 seconds plus the execution time of the specified command. In other words, for commands that include an execution time, such as the 0x22 inventory command, the timeout for waiting for a response from the module will be 5 seconds plus the inventory time specified in the command. The 5-second period is provided to allow for self-recovery in case of sudden abnormalities in the module. For the North American module's standing wave detection command, a timeout of 30 seconds is recommended.

Impinj RFID Series Protocol Document

3.1 Common Communication Protocol format

Host-to-Reader Communication Frame (request/send)

The communication between the host and the module is packaged according to the table below. The module can only accept one command at a time, and the commands are executed serially. Therefore, the host should wait for a response from the module before sending another command.

Header	Data Length	Command Code	Data	CRC-16
1 Byte, command header, must be 0xFF	1 Byte, length of the Data field	1 Byte, command code	Data field, high byte first	2 Bytes, cyclic redundancy check, high Byte first

Reader-to-Host Communication Frame(Response/Reception)

下表定义了从模块到主机的响应数据包的格式。

Header	Data Length	Command Code	Status Code	Data	CRC-16
1 Byte, command header, must be 0xFF	1 Byte, length of the Data field	1 Byte, command code	2 Bytes, status code (0x0000 = success, other = failure)	Data field, high Byte first	2 Bytes, cyclic redundancy check, high byte first

Field	Description
Header	1 Byte, the command header, must be 0xFF.
Data Length	1 Byte, the length of the Data field.

Field	Description
Command Code	1 Byte, the command code. Different command codes correspond to different functions for generic commands, and for extended commands, this value is fixed at 0xAA, with 2 Bytes of sub-command codes included in the Data field.
Status Code	2 Bytes, the status code. 0x0000 indicates success, and other values indicate failure.
Data	N Bytes, the data field, with the high Byte first. The length of this field is determined by the Data Length field. If the Data Length is 0, no Data field is present, and the Data field is determined by the Command Code.
CRC-16	2 Bytes, the cyclic redundancy check, with the high Byte first (refer to Appendix 4).

Command/Instruction Structure:

A single instruction consists of multiple fields.

A field may consist of multiple domains (only the Data field may consist of multiple domains).

A domain may consist of multiple sub-domains.

3.2 Extended Command Communication Protocol Format

When Command Code is 0xAA, it is considered an extended command.
The specific operation command is determined by the Subcommand Code. The Data field of the command sent contains the following domains:

Data Field of Extended Command

When the sent command is an extended command (0xAA), the Data field contains the following domains:

Field	Length	Description
Subcommand Marker	10	Always "Moduletech" (4D 6F 64 75 6C 65 74 65 63 68)
Subcommand Code	2	The extended subcommand code, which has the actual operational meaning. Different subcommand codes have different functionalities.
Subcommand Data	N	Data associated with the specific subcommand. Different subcommands have different data.
SubCRC	1	The checksum, calculated by adding all the bytes from the Subcommand Code to the end of the Subcommand Data, then taking the least significant byte. (See Appendix 6)
Terminator	1	0xBBAlways 0xBB

Data Field of Extended Command Response:

When the received command is an extended command, the Data field of the response contains the following domains:

Field	Length	Description
Subcommand Marker	10	Same as in the sent command Subcommand Marker.

Field	Length	Description
Subcommand Code	2	Same as in the sent command Subcommand Code
Subcommand Data	N	Same as in the sent command Subcommand Data

3.3 Command Construction and Parsing

Command Construction Process:

<1>Determine the operation code (Command Code) based on the functionality, and the corresponding Data (format refer to the specific chapters).

<2>Calculate the length of the Data field (Data Length).

<3>Calculate the CRC for the entire command frame.

<4>Merge the Header, Data Length, Command Code, Data, and CRC to obtain the buffer.

For example, sending FF 03 29 00 15 00 E1 22

<1>Command Code=29, Data contains Metadata Flags and Read Option=0015 00

<2>Data Length=03

<3>The CRC for the entire command frame=E1 22

<4>The merged command becomes FF 03 29 00 15 00 E1 22

FF	03	29	00 15 00	E1 22
Header	Data Length	Command Code	Data	CRC

Command Reception Process:

First, receive 5 Bytes (if not received, it is considered packet loss). These 5 Bytes must meet the following conditions:

<1>Header must be 0xFF。

<2>Data Length, specifies Data length. The total length of the response command is Data Length+7。

<3>Command Code must match the sent operation code. For example, if 0x22 is sent, 0x22 must be returned.

<4>Status Code must be 0x0000, otherwise, check the status code list to determine the error.

After receiving the first 5 Bytes, you can continue reading Data Length + 2 Bytes.

<5>Parse the Data field according to the specific chapter. The length will match the content in the documentation.

<6>After successfully receiving Data Length + 7 Bytes, calculate the CRC for the first Data Length + 5 Bytes to check if it matches the CRC field. If it does not match, consider the command reception as abnormal.

If Data Length + 7 bytes are not received, it is considered packet loss. At this point, the reception of the data frame and verification is complete.

Example: For synchronous inventory, receiving FF 04 22 00 00 04 00 00 02 B7 6E:

First, receive 5 Bytes. The total length is Data Length + 7 = 0x04 + 7 = 11 Bytes. After receiving a total of 11 Bytes, verify the CRC.

FF	04	22	00 00	After receiving 5 Bytes, calculate the total length as follows:	04 00 00 02	B7 6E	After receiving a total of 0x04 + 7 = 11 Bytes. verify the CRC.
Header	Data Length	Command Code	Status Code		Data	CRC	

4 Bootloader Command

The Bootloader automatically starts when the module is powered on, allowing access to the onboard flash memory and other commands. The commands listed in the table below can be executed during the Bootloader stage.

Bootloader Command Overview

Command	Command Code	Description
Write Flash	0x01	Writes to the onboard flash memory, used for updating the module's firmware.
Read Flash	0x02	Reads the content of the onboard flash memory.
Get Version	0x03	Retrieves the version information of the module.
Start Firmware	0x04	Boots the module into the application firmware layer.
Set Baud Rate	0x06	Changes the baud rate of the module's serial port.
Verify Firmware	0x08	Checks if the firmware was correctly written after an upgrade; not for other purposes.
Start Bootloader	0x09	Reverts the module back to the Bootloader layer.

Command	Command Code	Description
Get Running Stage	0x0C	Retrieves the current running stage of the module.
Get Serial Number	0x10	Retrieves the serial number of the module.

4.1 Write Flash(0x01)

Command Overview

Write Data to Onboard Flash for Firmware Update

Command Attributes

Command Code	Bootloader Command	App Firmware Command	Data Field
0x01	Yes	No	Data Field in Send Command, no Data Field in Receive Command

Send Command Data Field Format

When sending the Write Flash (0x01) command, the Data field contains the following fields:

Field	Byte Length	Description
FINFLAG	1	0 indicates that there is still data to be written to the flash. 0xFF indicates this is the last write to the flash, meaning the last block of the firmware data.
WRITEADDR	4	The initial programming address is 0x08008000， After each successful write, the next write address will be WRITEADDR+WRITELEN*4。
WRITELEN	1	Defines the length of WRITEDATA. The Byte length of WRITEDATA is WRITELEN * 4. The value of WRITELEN is fixed at 32, and it equals the actual number of Bytes written only when the last write to flash is smaller than 128 Bytes.
WRITEDATA	N	Data to be written to flash, and the length of this data must be a multiple of 4 bytes.

Note:

●This command rewrites the content of the FLASH block and is used specifically for upgrading the APP firmware segment.

Command Examples:

Example 1： First write

Send command：

FF	86	01	00	08 00 80 00
Header	Data Length	Command Code	FINFLAG	WRITEADDR

20	98 8D 01 20 A1 E3 00 00 E5 A3 01 00 31 35 01 00 53 58 01 00 B1 FC 00 00 55 D2 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 A9 B2 01 00 31 06 01 00 00 00 00 00 09 A6 01 00 D1 C8 01 00 39 35 01 00 49 35 01 00 59 35 01 00 69 35 01 00 79 35 01 00 89 35 01 00 99 35 01 00 A9 35 01 00 B9 35 01 00 C9 35 01 00 D9 35 01 00 E9 35 01 00 F9 35 01 00 09 36 01 00 19 36 01 00 29 36 01 00	33 2A
WRITELEN	WRITEDATA	CRC

Receive command:

FF	00	01	00 00	94 E1
Header	Data Length	Command Code	Status Code	CRC

Example 2: Last write

Send command:

FF	86	01	FF	08 03 04 00
Header	Data Length	Command Code	FINFLAG	WRITEADDR
02	12 01 52 05 23 C4 09 00			96 91
WRITELEN	WRITEDATA			CRC

Receive command:

FF	00	01	00 00	94 E1
Header	Data Length	Command Code	Status Code	CRC

4.2 Read Flash(0x02)

Command Overview

Read the Onboard Flash Content

Command Attributes

Impinj RFID Series Protocol Document

Command Code	Bootloader Command	App Firmware Command	Data Field
0x02	Yes	No	Data Field in Send Command,　Data Field in Receive Command

Send Command Data Field Format

When sending the Read Flash (0x02) command, the Data field contains the following fields, as shown in the table:

Field	Byte Length	Description
READADDR	4	The address to be read from, with the lowest address being 0x08008000
READLEN	1	0~32，the Bytes reading is READLEN * 4

Receive Command Data Field Format

When receiving the Read Flash (0x02) command, the Data field contains the following fields, as shown in the table:

Field	Byte Length	Description
READDATA	N	The data read from the flash memory, with the length being READLEN * 4 Bytes.

Note：

●This command is used as an auxiliary command for burning the APP Firmware and should not be used for any other purposes.

4.3 Get version(0x03)

Command Overview

The command is use to get information of the version No. of the module.

Command Attributes

Command Code	Bootloader Command	App Firmware Command	Data Field
0x03	Yes	Yes	No Data Field in Send Command, Data Field in Receive Command

Receiving Command Data Format

When receiving the Get Version (0x03) command, the Data field includes the following fields as shown in the table below:

Field	Byte Length	Description
Bootloader Version	4	Bootloader version In BOOT layer: value retrieved from the BOOT firmware In APP layer: value read from a storage area
Hardware Version	4	Hardware version
Firmware Date	4	Firmware compilation date
Firmware Version	4	Firmware version
Supported Protocol	4	Supported tag protocol, always 0x00000010 (Gen2 protocol)

Hardware Version Field Explanation

Byte	Hardware Version
Byte 3	Chip type，E710=0x31、E510=0x32、E310=0x33、E910=0x34
Byte 2	Lower 4 bits represent the number of antenna ports:, ANTPORT_1=0，ANTPORT_2=1，ANTPORT_4=2，

Byte	Hardware Version
	ANTPORT_8=3，ANTPORT_16=4，ANTPORT_32=5；Upper 4 bits represent different module types for each antenna port.
Byte 1	Represents the certification region used by the module: CHINA=0x00；FCC=0x01；JAPAN=0x02；JAPAN2=0x18；JAPAN3=0x19；CE_LOW=0x03；KOREA=0x04；CE_HIGH=0x05；HK=0x06；TAIWAN=0x07；MALAYSIA=0x08；SOUTH_AFRICA=0x09；BRAZIL=0x0a；THAILAND=0x0b；SINGAPORE=0x0c；AUSTRALIA=0x0d；INDIA=0x0e；URUGUAY=0x0f；VIETNAM=0x10；ISRAEL=0x11；PHILIPPINES=0x12；INDONESIA=0x13；NEW_ZEALAND=0x14；PERU=0x15；RUSSIA=0x16；CE_LOW_AND_HIGH=0x17（暂不支持）；
Byte 0	Represents the version update serial number.

Command Example:

Send command：

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

Receive Command (Module is single-port SIM5100, initialized for China, using firmware dated 2023.9.3):

FF	14	03	00 00	22 02 11 00
Header	Data Length	Command Code	Status Code	BootLoader Version
32 00 00 00	20 23 09 03	23 09 03 00	00 00 00 10	63 5C
Hardware Version	Firmware Date	Firmware Version	Supported Protocol	CRC

4.4 Start APP Firmware(0x04)

Command Overview

Transition to APP Firmware Layer:

When the module is in the Bootloader layer and receives this command, it will transition to the APP Firmware layer.
If the module is already in the APP Firmware layer, it will return a success response without performing any further actions.

Command Attributes

Command Code	Bootloader Command	App Firmware Command	Data Field
0x04	Yes	Yes	No Data Field in Send Command, Data Field in Receive Command

Receiving Command Data Field Format:

When receiving the Start Firmware (0x04) command, the Data field format follows the same structure as the Get Version (0x03) receiving command.

Note: The BootLoader Version is read from a specific storage area.

Command Examples:

Send command:

FF	00	04	1D 0B

Header	Data Length	Command Code	CRC

Receive command:

FF	14	04	00 00	22 02 11 00
Header	Data Length	Command Code	Status Code	BootLoader Version
32 00 00 00	20 23 09 03	23 09 03 00	00 00 00 10	6A DC
Hardware Version	Firmware Date	Firmware Version	Supported Protocol	CRC

4.4Set Baud Rate(0x06)

Invalid. To modify the baud rate, use the "Modify Power-On Default Baud Rate" in the "Permanent Configuration Save Command AA40".

4.5 Verify APP Firmware(0x08)

Command Overview

This command is used to verify whether the APP Firmware has been correctly written after flashing. It should not be used for any other purpose.

Command Attributes

Command Code	Bootloader Command	App Firmware Command	Data Field
0x08	Yes	No	Data Field in Send Command, no Data Field in Receive Command

Send Data Field Format:

The sending data field for the Verify Firmware (0x08) command contains the following fields:

Field	Byte length	Description
CHECKADDR	4	Starting address for verification, must be 0x08008000.
CHECKDATALEN	4	The value is the total number of Bytes written in Flash by the 0x01 command divided by 4.
CHECKCRC	4	Write the 0x01 instruction to all Bytes of the Flash (that is, all WRITEDATA). Divide it into numbers grouped in sets of 4 bytes each, with a total of N groups. For each group, accumulate the first byte of the group into DATA1. Same as DATA2，DATA3. Accumulate the last byte of each group into DATA4. DATA1 - DATA4 are single - byte unsigned types, and natural overflow occurs during accumulation. This field contains DATA1 - DATA4.

Command Example:

Send command:

FF	0C	08	08 00 80 00	00 00 A1 02	05 08 0C 08	2A 05
Header	Data Length	Command Code	CHECKADDR	CHECKDATA LEN	CHECKCRC	CRC

Receive command:

FF	00	08	00 00	05C8
Header	Data Length	Command Code	Status Code	CRC

4.6 Start Bootloader(0x09)

Command Overview

If the module is in the APP Firmware layer and receives this command, it will transition back to the Bootloader layer.

If the module is already in the Bootloader layer, it will return a success response without any further action.

After sending this command and receiving a successful response, you should wait 250ms before sending another command.

Command Attributes

Command Code	Bootloader Command	App Firmware Command	Data Field
0x09	Yes	Yes	No Data Field in Send Command, no Data Field in Receive Command

Command Example:

Send command:

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

Receive command:

FF	00	09	00 00	15 E9
Header	Data Length	Command Code	Status code	CRC

Notes:

●After sending the 0x09 command, wait for the firmware to process.

●If "Boot to APP on Power-up" is configured, you should send a "Prepare for Upgrade AB" command first before sending 0x09 to ensure the Bootloader is activated.

4.7 Get Current Running Layer(0x0C)

Command Overview

Get the current running layer of the module（whether is Bootloader layer or App Firmware layer）。

Command Attributes

Command Code	Bootloader Command	App Firmware Command	Data Field
0x0C	Yes	Yes	No Data Field in Send Command, Data Field in Receive Command

Receive Data Field Format

When receiving the "Get Version (0x0C)" instruction, it comes with a Data field. At this time, the Data field contains the following domains, as shown in the table:

Field	Byte Length	Description
Program	1	0x11 indicate Bootloader layer. 0x12 indicate APP Firmware layer.

Command Example:

Send command：

Impinj RFID Series Protocol Document

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

Receive command:

FF	01	0C	00 00	12	63 43
Header	Data Length	Command Code	Status Code	Program	CRC

4.8 Get Serial Number(0x10)

Command Overview

Get serial number of the module.

Note: If the module’ s serial number (S/N) sticker contains 12 digits, only the last 10 digits are used.

For example, S/N: 202212120101 should be interpreted as "202212120101".

Command Attributes

Command Code	**Bootloader Command**	**App Firmware Command**	**Data Field**
0x10	Yes	Yes	Data Field in Send Command, Data Field in Receive Command

Send Data Field Format:

When the "Get Serial Number (0x10)" command is sent, the Data field contains the following fields as shown below:

Field	**Byte Length**	**Description**
Option	1	Reserved parameter, this value is zero and meaningless
Data Flags	1	Reserved parameter, this value is zero and meaningless

Receive Command Data Field Format

When the "Get Serial Number (0x10)" command is received, the Data field contains the following fields as shown in below:

For old modules (before July 2024) with S/N on the label as 2212120101, the format is as follows:

Field	Byte Length	Description
Year Month Day	8	Manufacturing date of the product. For example, 02 00 02 02 01 02 01 02 means the module was produced on December 12, 2022
Serial Number	4	Product serial number. For example, 00 01 00 01 means the serial number is 0101

For new modules (after August 2024) with S/N on the label as 102437064B, the format is as follows:

Field	Byte Length	Description
Factory code	4	First 3 Bytes are meaningless, the last Byte indicates the manufacturing factory 10 is Factory 1, 30 is Factory 2, 40 is Factory 3
Production time	4	First 2 Bytes are meaningless, the last 2 Bytes represent the production year and week For example, 00002437 means the production time is week 37 of 2024
Serial number	4	First 2 Bytes are meaningless, the last 2 Bytes represent the product serial number For example, 0000064B means the serial number is 064B

Send command:

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

Receive command(old modules):

FF	0C	10	00 00	02 00 02 02 01 02 01 02	00 01 00 01	52 68
Header	Data Length	Command Code	Status Code	Year Month Day	Serial Number	CRC

Receive command(new module)：

FF	0C	10	00 00	00 00 00 10	00 00 24 37	00 00 06 4B	E6 CA
Header	Data Length	Command Code	Status Code	Factory code	Production time	Serial number	CRC

5 Tag Inventory Command

The commonly used command at the APP layer is the tag inventory command, which is used for inventorying labels. The fundamental operation of label inventory is to collect the Electronic Product Code Identifier (EPCID) of the tags. To cater to various application scenarios, the module supports different inventorying methods. The EX10 series module has implemented four label inventory modes: single tag inventory, synchronous inventory (regular inventory), asynchronous inventory (fast inventory), and EX10 series asynchronous inventory (fast inventory).

Command	Command Code	Describe
single tag inventory	0x21	Inventory a single tag, read the first tag will stop working and return data. Applicable to single antenna single tag real-time scenario.
synchronous inventory	0x22	The execution time of the inventory must be specified. After the command is sent to the module, the module executes the inventory in this time period and stores the tag data in the memory. When the execution time ends, the number of tags counted is returned. After that, can get the tag information in the module memory through the Get Tag Buffer 0x29 command. Suitable for scenarios where there are few tags and the reading time is limited.
Get tag buffer	0x29	Get the tag information stored in the synchronization disk.

Command	Command Code	Describe
asynchronous inventory	0xAA48 0xAA49	The asynchronous inventory includes a set of commands: start inventory AA48, stop inventory AA49, and actively upload AA. The host can start the inventory through AA48, and the module will immediately reply to the host whether it is successfully started. Then the module will maintain the continuous inventory state, and once the inventory is reading a tag, it will be uploaded to the host immediately. If you want to stop the inventory, send AA49. Suitable for scenarios with high real-time requirements.
EX asynchronous inventory	0xAA58 0xAA59	EX asynchronous inventory includes a set of commands: start inventory AA58, stop inventory AA59, actively upload AA. The host can start the inventory through AA58, and the module will immediately reply to the host whether it is successfully started. Then the module will maintain the continuous inventory state, and once the inventory is reading a tag, it will be uploaded to the host immediately. If you want to stop the inventory, send AA59. Suitable for scenarios with a large number of tags. Currently only EX10 series modules support.

In addition, some parameters and fields that are often used in tag inventory commands and tag access commands need to be join in.

5.1 Commonly Used Domain Descriptions

Some parameters and fields that are frequently used in the Data field of tag inventory commands and tag access commands.

5.1.1 Option

Option field is a control flag field, which is used to enable/disable filtering and other functions, and also affects the subsequent related domain composition.

Field	Byte length	Subdomain	Control bit	Description
Option	1	Non-Sel-Option Bits	BIT4/BIT6/BIT7	Used to control other functions. Depending on the opcode, there are different meanings.
		Select-Option Bits	BIT0/BIT1/BIT2/BIT3/BIT5	Generic function, used for selecting filter tags, the value will affect the "Access Password Select Address Select Data Length Select Data" field in the Data field

Select-Option Bits control bit BIT0/BIT1/BIT2/BIT3/BIT5 corresponding functional description.

Control bit	Sample value	Description
BIT0 BIT1	0x00	Disable selection filtering function.
	0x01	Filter and select the EPCID value.

Control bit	Sample value	Description
BIT2	0x02	Filter and select the contents of the TID bank.
	0x03	Filter and select the contents of the USER bank.
	0x04	Filter and select the contents of the EPC bank.
	0x05	If you want to operate a locked storage area without filtering the selection, use this option(so that you can enter a password).
	0x07	Multi-label match filtering. Only supported by 22 commands and AA48 commands (unless explicitly supported).
BIT3	0x08	Sets the inverted flag, which will cause tags that do not match the filter selection rules to be returned.
BIT5	0x20	Select Data Length. The length is 2 Bytes, the comparison data can be >255bit.

Select-Option Bits control bit BIT0/BIT1/BIT2/BIT5 affects the following command fields, as shown in the following table:

Length	Length is 4 Bytes	The length of Tag Singulation is shown below		
sample value	AccessPassword	Select Address	Select Data Length	Select Data
0x00	none	none	none	none
0x01	exist	none	exist	exist
0x02	exist	exist	exist	exist
0x03	exist	exist	exist	exist
0x04	exist	exist	exist	exist
0x05	exist	none	none	none

Length	Length is 4 Bytes	The length of Tag Singulation is shown below		
sample value	AccessPassword	Select Address	Select Data Length	Select Data
0x07	exist	none	none	none
0x20			Length is 2 Bytes	

5.1.2 Tag Singulation

Tag Inventory and Tag Access both support Tag Singulation field, to enable the filter function.
For Tag Inventory, only tags that meet the tag filtering rules can be inventoried.
For Tag Operation (read/write/lock), only the tag that meets the rules will be operated.

The sub-domains in the Tag Singulation domain are as follows ((whether they exist is determined by Option BIT0/BIT1/BIT2):

Field	Byte length	Description
Select Address	0/4	The offset within the Bank (bit unit, starts from zero).
Select Data Length	0/1/2	The length of the data to be compared (bit unit). Usually is 1 Byte. If BIT5 of Option is 1, the length of this field is 2 Bytes.
Select Data	0/N	Data to be compared with the tag data specified in the bank. Note that N = Select Data Length/8, then round up to the integer.

For example

```
The following EPCIDs (first 8 bits) are in the field:
0xAAAA (10101010)
0xCCCC (11001100)
0x4444 (01000100)
0x3000 (00110000)
Select Option=0x04 (EPC Bank)
Select Data Length=0x01 (only match 1 bit)
Select Data=0x80 (10000000, select data length is 1 bit, so others
bits no effect)
Select Data Address=0x00000022 (third bit in the EPCID, EPCID
address is start from 0x20 bits)
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
0x3000
```

Note:

●If you need to use the multi-tag matching and filtering function, you must successfully configure the multi-tag matching and filtering data (0xAA4C) before it, and then can be executed correctly. Otherwise, will return error.

5.1.3 Metadata Flags

If the Metadata Flags value in the command is non-zero, then subsequent commands will exist Metadata items.

The existence of each item of Metadata is determined by the control bits BIT0~BIT7 of Metadata Flags.

For example, Metadata Flags=0x000A indicates that RSSI and frequency are required, the length of Metadata is 4 Bytes.

Metadata Flags control bit	Item	Metadata Byte length	Description
BIT0	Read Count	0/1	The number of times the inventory was taken during the inventory time.
BIT1	RSSI	0/1	Indicates the signal strength of the tag been inventoried, unit is dBm. Signed Byte, stored in complement representation. For example, 0xE6(230) indicate-26dBm. (230-256=-26)
BIT2	Antenna ID	0/1	Indicates the number of the antenna has been inventoried.
BIT3	Frequency	0/3	Indicates the frequency has been inventoried, unit is kHz.
BIT4	Timestamp	0/4	Indicates the time elapsed from the start of this round of inventory command to the time of obtaining this tag, unit is millisecond.
BIT5	PHASE	0/2	If command is 0x21or 0x28. The high Byte is the starting phase value, The low Byte is the ending phase value. The method for converting phase value into degrees is: (phase value/256)*360(degree)

Metadata Flags control bit	Item	Metadata Byte length	Description
			If command is 0x29, 0xAA48. This field is the end phase value, For the start phase value, refer to PHASE2 below. The method for converting phase data into degrees is: Low 12BIT value/4096*360(degree)
BIT6	Protocol ID	0/1	Protocol number Gen2=5.
BIT7	Tag Data Length	0/2	Additional data bit length. If is 21 and 28 command, Tag Data Length=0. In other inventory commands, if inventory embed command is enabled and the Tag Data Length is not zero, it indicates that additional data has been successfully read out, with the value being the bit length of the Tag Data.
	Tag Data	0/N	The Byte length is Tag Data Length/8(maybe is 0). Additional data returned by the inventory.

5.1.4 Metadata and Tag EPC

In the inventory operation, the tag EPCID and other attribute items are often returned. Such as PC and Tag CRC of the EPC bank. Such as the antenna number and RSSI signal strength of the Meta Data, etc.

Meta Data and Tag EPC field

Field	Byte length	Description
Metadata	N	The composition of this field is determined by Metadata Flags, see the previous section.
EPC Length	2	If the opcode is 0x29 command, this field represents the bit length of PC + EPCID + TagCRC. For example, 16 + 64 + 16 = 0x0060.
	1	If the opcode is 0xAA command, this field represents the Byte length of PC + EPCID + TagCRC. For example, 2+8+2=0x0C.
PC Word	2	The PC field in the EPC bank. The high 5 bits of the PC represent the block length of the EPCID (1 block = 2 Bytes). For example, 3000 or 3400 both indicate that the EPCID is 12 Bytes.
EPCID	N	Tag EPC. If the FASTID function is enabled and the TID is successfully returned, this field can be subdivided into EPCID0 + TagCRC0 + TID.
TagCRC/ PHASE2	2	If the command is 29 synchronous inventory or AA48 asynchronous inventory, and when the Metadata Flags BIT5 is 1. This field is the start phase value (2 Bytes), and the end phase value is described above in PHASE. The method for converting phase data into degrees is: Low 12BIT value/4096*360(degree)
		In other cases, this field is the TagCRC. See Appendix 5.

5.1.5 Timeout

Both synchronous inventory and tag operations have this field, which specifies the maximum execution time of the command (unit is milliseconds). If the command completes the operation before the timeout, the module will respond to the host early. Otherwise, it will respond to the host after the timeout expires. The Timeout field is 2 Bytes, with a maximum timeout of 65.535 seconds (0xFFFF).

5.2 Single Tag Inventory(0x21)

Command Description

This command is used to inventory a single tag within a specified time, meaning it will return after inventorying one tag within the specified time. This command follows the general command communication protocol format.

Command Features

Command Code	Bootloader command	App Firmware command	Data field
0x21	none	Exist	Send command exist, receive command exist

Send command Data field format

Single-tag inventory (0x21) with Data field when sending the command. At this time, the Data field contains the following fields, as shown in the table:

Field	Byte length	Description
Timeout	2	Please find Timeout as reference.
Option	1	Option field include Select-Option Bits control bit and BIT4
Metadata Flags	0/2	"This field tells the module the metadata to be returned. This field exists only when Option BIT4=1.

Field	Byte length	Description
Tag Singulation	0/N	The meaning is the same as 0x22 command

Receive command Data field format

Single-tag inventory (0x21) with Data field when receiving the command.

Field	Byte length	Description
Option	1	Same as the Option field of the send command.
Metadata Flags	0/2	Same as the Metadata Flags field in the send command. This field only exists when Option BIT4=1.
Metadata	0/N	The length of the Metadata field is determined by Metadata Flags. This field only exists when Option BIT4=1.
EPCID	N	EPCID
TagCRC	2	TagCRC

Note:

●If set dynamic Q,　Q=0 will be used in the module. If set static Q ,　the module will follow the corresponding configuration.
●If set Target A-B,　Target A will be used in the module. If set Target B-A,　Target B will be used in the module. If set static Target,　the module will follow the corresponding configuration.
●A single operating antenna must be specified first.

Command sample:

Sample 1: return the EPCID of the first tag read within 1 second (1000ms)

Send command:

FF	03	21	03 E8	00	A5E8
Header	Data Length	Command Code	Timeout	Option	CRC

Receive command:

FF	0F	21	00 00	00	C0C011112222 3333AAAA0009	641F	A542
Header	Data Length	Command Code	Status Code	Option	EPC	Tag CRC	CRC

Sample 2: get the EPC number and get the antenna ID number and module system time information at the same time.

timeout=488ms, Metadata Flags=0x0004|0x0010=0x0014

Disable selection matching filtering function, will return the first was inventoried tag:

Send command:

FF	05	21	01 E8	10	0014	2F 6D
Header	Data Length	Command Code	Timeout	Option	Metadata Flags	CRC

Receive command:

FF	16	21	00 00	10	00 14
Header	Data Length	Command Code	Status Code	Option	Metadata Flags
01	00 BB 5F 04	01 23 45 67 89 AB CD EF 01 23 45 67		E6 C8	83 D0
Ant ID	Timestamp	Tag EPC		Tag CRC	CRC

Sample 3: **get EPC and return Antenna ID and Timestamp**

Metadata Flags=0x0014, The filtered EPC is 0x111122223333444455556666

Send command:

FF	12	21	01 E8	11	0014
Header	Data Length	Command Code	Timeout	Option	Metadata Flags
60		11 11 22 22 33 33 44 44 55 55 66 66			9F CE
Select Data Length		Select Data (EPC)			CRC

Receive command:

FF	16	21	00 00	11	0014
Header	Data Length	Command Code	Status Code	Option	Metadata Flags

02	0F C8 C0 B7	11 11 22 22 33 33 44 44 55 55 66 66	18 35	AF D0
Ant ID	Timestamp	Tag EPC	Tag CRC	CRC

5.3 Synchronous Inventory(0x22)

Command Description

The difference between this command and the single tag inventory 21 command is that this command counts all tags in the antenna field within the set time and returns the number of tags until the set time expires.

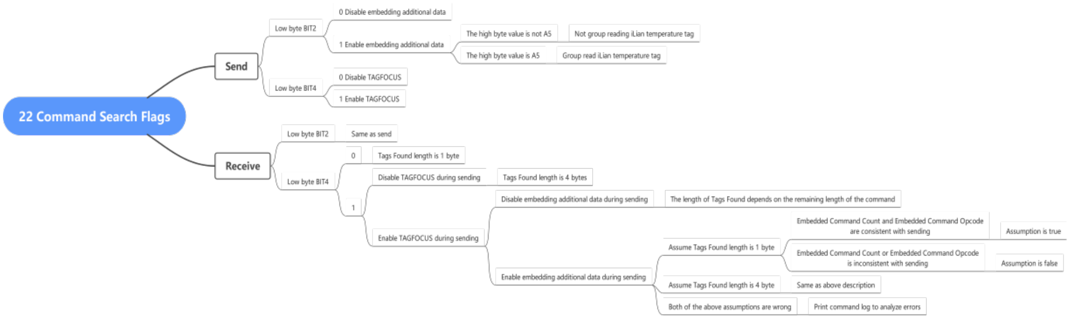
After send command, if inventoried tags, need send get tag buffer 29 command, to get the tag information.

Currently, the tag buffer can store up to 1200 tags. Therefore, after send command, when 1200 tags are accumulated in the tag buffer, the inventory will stop and the result will be returned.

If the 0x22 command was sent previously, without sending the 0x29 command to get the buffered tags, all buffered tags will be automatically cleared before the next execution of the 0x22 command. This command follows the general command communication protocol format.

Command Features

Command Code	Bootloader command	App Firmware command	Data field
0x22	None	exist	Send command exist, receive command exist


22 Command Search Flags
Send
Low byte BIT2
0 Disable embedding additional data
1 Enable embedding additional data
The high byte value is not A5
Not group reading iLian temperature tag
The high byte value is A5
Group read iLian temperature tag
Low byte BIT4
0 Disable TAGFOCUS
1 Enable TAGFOCUS
Receive
Low byte BIT2
Same as send
Low byte BIT4
0
Tags Found length is 1 byte
1
Disable TAGFOCUS during sending
Tags Found length is 4 bytes
Enable TAGFOCUS during sending
Disable embedding additional data during sending
The length of Tags Found depends on the remaining length of the command
Enable embedding additional data during sending
Assume Tags Found length is 1 byte
Embedded Command Count and Embedded Command Opcode are consistent with sending
Assumption is true
Embedded Command Count or Embedded Command Opcode is inconsistent with sending
Assumption is false
Assume Tags Found length is 4 byte
Same as above description
Both of the above assumptions are wrong
Print command log to analyze errors

Send command Data field format

Synchronous inventory(0x22) with Data field when sending command, the Data

field contains the following fields, as shown in the table:

Field	**Byte length**	**Description**
Option	1	Option field contains Select-Option Bits control bit and BIT7. If BIT7=1, indicates enable FASTID function. If multi-tag matching filtering or additional data is enabled, the FASTID function will fail.
Search Flags	2	Low Byte control bit as follow(1 enable, 0 disable)(See the picture above for details): When BIT4=1, Use the TAGFOCUS function of IMPINJj.* When BIT2=1, enable embedding additional data. When BIT2=1, and high Byte value is A5, group reading iLian*Temperature tag.
Timeout	2	Refer to Timeout field description.
Access Password	0/4	Access password. If tag not locked, then the access password is 00000000. If the memory area is locked, the access password must be correct. Whether this field exists, depends on Option BIT0/BIT1/BIT2.
Tag Singulation	0/N	filtering function. Whether this field exists, depends on Option BIT0/BIT1/BIT2.
Embedded Command Content	0/N	Additional data function. Synchronous inventory command can embed another tag access operation command. Only support embed 0x28 command. When BIT=1 of Search Flags, this field exist.

Explain: group reading iLian*Temperature tag, need to read the corresponding access area according to the iLian tag rules. The difference between group reading temperature tags and ordinary embedded reading is that after inventory the tags and before reading the tag memory, the group reading temperature tag function will first allow the carrier wave to continue sending for 40 milliseconds before reading. This function only Chinese version module can use.

Embedded Command Content Field

Field	Byte length	Description
Embedded Command Count	1	Several sets of additional data need to be read, 0x01~0x0A, at most ten sets.
Embedded Command Length	1	The length (Bytes) of the data field of the embedded command, N groups, the value is 3+6*N.
Embedded Command Opcode	1	Embedded command code is 0x28.
Embedded Values	N	The data field of the embedded command is the send Data field of the 0x28 command*. If multiple groups are read, there are multiple consecutive

Field	Byte length	Description
		"the send Data field of 0x28 command".

Receive Command Data Format

Synchronous Inventory (0x22) with Data field when receive command. At this time, the Data field contains the following fields, as shown in the table:

Field	**Byte length**	**Description**
Option	1	Same as the Option field of the send command.
Search Flags	2	Same as the Search Flags field of the send command. If the number of inventory tags is bigger than 255, BIT4 of Search Flags will be set to 1.
Tags Found	1/4	The number of tags has inventoried. If the number of tags is ＞ 255 (BIT4 of Search Flags is 1), this field is 4 Bytes. Otherwise, it is 1 Byte.
Embedded Command Result	0/N	When BIT2=1 of Search Flags, this field is exist。

Embedded Command Result

Filed	Byte length	Description
Embedded Command Count	1	Read out several sets of additional data, the same as the Embedded Command Count field of the sent command.
Embedded Command Opcode	1	The same as Embedded Command Opcode field od the send command, is 0x28.
Operations Succeeded	2	The number of successful operations of the embedded command, just for reference only.
Operations Failed	2	The number of fail operations of the embedded command, just for reference only.
Embedded Command Data Returned	N	Embed the data returned by the successful execution of the command (if the 28 command operation is successful, the tag data of the first tag read will be returned. If it is unsuccessful, there is no such field).

Note:

●TAGFOCUS function, Only valid when set to S1and static TARGET A;

●If the module is a multi-antenna module and is connected to multiple antennas, you need to use 91 to configure the antenna before sending 22 synchronization inventory. If multiple-antennas are configured, the antenna polling rule is: for example, if antennas 1, 3, and 4 are enabled, the inventory will start from 1. If no new tags are read, it will jump to 3, then jump to 4, and then jump back to 1...

●When the 0x28 command is embedded in the inventory, the maximum length of a single group is 32 blocks (64 Bytes), with a maximum of ten groups and a total length of 56 blocks (112 Bytes). * The format of the embedded 0x28 command can be found in the Read Tag Data section.

The operation flow of the inventory embedded with 0x28 command is that after each inventory, 0x28 command is executed on the tag. Regardless of whether the operation of command 0x28 is successful, the EPC of the tag will be saved and returned when exiting.

●In the Embedded Values (send Data field of 0x28), the values of (Emb Cmd) Timeout and (Emb Cmd) Option are zero and have no effect. The execution time of the entire command is the time specified by Timeout.

Command sample:

Sample 1: enable matching filter, matching area is EPC

Send command:

FF	0F	22	04	00 00	03 E8	00 00 00 00	00 00 00 78	08	66	DE C0
Header	Data Length	Command Code	Option	Search Flags	Timeout	Access Password	Select Address	Select data length	Select data	CRC

Receive command:

FF	04	22	00 00	04	00 00	02	B7 6E
Header	Data Length	Command Code	Status Code	Option	Search Flags	Tag Found	CRC

If the number of tags inventoried 255, the length of the Tag Found field will be 4 Bytes, and BIT4 of the Search Flags will be set to 1. If 257 tags are found, the return format will be as follows.

FF	07	22	00 00	04	00 10	00 00 01 01	5A 0E
Header	Data Length	Command Code	Status Code	Option	Search Flags	Tag Found	CRC

Sample 2:

Do not use the filter matching function, enable the FASTID function.

Send command:

FF	05	22	80	00 00	00 C8	332D
Header	Data Length	Command Code	Option	Search Flags	Timeout	CRC

Receive command:

FF	04	22	00 00	80	00 00	00	6030
Header	Data Length	Command Code	Status Code	Option	Search Flags	Tag Found	CRC

Sample 3:

Do not use the filter matching function, embed the 0x28 command to read the data of 32 blocks starting from block address 0 in the USER area.

Send command:

FF	11	22	00	00 04	03 E8	01	09	28
Header	Data Length	Command Code	Option	Search Flags	Time out	Embedded Command Count	Embedded Command Length	Embedded Command Opcode

0000	00	03	00000000	20	2D91
Embedded Command Timeout	Embedded Command Option	Read MemBank	Read Address	Read Word Count	CRC

Sample 4:

Using tag match filtering, the match area is 8 bits starting from address 0x00 of the TID bank, the match value is 0xE2, and the inventory embeds the 0x28 command to read 2 blocks starting from address 0x02 of the RESERVED bank.

Send command:

FF	1B	22	02	00 04	03 E8	22221111	00 00 00 00	08
Header	Data Length	Command Code	Option	Search Flags	Time out	Access Password	Select Data Address	Select Data Length

E2	01	09	28	00 00	00	00	00 00 00 02	02	82 CF
Select Data	Embedded Command Count	Embedded Command Length	Embedded Command Opcode	Embedded Command Timeout	Embedded Command Option	Read MemBank	Read Address	Read Word Count	CRC

Receive command:

FF	0E	22	00 00	02	00 04	1C	01
Header	Data Length	Command Code	Status Code	Option	Search Flags	Tag Found	Embedded Command Count

28	00 01	00 2F	22 22 11 11	C6F2
Embedded Command Opcode	Operations Succeeded	Operations Failed	Data Read	CRC

Sample 5:

Not use filtering, embed 0x28 command to read four sets of additional data, read: reserved bank 0~3 blocks, EPC bank 0~7 blocks, TID bank 0~5 blocks, user bank 0~3 blocks.

Send command:

FF	23	22	00	00 07	0032	04	1B	28

Header	Data Length	Command Code	Option	Search Flags	Time out	Embedded Command Count	Embedded Command Length	Embedded Command Opcode

0000	00	00	00000000	04
Embedded Command Timeout	Embedded Command Option	Read MemBank	Read Address	Read Word Count

01	00000000	08	02	00000000	06
Read MemBank	Read Address	Read Word Count	Read MemBank	Read Address	Read Word Count

03	00000000	04	B3C5
Read MemBank	Read Address	Read Word Count	CRC

Receive command:

FF	36	22	00 00	00	00 07	02	04
Header	Data Length	Command Code	Status Code	Option	Search Flags	Tag Found	Embedded Command Count

28	00 02	00 01	0000000000000000 9A58080022220000 0020111020000080 E280110520004141 AD8D0079 0000000000000000	5548
Embedded Command Opcode	Operations Succeeded	Operations Failed	Data Read	CRC

5.4 Get Tag Buffer(0x29)

Command Description

This command is used to get the tag information inventoried by the synchronous inventory command (0x22). The information that can be get includes the tag's EPC and its related metadata. After getting the tag data from the buffer, the buffered tags will be deleted from the buffer. This command follows the general command communication protocol format.

Command Features

Command Code	Bootloader command	App Firmware command	Data field
0x29	None	Exist	Send command exist, Receive command exist

Send command Data field format

Get tag buffer(0x29) with Data field when send command. At this time, the Data field contains the following fields, as shown in the table:

Field	Byte length	Description
Metadata Flags	2	Please refer to Metadata Flags field description.
Read Option	1	0x00 indicates getting information about tags that have not yet been obtained. 0x01 indicates getting the tag information obtained by the previous 0x29 command.

Field	Byte length	Description
		Hereinafter referred to as Option.

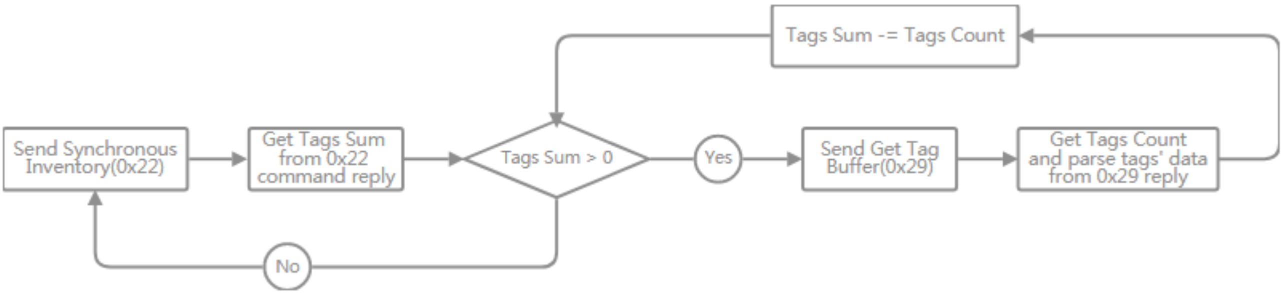
Receive command Data field format

Get tag buffer (0x29) with Data field receive command. At this time, the Data field contains the following fields, as shown in the table:

Field	Byte length	Description
Metadata Flags	2	Please refer to Metadata Flags field description.
Read Option	1	Same as the Read Option of the Send command above. (Hereinafter referred to as Option.)
Tag Count	1	Returns the number of tags contained in the information.
MetaData and TagEPC	N	The information of each tag is packaged into MetaData and TagEPC data blocks. The number of these data blocks is Tag Count.

Note:

●Use Synchronous Inventory, the command sending process is as follows.


Tags Sum -= Tags Count
Send Synchronous Inventory(0x22)
Get Tags Sum from 0x22 command reply
Tags Sum > 0
Yes
Send Get Tag Buffer(0x29)
Get Tags Count and parse tags' data from 0x29 reply
No

5.4.1 IMPINJ FASTID Function

EPC bank composition: 2 Bytes TagCRC0+2 Bytes PC0+N Bytes EPC0.
The EPC0, TagCRC0 and PC0 in the following text represent the original true EPC, TagCRC and PC of the tag.
PC2 and TagCRC2 represent the fields in the transmission protocol.
The high 5 bits of the PC0 field in the EPC bank represent the word length of EPC0, and PC0 and EPC0 can be used to calculate TagCRC0. See Appendix 5 for the algorithm for calculating Tag CRC.

Option BIT7=1 means that the FASTID function is enabled. When (inventory embedding read function) or (multi-tag matching filter) is enabled, the FASTID function will not be used regardless of whether OPTION BIT7 is 1.

The TID length of the tag that supports FASTID function is fixed to 12 bytes (only supports IMPINJ FASTID.

After enabling the FASTID function, the data after EPC Length in the Meta Data and TagEPC field has three formats:
①IMPINJ M4 and M5 tag, the return format is:
PC2+(EPC0+TagCRC0+TID)+TagCRC2.
②IMPINJ M6 and update tag, return format is : PC2+(EPC0+TID)+TagCRC2.
③Not support FASTID function tag, return format is: PC0+EPC0+TagCRC0.

If enable FASTID function, need to determine whether the above data (except the first and last 2 Bytes) contains TID:

1. Calculate EPCWORDLEN=high Byte of PC (following the first 2 Bytes of EPC Length)>>3.
    a) If EPCWORDLEN<7 blocks, tag not support TID, process according to the format of ③.
    b) If EPCWORDLEN≥7 blocks, the returned data may contain TID, see below.
2. Check the first 4 Bytes of the last 12 Bytes (ignore the TagCRC at the end) (i.e. the guessed TID) and compare them with the table below.
    1) For tags of Impinj M6 and later, process them according to the format of ②.
    2) If the tag is not in the table, that is, the tag does not support FASTID, process it according to the format of ③.

3) For tags of Impinj M4 or M5 (supporting FASTID), the following judgment needs to be made first.

3. Judgment method (see instruction example):
    a) EPC0 is: The data of the (EPCWORDLEN-7) block immediately following the PC.
    b) PC0 high Byte = the high Byte of PC -0x38.
    c) PC0 low Byte = the low Byte value of PC.
    d) Calculate the assumed TagCRC value based on the above assumed PC0 and EPC0.
    e) Compare with TagCRC0 (the 2 Bytes following EPC0).
        i. If they are equal, the returned data contains TID and is processed according to the format of ①.
        ii. If they are not equal, the returned data does not contain TID and is processed according to the format of ③.

Command Sample①:

●Synchronous Inventory 29 receive FF 24 29 00 00 00 00 00 01 00 F0 {6C 00 (30 08 33 B2 DD D9 01 40 00 00 00 00 C4 1E **E2 80 11 05** 20 00 80 D4 5B 60 0A FF) B5 F9} B4 59

●Asynchronous Inventory AA48 receive FF 27 AA 00 00 00 16 C7 01 00 00 00 39 1E {6C 00 (30 08 33 B2 DD D9 01 40 00 00 00 00 C4 1E **E2 80 11 05** 20 00 80 D4 5B 60 0A FF) B5 F9} 0A 89

● Analysis: Synchronous Inventory EPC Length=0x00F0={240bit}, Asynchronous Inventory EPC Length=0x1E={30Byte}.

●Follow: PC2=6C00, 0x6C shifted right by three bits is thirteen, thirteen＞seven.

●Determine that E2801105 is of M4QT type and supports FASTID function, and need to do TagCRC check.

●Calculate PC0=3400 (high Byte 0x6C-0x38=0x34, low Byte 00 is continue to use).

●Calculate the length of EPC0 as (13-7=6Word=12Byte), that is, EPC0=30…00, TagCRC0=C41E.

●Calculate TagCRC=C41E through PC0 and EPC0, which is equal to TagCRC0, and process it according to the format of ①.

● If TagCRC is not equal to TagCRC0, process it according to the format of ③.

Command Sample②:

●Asynchronous Inventory AA48 receive:

FF23AA0000000020{7400(44332222000000000000225000000000**E28011C1**20000B33E2E40310)D036}10F8

Because 0x74 shifted three bits right is 14, > 7. The tag chip type is determined to be M781.

Where EPCID=44332222000000000000225000000000.

Where TID=E28011C120000B33E2E40310.

●Asynchronous Inventory AA48 receive:

FF19AA0000000016{4C00{000639394141**E2801170**2000040693A60940)A280}F7C4

Because 0x4C shifted three bits right is 9, > 7. The tag chip type is determined to be MR6-P.

Where EPID=000639394141。

Where TID=E2801170200001 9D460B0A71。

Command Sample③:

●Asynchronous Inventory AA48 receive:

FF07AA0000000004{0000()E2F0}4C01

Because 0x00 is shifted right by three bits is zero, < seven (i.e., the EPCID is empty), the tag does not support TID and is processed according to the format of ③.

●Asynchronous Inventory AA48 receive:

FF43AA0000000040{F400(300833B2DDD9014000000000300833B2DDD9014000000000300833B2DDD9014000000000300833B2DDD9014000000000**300833B2**DDD9014000000000)C5AE}5A63

Because 0xF4 shifted three bits to the right is thirty, > seven. It is determined that the tag chip type is not in the table, the tag does not support TID, and is processed according to the format of ③ (the EPCID of this tag is very long, with sixty Bytes).

The tags that support FASTID function are available on IMPINJ, as shown in the following table (tags not listed do not support FASTID function):

Chip category	Chip model	TID starts with 4 Bytes
Monza4 and Monza5 tags	M4D	E2801100
	M4I	E2801114
	M4QT	E2801105
	M4U	E2801104
	M5	E2801130
	M5U	E2801132
	M4E	E280110C
Monza6 and newer Impinj tags	MR6	E2801160
	MR6-A or MR6-B	E2801171
	MR6-P	E2801170
	M730	E2801191
	M750	E2801190
	M770	E28011A0
	M775	E28011A2
	M780	E28011C0
	M781	E28011C1
	M800	E28011B0

Note, M4E tag, the TID tag starting with E280110C does not support the FASTID function.

Command Sample:

Sample 1: get tag, and return the reading count, antenna ID and timestamp.

Metadata Flags=0x0001|0x0004|0x0010=0x0015

Send command:

FF	03	29	00 15	00	E1 22
Header	Data Length	Command Code	Metadata Flags	Option	CRC

Receive command:

FF	34	29	00 00	00 15	00	02	22	01
Header	Data Length	Command Code	Status Code	Metadata Flags	Option	Tag Count	Read Count	Ant ID

02 50 CE F6	00 80	31 C1	11 11 22 22 33 33 44 44 55 55 66 66	FB 15	0E
Timestamp	EPC Length	PC Word	EPC ID	Tag CRC	Read Count

01	04 1D 3D 3C	00 80	30 00	05 00 00 00 00 00 00 00 00 00 23 54	4A C8	92A3
Ant ID	Timestamp	EPC Length	PC Word	EPC ID	Tag CRC	CRC

Sample 2: get tag, and returns all tag metadata except Protocol ID, Metadata Flags=0x00BF.

Send command:

FF	03	29	00 BF	00	4B 22
Header	Data Length	Command Code	Metadata Flags	Option	CRC

Receive command:

FF	4A	29	00 00	00 BF	00	02	07	E3	01	0E 22 2A
Header	Data Length	Command Code	Status Code	Metadata Flags	Option	Tag Count	Read Count	RSSI	Ant ID	Frequency

00 00 8D 8F	00 00	00 00	00 60	20 00	11 11 22 22 33 33 44 44	C2 41	07	D0
Timestamp	PHASE	Tag Data Length	EPC Length	PC Word	EPC ID	Tag CRC	Read Count	RSSI

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	FD 4C

Ant ID	Frequency	Timestamp	PHASE	Tag Data Length	EPC Length	PC Word	EPC ID	Tag CRC	CRC

Sample 3: command 0x22 embeds command 0x28, reads 2 words starting from address 0 in the TID bank, and get all tag metadata except the Protocol ID. Metadata flag = 0x00BF.

Send command:

FF	03	29	00 BF	00	4B 22
Header	Data Length	Command Code	Metadata Flags	Option	CRC

Receive command:

FF	6E	29	00 00	00 BF	00	03	08	D7	01	0D F7 32
Header	Data Length	Command Code	Status Code	Metadata Flags	Option	Tag Count	Read Count	RSSI	Ant ID	Frequency

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
Timestamp	PHASE	Tag Data Length	Tag Data	EPC Length	PC Word	EPC ID	Tag CRC	Read Count	RSSI	Ant ID

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
Frequency	Timestamp	PHASE	Tag Data Length	Tag Data	EPC Length	PC Word	EPC ID	Tag CRC

07	D4	01	0D F7 32	00 00 71 8D	00 00	00 20	E2 00 60 04	00 20	00 00	E2 F0	96 E7
Read Count	RSSI	Ant ID	Frequency	Timestamp	PHASE	Tag Data Length	Tag Data	EPC Length	PC Word	Tag CRC	CRC

Sample 4: command 0x22 embeds 0x28 command to read four sets of additional data. Read: reserved bank 0~3 blocks, EPC bank 0~7 blocks, TID bank 0~5 blocks, user bank 0~3 blocks.

Send command:

FF	03	29	00 80	00	74 22
Header	Data Length	Command Code	Metadata Flags	Option	CRC

Receive command:

FF	7C	29	00 00	00 80	00	02	0160	00000000 00000000
Header	Data Length	Command Code	Status Code	Metadata Flags	Option	Tag Count	Tag Data Length	reserved bank 4 blocks

0BF83000 E201E2F6 43090E1C FAAF8700	E201E2F6 43090E1C 00008600	0000 0000 8700 0000	00 80	30 00	E201E2F6 43090E1C FAAF8700	0B F8	0160	01234567 01234567
EPC bank 8 blocks	TID bank 6 blocks	User bank 4 blocks	EPC Length	PC Word	EPC ID	Tag CRC	Tag Data Length	reserved bank 4 blocks

93881400 AAAC1122 15920020 308FFFFF	E2801105 200076C2 8B570AD1	1111 2222 3333 4444	00 40	14 00	AAAC 1122	9388	70 75
EPC bank 8 blocks	TID bank 6 blocks	User bank 4 blocks	EPC Length	PC Word	EPC ID	Tag CRC	CRC

5.5 Clear buffer command (0x2A)

Originally used before sending the synchronous inventory command (0x22), it is **no longer necessary**.

now every time a new 22 synchronous inventory is started, the buffer will be automatically cleared.

5.6 Asynchronous Inventory

Asynchronous Inventory includes a group of commands, all of which have the command code 0xAA. Different command functions are encapsulated in the data field. Therefore, different commands of Asynchronous Inventory use different sub-command codes. Asynchronous Inventory is often referred to as fast inventory mode/high-speed inventory mode/non-stop inventory mode.

5.6.1 Asynchronous Inventory(0xAA48)

Command Description

After sending the AA48 command, if the inventory is successfully started, the AA48 success command will be returned immediately. The subsequent module will remain in a continuous asynchronous state, and once the tag is read, it will be actively uploaded to the host.

In this mode, the module's inventory performance is optimal, and it is suitable for scenarios with high performance requirements.

Modules based on R2000 chips and E series chips support this command.

During the inventory process, if you want to end the inventory, send the AA49 command and return the 0000 status code.

During the inventory process, if other CRC correct commands are sent, the inventory will end and the "status code is AA49" command will be returned.

During the inventory process, if the module is abnormal, the AA49 command containing the "error status code" will be returned.

Command Features

SubCommand Code	Bootloader command	App Firmware command	Subcommand Data
0xAA48	None	exist	Send command exist, Receive command none

Send command SubData Field Format

Asynchronous Inventory (0xAA48) with SubData fiels when send command. At this time, the Data field contains the following fields, as shown in the table:

Field	Byte length	Description
Metadata Flags	2	Please refer to Metadata Flags field description.
Option	1	Option field contains Select-Option Bits control bit and BIT7. If BIT7=1, indicate enable FASTID function. If multi-tag matching filtering or additional data is enabled, the FASTID function will be disabled. If BIT4=1, the CC33 customization function is enabled.
Search Flags	2	The low Byte control bits are as follows (1 is enable, 0 is disable) (does not support "group read iLian temperature tag"): When BIT4=1, use the TAGFOCUS function of IMPINJ.* When BIT2=1, enable embedding additional data. The high Byte control bits are as follows (1 is enable, 0 is disable): BIT7=1 indicate that heartbeat packet is sent to the host every 15 seconds. If the asynchronous inventory stops, the module will no longer send heartbeat packet. For the heartbeat packet format, refer to the heartbeat data packet. BIT6=1 indicate that if "single antenna is enabled and (antenna dwell time expires or new tag cannot be read)", the module stops inventory and returns AA49. This function is usually used to expand a single antenna port to multiple antenna ports. BIT5=1 indicate that if "multiple antennas are enabled", the module will send a notification frame "after each polling of the antennas, indicating that all currently enabled antennas have been polled". For the notification frame format, refer to the notification frame data packet.

<table>
<tr><th>Field</th><th>Byte length</th><th>Description</th></tr>
<tr><td></td><td></td><td>BIT3~BIT0 are four bits in total, used to set the stop ratio of the duty cycle:
<table>
<tr><td>0</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td></tr>
<tr><td>No stop</td><td>Stop 5%</td><td>10%</td><td>15%</td><td>20%</td><td>25%</td><td>30%</td><td>35%</td></tr>
<tr><td>8</td><td>9</td><td>A</td><td>B</td><td>C</td><td>D</td><td>E</td><td>F</td></tr>
<tr><td>40%</td><td>45%</td><td>50%</td><td>55%</td><td>60%</td><td>70%</td><td>80%</td><td>90%</td></tr>
</table>
Note: need to use 0x95 to configure the "base time and full load working time" in advance.</td></tr>
<tr><td>CC33 custom data</td><td>0/N</td><td>When BIT4=1 of Option, this field is exist.
If the CC33 customization function is enabled, the format of this field is as shown in the table below.</td></tr>
<tr><td>Access Password</td><td>0/4</td><td>The meaning is the same as 0x22 command.</td></tr>
<tr><td>Tag Singulation</td><td>0/N</td><td>The meaning is the same as 0x22 command.</td></tr>
<tr><td>Embedded Command Content</td><td>0/N</td><td>The meaning is the same as 0x22 command.</td></tr>
</table>

Note:

●The antenna polling rule is: if multiple antennas are enabled, they will be sorted in ascending order by antenna number. Then the inventory will start from the lowest antenna number. If the antenna does not read a new tag within a period of time (this time is the judgment time for the module's internal processing), it will jump to the next antenna, or the antenna's residence time exceeds the specified time (the default is 4 seconds, refer to the 0x95 command for modification), it will be forced to switch to the next antenna. After polling all antennas in turn, it will start again from the antenna with the lowest serial number, and so on.

CC33 custom function:

If enable CC33 custom function (BIT4=1 of Option), the field of send command

"CC33 custom function data" as follow:

Field	Byte length	Description
FIXDATA	2	Fixed is 0xCC33.
CMD	1	(1)CMD=0X01: During the inventory process, each time the amplifier is turned on, the detected antenna connection status + standing wave condition + module temperature are returned. (Available for all modules) (2)CMD=0X02: Configure the working time of each antenna. When the working time is reached, it will jump to the next antenna. (It also has the function of CMD=0x01, which is only available for Chinese modules). (3)CMD=0X03: Configure the Q value used by each antenna. After completing an inventory cycle, it will jump to the next antenna. (Also has the function of CMD=0x01, only available for Chinese modules). Note: If the configured Q value is too large and a counting cycle has not been completed within the working time of a frequency, it will jump directly to the next antenna after the current frequency working time expires.
Data	4/ 4+N*2/ 4+N	The initial value of MODUSTATUS is 00000000, which controls the data to be returned. The lowest Byte BIT0=1 returns the antenna connection status; (BIT0=0 is disable) The lowest Byte BIT1=1 returns the antenna standing wave; (BIT1=0 is disable) (only accurate around 20dBm) The lowest Byte BIT2=1 returns the module temperature; (BIT2=0 is disable) For example, MODUSTATUS=00000007 indicate that all three functions are enabled. If the module does not support this function, the returned data is invalid and can be ignored. (1)CMD=0X01, this field is only MODUSTATUS. (2)CMD=0X02, this field is MODUSTATUS+ANT1TIME+...+ANTNTIME. There are as many groups of 2-Byte ANTTIME as there are antenna ports on the module. The value range is 20~60000ms.

Field	Byte length	Description
		(3) CMD = 0X03, this field is MODUSTATUS + ANT1Q + ... + ANTNQ. The module has as many groups of 1-Byte ANTQ as the number of antenna ports. The value range is 0x00~0x0F. Note: Compared with 95 configuration of antenna dwell time and 9B configuration of Q, the current configuration has a higher priority.

Command sample:

Sample 1:

Start Asynchronous Inventory without use Tag Singulation and Embedded Command Content. Metadata Flags is 0x00BF, which indicate that the module is required to return all metadata except Protocol ID.

Send command:

FF	13	AA	4D 6F 64 75 6C 65 74 65 63 68	AA 48
Header	Data Length	Command Code	Subcommand Marker (Moduletech)	Subcommand Code

00 BF	00	80 03	34	BB	29 0F
Metadata Flags	Option	Search Flags	SubCRC	Terminator	CRC

Receive command:

FF	0C	AA	00 00	4D 6F 64 75 6C 65 74 65 63 68	AA 48	0F 23
Header	Data Length	Command Code	Status Code	Subcommand Marker (Moduletech)	Subcommand Code	CRC

Sample 2: start Asynchronous Inventory, and enable filtering function, Metadata Flags is 0x00BF.

Send command:

FF	1D	AA	4D 6F 64 75 6C 65 74 65 63 68	AA 48	00 BF	04
Header	Data Length	Command Code	Subcommand Marker (Moduletech)	Subcommand Code	Metadata Flags	Option

80 03	00 00 00 00	00 00 00 20	08	E2	42	BB	AB 26

Search Flags	Access Password	Select Address	Select Data Length	Select Data	SubCRC	Terminator	CRC

Sample 3: start Asynchronous Inventory, and enable filtering and additional data, and Metadata Flags is 0x00BF.

Send command:

FF	2A	AA	4D 6F 64 75 6C 65 74 65 63 68	AA 48	00 BF	02	80 07
Header	Data Length	Command Code	Subcommand Marker (Moduletech)	Subcommand Code	Metadata Flags	Option	Search Flags

00 00 00 00	00 00 00 20	0C	E2 00	01	09
Access Password	Select Address	Select Data Length	Select Data	Embedded Command Count	Embedded Command Length

28	00 00	00	02	00 00 00 00	02	7E	BB	D0 91
Embedded Command Opcode	Embedded Command Timeout	Embedded Command Optionn	Read Membank	Read Address	Read Word Count	SubCRC	Terminator	CRC

Sample 4: start Asynchronous Inventory, not filter, enable additional data, embed 0x28 command to read four sets of additional data, read: reserved bank 0~3 blocks + EPC bank 0~7 blocks, TID bank 0~5 blocks, user bank 0~3 blocks

Send command:

FF	31	AA	4D 6F 64 75 6C 65 74 65 63 68	AA 48	00 80	00	0004
Header	Data Length	Command Code	Subcommand Marker (Moduletech)	Subcommand Code	Metadata Flags	Option	Search Flags

04	1B	28	0000	00
Embedded Command Count	Embedded Command Length	Embedded Command Opcode	Embedded Command Timeout	Embedded Command Option

00	00000000	04	01	00000000	08

Read MemBank	Read Address	Read Word Count	Read MemBank	Read Address	Read Word Count

02	00000000	06	03	00000000	04	D9	BB	DB23
Read MemBank	Read Address	Read Word Count	Read MemBank	Read Address	Read Word Count	SubCRC	Terminator	CRC

5.6.2 Asynchronous Inventory actively upload data packets

When the module is in the process of Asynchronous Inventory, the module can actively send data frames to the host. These command frames sent without a request are called active upload data packets.

Note:

●The following values are fixed:

Command Code :0xAA

5.6.2.1 Tag information data packet

The Asynchronous Inventory operation is started. If a tag is inventoried, the module will immediately upload the tag information data packet. The format of the tag information data packet complies with the general command communication protocol format.

Receive command Data field format

The tag information data packet contains the Data field when receive command.

At this time, the Data field contains the following fields, as shown in the table:

Field	**Byte length**	**Description**
Metadata Flags	2	Refer to Metadata Flags field description.
Meta Data and Tag EPC	N	Refer to Meta Data and Tag EPC field description.

Command sample:

Sample 1: Tag information data packet 1

Receive command:

FF	1B	AA	00 00	003F	01BD020DF7320000001300000C2000111120190211019422AF	E259
Header	Data Length	Command Code	Status Code	Metadata Flags	Meta Data and Tag EPC	CRC

Analysis Meta Data and Tag EPC: the metadata included can be obtained from

Metadata Flags=003F（0x0001|0x0002|0x0004|0x0008|0x0010|0x0020）

01	BD	02	0DF732	00000013	0000
Read Count	RSSI	Antenna ID	Frequency	Timestamp	Phase
0C	2000	1111201902110194			22AF
EPCLENGTH	PC	EPC			EPCCRC

Sample 2: Tag information data packet 2

Receive command:

FF	21	AA	00 00	00BF	01 D3 01 0D CC 3A 00 00 00 1A 00 17 00 00 10 30 00 E2 00 00 1D 40 01 01 58 10 40 82 73 36 C1	42 A1

Header	Data Length	Command Code	Status Code	Metadata Flags	Meta Data and Tag EPC	CRC

Then analyze Tag EPC and Meta, analyzed by Metadata Flags=00BF

（0x0001|0x0002|0x0004|0x0008|0x0010|0x0020|0x0080）

01	D3	01	0D CC 3A	0000001A	0017	0000
Read Count	RSSI	Antenna ID	Frequency	Timestamp	Phase	Tag Data Length
10	3000	E200001D4001015810408273			36C1	
EPCLENGTH	PC	EPC			EPCCRC	

Sample 3: Tag information data packet 3

Enable additional data, embed 0x28 command to read four sets of additional data, read: reserved bank 0~3 blocks + EPC bank 0~7 blocks, TID bank 0~5 blocks, user bank 0~3 blocks

Receive command:

FF	39	AA	00 00	0080	0160012345670123456793881400AAAC11221592002030 8FFFFFE2801105200076C28B570AD111112222333344440814 00AAAC11229388	AC7E
Header	Data Length	Command Code	Status Code	Metadata Flags	Meta Data and Tag EPC	CRC

Then analyze Meta Data and Tag EPC

0160	01234567 01234567	93881400 AAAC1122 15920020 308FFFFF	E2801105 200076C2 8B570AD1	1111 2222 3333 4444	08	1400	AAAC 1122	9388
Tag Data Length	reserved bank 4 blocks	EPC bank 8 blocks	TID bank 6 blocks	User bank 4 blocks	EPCLENGTH	PC	EPC	EPCCRC

Sample 4: Tag information data packet 4

Enable additional data, embed 0x28 command to read four sets of additional data, read: reserved bank 0~3 blocks + EPC bank 0~7 blocks, TID bank 0~5 blocks, user bank 0~3 blocks

Receive command:

FF	41	AA	00 00	0080	016000000000000000000092AB3400E28011052000719308240A5AE28011052000719308240A5A0000E731F6974326103400E28011052000719308240A5A92AB	AFC3
Header	Data Length	Command Code	Status Code	Metadata Flags	Meta Data and Tag EPC	CRC

Then analyze Meta Data and Tag EPC

0160	0000000000000000	92AB3400E28011052000719308240A5A	E28011052000719308240A5A	0000E731F6974326	10	3400	E28011052000719308240A5A	92AB
Tag Data Length	reserved bank 4 blocks	EPC bank 8 blocks	TID bank 6 blocks	User bank 4 blocks	EPCLENGTH	PC	EPC	EPCCRC

5.6.2.2 Heartbeat Data Packet

When the module enables the heartbeat function in the start Asynchronous Inventory command (BIT7 of Search Flags = 1), the module will periodically (approximately every 15 seconds) send a heartbeat data packet. The format of the heartbeat data packet complies with the general command communication protocol format.

Receive command Data field format

Heartbeat data packet with Data field when receive command.

At this time, the Data field contains the following fields, as shown in the table:

Field	**Byte length**	**Description**
Heartbeat Marker	4	Always "XTSJ", this field is a string represented by ASCII code.
Search Flags	2	The same as Search Flags of Send command.

Command sample: Heartbeat packet

Receive command:

FF	06	AA	00 00	58 54 53 4A	80 03	17 24
Header	Data Length	Command Code	Status Code	XTSJ	Search Flags	CRC

5.6.2.3 Polling cycle data packet

When multiple antennas are enabled and polling cycle notification is enabled (BIT5=1 of Search Flags), a notification frame will be sent in each cycle (all antennas are counted in turn), called a polling cycle data packet. The format of the polling cycle data packet follows the general command communication protocol format.

Receive command Data field format

Polling cycle data packet with Data field when receive command. At this time, the Data field contains the following fields, as shown in the table:

Field	Byte length	Description
Metadata Flags	2	Refer to Metadata Flags field description.
Meta Data and Tag EPC	N	Refer to Meta Data and Tag EPC field description. Note, The following fields in the tag data frame will be fixed or redefined as follows: EPC Length: fixed 1 Byte, value fixed is 0x05 PC Word: 2 Byte, fixed to 0x0000 EPCID: 1 Byte, the actual meaning here is ANTWORKCNT, which indicates the number of rounds of antenna polling to complete the notification frame. When ANTWORKCNT=0xFF, the next notification frame will become 0 and then start counting again. EPCCRC: 2 Byte, , fixed is 0x0000

Command sample: returns the first round of antenna polling completion notification frame.

Receive command:

<table>
<tr><td>FF</td><td>09</td><td colspan="2">AA</td><td>00 00</td><td colspan="2">00 04</td></tr>
<tr><td>Header</td><td>Data Length</td><td colspan="2">Command Code</td><td>Status Code</td><td colspan="2">Metadata Flags</td></tr>
<tr><td>02</td><td>05</td><td>00 00</td><td colspan="2">01</td><td>00 00</td><td>F5 75</td></tr>
<tr><td>Header</td><td>EPC Length</td><td>PC Word</td><td colspan="2">EPCID
(ANTWORKCNT)</td><td>EPCCRC</td><td>CRC</td></tr>
</table>

5.6.2.4 CC33 customized data packet

If CC33 customized function is enabled (Option BIT4=1), and the sent MODUSTATUS is non-zero, it includes antenna connection status + standing wave condition + module temperature. At this time, the Data field contains the following fields, as shown in the table:

Field	Byte length	Description
FIXDATA	2	Fixed is 0xCC33.
MODUSTATUS	4	Same as the host sends the module command.
ANTX	1	The currently working antenna ID.
FRE	3	The currently frequency, unit is kHz
ANT CONNECT	0/1	Antenna connection status. 0 indicates no antenna is detected; 1 indicates antenna is detected; This field is only exist when the lowest Byte BIT0=1 of MODUSTATUS.
ANT RL	0/1	Return loss value = transmission power value - reflection power value, unit is 0.1dB. This field is exist only when the lowest Byte BIT1=1 of MODUSTATUS. For the method of calculating standing wave through echo and judgment, see Standing wave detection (0xAA4A).
MODU TEMP	0/1	Module temperature value, 1 Byte, signed number, unit is Celsius. This field is only exist when the lowest Byte BIT2=1 of MODUSTATUS.

5.6.3 Stop Asynchronous Inventory(0xAA49)

Command Description

If enable Asynchronous Inventory operation, can use this command to stop Asynchronous Inventory.

Command features

SubCommand Code	Bootloader command	App Firmware command	Subcommand Data
0xAA49	None	exist	Send command none, Receive command none

Note:

●If the module is currently running Asynchronous Inventory and receives other commands with correct CRC (including the command to start Asynchronous Inventory), the module will exit Asynchronous Inventory and return a command failure response with status code 0xAA49. For example, if FF00031D0C is sent after starting Asynchronous Inventory, the module will return FF0003AA491EEA. If it is other status codes, it means other abnormal conditions of the module.

●If the module is not currently started with Asynchronous Inventory, it will return a successful execution if it receives the AA49 command.

Command sample:

Send command:

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

Header	Data Length	Command Code	Subcommand Marker (Moduletech)	Subcommand Code	Sub CRC	Terminator	CRC

Receive command:

FF	0C	AA	00 00	4D 6F 64 75 6C 65 74 65 63 68	AA 49	0F 22
Header	Data Length	Command Code	Status Code	Subcommand Marker (Moduletech)	Subcommand Code	CRC

5.6.4 EX Asynchronous Inventory(0xAA58)

Command Description

This inventory mode use Asynchronous mode (the same as AA48).

AA58 can be used in a large number of tag environments. UHF modules based on E series chips support this command.

During Asynchronous Inventory, the normal end command is to stop the Asynchronous Inventory command and return a normal status code. Sending other commands or module abnormalities will end the inventory and return "AA59 Stop Asynchronous Inventory with an error status code".

Command Features

SubCommand Code	Bootloader command	App Firmware command	Subcommand Data
0xAA58	None	exist	Send command exist, Receive command none

Send command SubData field format

Asynchronous Inventory (0xAA58) with SubData field when send command. At this time, the Data field contains the following fields, as shown in the table:

Field	Byte length	Description
ExConfigData	20	Only the first Byte can be set, and the other Bytes can be 0. When the first Byte is 0, it is dense tag mode, which is mainly used for reading more and reading all tags, a large number of tags or in complex environments. When the first Byte is 1, it means that the number of tags is not large and it is very easy to read, which can relatively reduce the time to read all tags.
Metadata Flags	2	Refer to Metadata Flags field description.
Option	1	Meaning is the same as 0x22 command, not support Match Filter.
Search Flags	2	The meaning of low Byte, refer to 0x22 command, not support embed additional data functionality, not support TagFocus. High Byte control bit refer to AA48 command, not support BIT6-bit single antenna inventory without automatic stop function for adding new tags.
Access Password	0/4	Meaning the same as 0x22 command.
Tag Singulation	0/N	Meaning the same as 0x22 command.
Embedded Command Content	0/N	Meaning the same as 0x22 command.

Note:

●For inventory polling rules, refer to the polling rules in the precautions of Asynchronous Inventory (0xAA48).

●This command is applicable to environments where a large number of tags are read, such as a scene where a large number of tags are counted by a handheld device, a scene where a large number of tags are counted in a smart cabinet or filing cabinet, or a scene where the items in the cabinet are complex and difficult to read, or a scene where the tags are stacked and difficult to read.

●This command does not require/cannot specify Session, Target, Q, RF_mode. The module handles it internally, and the configuration does not work. Filtering is not supported, and additional data is not supported.

●This command is only supported in China, CE, INDIA, RUSSIA, PHILIPPINES, JAPAN (all), and ISRAEL. Other regions do not support it.

Send command:

FF	27	AA	4D6F64756C6574656368	AA 58
Header	Data Length	Command Code	Subcommand Marker (Moduletech)	Subcommand Code

00000000000000000000 00000000000000000000	00 3F	00	00 00	41	BB	3F7D
ExConfigData	Metadata Flags	Option	Search Flags	SubCRC	Terminator	CRC

Receive command:

FF	0C	AA	00 00	4D 6F 64 75 6C 65 74 65 63 68	AA 58	0F 33
Header	Data Length	Command Code	Status Code	Subcommand Marker (Moduletech)	Subcommand Code	CRC

5.6.5 Stop EX Asynchronous Inventory (0xAA59)

Command Description

If enable EX Asynchronous Inventory operation, then can use this command to stop EX Asynchronous Inventory。

Command Features

SubCommand Code	Bootloader command	App Firmware command	Subcommand Data
0xAA59	none	exist	Send command none, Receive command none

Note:

●If the module is running EX Asynchronous Inventory and receives other valid commands (including the command to start EX Asynchronous Inventory), the module will exit EX Asynchronous Inventory and return a command failure response with error code 0xAA59. If it is other codes, it is other abnormal conditions of the module; for example, if FF00031D0C is sent after starting Asynchronous Inventory, the module will return FF0003AA591EEA.

●If the module is not currently started and EX Asynchronous Inventory receives the EX Asynchronous Inventory command stop command, it returns execution success.

Command Sample:

Send command:

FF	0E	AA	4D 6F 64 75 6C 65 74 65 63 68	AA 59	F3	BB	E1 A0

Header	Data Length	Command Code	Subcommand Marker (Moduletech)	Subcommand Code	Sub CRC	Terminator	CRC

Receive command:

FF	0C	AA	00 00	4D 6F 64 75 6C 65 74 65 63 68	AA 59	0F 32
Header	Data Length	Command Code	Status Code	Subcommand Marker (Moduletech)	Subcommand Code	CRC

6 Tag Access Commands

Tag access operations include reading, writing, locking, and destroying tags. The first tag that responds to the module will be the actual target of the operation.

It is necessary to have a certain understanding of the Gen2 protocol tag memory. Refer to Appendix 3 for the Gen2 protocol memory.

Tag access instructions comply with the general command communication protocol format.

Tag Access Command Abstract

Command	Command Code	Description
Write Tag EPC	0x23	Updating the tag EPC code (which will automatically modify the PC block content) will affect the EPC ID data content or length read during inventory operations.
Write Tag Data	0x24	Writing data to the specified address in the tag memory bank, note that modifying the EPCID content block will not change the length of the EPCID read during inventory, it only modifies the corresponding data block.
Lock Tag	0x25	Lock or unlock the specified tag memory bank.
Kill Tags	0x26	Kill the tags.
Read Tag Data	0x28	Read the contents of the tag memory bank.

Notes:

●Tag memory operations must first specify a single operating antenna.
●Required power: Writing tag > Reading tag.

6.1 Write EPCID(0x23)

Command Description

This is used to update the tag EPC code, the difference from the 0x24 command is that this command automatically changes the value of the bit in the PC that indicates the EPCID length based on the length of the data written by the user. This command writes the EPC ID to the EPC area starting from the 0x20 bit address. The first responding module's tag will be the one actually operated.

Command Features

Command Code	Bootloader Command	App Firmware Command	Data field
0x23	Valid	Invalid	Has data when sending, no data when not embedding read command in receiving, has data when embedding read command.

Send Command Data Field Format

When sending the Write Tag EPC (0x23) command, the Data field is included. The Data field contains the following fields, as shown in the table：

Field	Byte length	Description
Timeout	2	Refer to the Timeout field description.
WriteReadFlag	0/1	Enable the function of reading the memory bank after writing. When enabled, this field must be present with a fixed value of 0x8C. When not enabled, won’ t need this field.
Option	1	The Option field contains Select-Option Bits control bits.

Field	Byte length	Description
RFU	0/1	Determined by Option, this field exists only when WriteReadFlag is absent and Option = 0x00, with a fixed value of 0x00. Otherwise, this field does not exist.
Access Password	0/4	Meaning is the same as command 0x22.
Tag Singulation	0/N	Meaning is the same as command 0x22.
Tag EPC ID	N	The written EPCID, with an even number of Bytes in length, can write up to 31 blocks (62 Bytes) at a time.
ReadBank	1	Specify the tag bank to be read, this field exists only if the WriteReadFlag field is present.
Read Address	4	Starting address word to be read, this field exists only if the WriteReadFlag field is present.。
Read Length	1	Length of data words to be read, this field exists only if the WriteReadFlag field is present.

Receive Command Data Field Format

When the 0x23 command has the embedded read function, the receiving command contains the Data field, which includes the following domains:

Field	Byte Length	Description
WriteReadFlag	1	Indicates enable the function to write and then read the memory bank, with a fixed value of 0x8C.
Option	1	Same as send command Option
Read DATA	N	The data read (with a length specified in the sent command).

Notes:

●If dynamic Q is setted, the module will use Q=2. If static Q is setted, the module will follow the corresponding settings.

●If Target A-B is set, the module will set Target A. If Target B-A is set, the module will set Target B. If static Target is set, the module will follow the corresponding setting.

●A single operating antenna must be specified first.

●The tag must have an EPC bank, be in a writable/modifiable state (not permanently locked), and have sufficient storage capacity to accommodate the EPCID to be written.

Command Example:

Example 1: Do not enable selective matching filter.

Send Command:

FF	0C	23	03 E8	00	00	1111222233334444	632C
Header	Data Length	Command Code	Timeout	Option	RFU	Tag EPC ID	CRC

Received Command:

FF	00	23	00 00	90 C1
Header	Data Length	Command Code	Status Code	CRC

Example 2: Enable tag match filter, matching filter region is EPC bank, matching address is 0x00000020, matching data length is 0x08 bits, matching data is 0x11, matching rule is to select tags that do not match the data characteristics, i.e., tags whose data starting at address 0x00000020 is not 0x11 are selected.

Send Command:

FF	19	23	03 E8	0C	00000000
Header	Data Length	Command Code	Timeout	Option	Access Password

00 00 00 20	08	11	111122223333444455556666	57 3E
Select Address	Select Data Length	Select Data	Tag EPC ID	CRC

If there are no tags that meet the conditions,

Received Command:

FF	00	23	04 00	94 C1
Header	Data Length	Command Code	Status Code	CRC

Example 3: Enable tag match filter, matching filter region is EPC region, matching address is 0x00000020, matching data length is 0x08 bits, matching data is 0x11, i.e., tags whose data starting at address 0x00000020 is 0x11 are selected.

Send Command:

FF	19	23	03 E8	04	00000000
Header	Data Length	Command Code	Timeout	Option	Access Password

00 00 00 20	08	11	111122223333444455556666	98 48
Select Address	Select Data Length	Select Data	Tag EPC ID	CRC

Received Command:

FF	00	23	00 00	90 C1
Header	Data Length	Command Code	Status Code	CRC

Example 4: write EPC data, 1122334455667788 99AABBCC11223344 5566778899AABBCC 1122334455667788 99AABBCC11223344 5566

And read CRC+PC+EPC, i.e., read the content starting from EPC region address 0 with a word length of 0x17.

Send Command:

FF	34	23	03 E8	8C	00	1122334455667788 99AABBCC11223344 5566778899AABBCC 1122334455667788 99AABBCC11223344 5566
Header	Data Length	Command Code	Timeout	WriteReadFlag	Option	Tag EPC ID

01	00 00 00 00	17	E4 A5
ReadBank	Read Address	Read Length	CRC

Received Command:

FF	30	23	00 00	8C	00
Header	Data Length	Command Code	Status Code	WriteReadFlag	Option

54 B8 AC 00 1122334455667788 99AABBCC11223344 5566778899AABBCC 1122334455667788 99AABBCC11223344 5566	A6 B3
Read DATA	CRC

Example 5: Select Option=0x01, matching filter EPC region, Access Password=0x00000000, filter bit length 0x20, filter data 0x11223344,

Write EPC data: 1122334455667788 99AABBCC11223344 5566778899AABBCC 1122334455667788 99AABBCC11223344 5566

And read the TID region, starting address 0, word length 0x06

Send Command:

FF	3D	23	03 E8	8C	01	00000000	20
Header	Data Length	Command Code	Timeout	WriteReadFlag	Option	Access Password	Select Data Length

11223344	1122334455667788 99AABBCC11223344 5566778899AABBCC 1122334455667788 99AABBCC11223344 5566	02	00000000	06	59 21
Select Data	Tag EPC ID	Read Bank	Read Address	Read Length	CRC

Received Command:

FF	0E	23	00 00	8C	01
Header	Data Length	Command Code	Status Code	WriteReadFlag	Option

E2 80 11 0C 20 00 77 0B 04 BE 09 71	3D 26
Read DATA	CRC

6.2 Write Memory Bank (0x24)

Command Description

This command is used to write data to the specified address of the tag bank. This command performs word writing, with the minimum write unit being one word (2 bytes). The first tag that responds to the module will be actually operated on.

Command Features

Command Code	Bootloader Command	App Firmware Command	Data Field
0x24	Invalid	Valid	The send command exists, while the receive command depends on whether there is a need for a read-back.

Send Command Data Field Format

When sending the command for writing tag data (0x24), the Data field includes the following domains, as shown in the table:

Field	Byte Length	Description
Timeout	2	Refers Timeout field description.
WriteReadFlag	0/1	Enable the function to write and read the storage area. When enabled, this field must be present and have a fixed value of 0x84. When not enabled, this field will not be present.
Option	1	The Option field contains Select-Option Bits control bits.
Write Address	4	Write the starting block address. Start from 0.

Field	Byte Length	Description
Write MemBank	1	RESERVED=0; EPC=1; TID=2; USER=3
Access Password	0/4	Same definition with 0x22 Command.
Tag Singulation	0/N	Same definition with 0x22 Command.
Write Data	N	The written data, with an even number of bytes in length, can be written up to 32 blocks (64 bytes) at a time.
ReadBank	1	The specified tag memory region to read is present only when the WriteReadFlag field is included
Read Address	4	The starting address of the data to be read is present only when the WriteReadFlag field is included.
Read Length	1	The length of the data to be read is present only when the WriteReadFlag field is included.

Received Command Data Field Format

When the 0x24 command includes embedded read functionality, the Data field in the received instruction contains the following fields:

Field	Byte Length	Description
WriteReadFlag	1	Indicates the enablement of the function to read out the storage area after writing, with a fixed value of

Field	Byte Length	Description
		0x84.
Option	1	Same as send command Option
Read DATA	N	The data read from the storage area, with a length specified in the sent command

Notes：

- If dynamic Q is configured, the module will use Q=2. If static Q is configured, the module will follow the corresponding configuration.
- If Target A-B is configured, the module will use Target A. If Target B-A is configured, the module will use Target B. If a static Target is configured, the module will follow the corresponding configuration.
- A single operating antenna must be specified first.
- The tag must have the corresponding memory bank, its current state must allow writing/modification (not permanently locked), and the memory size must be sufficient to accommodate the data to be written.。

Command Example:

Example 1: To write the data 0xAAAABBBBCCCCDDDD to the starting address 1 in the USER bank without using tag matching filtering.

`Write Address=0x00000001;`

`Write MemBank=0x03`

`Write Data=0xAAAABBBBCCCCDDDD`

Send Command:

FF	10	24	03 E8	00	00 00 00 01
Header	Data Length	Command Code	Timeout	Option	Write Address

03	AA AA BB BB CC CC DD DD	C7 B3
Write MemBank	Write Data	CRC

Received Command(Write failed, as memory bank locked):

FF	00	24	04 24	E4 02
Header	Data Length	Command Code	Status Code	CRC

Example 2: Without using tag match filtering, write 0xAAAABBBBCCCCDDDD into 1 block of the USER bank.

`Write Address=0x00000001`

`Write MemBank=0x03`

`Write Data=0xAAAABBBBCCCCDDDD`

Send Command:

FF	10	24	03 E8	00	00 00 00 01	03
Header	Data Length	Command Code	Timeout	Option	Write Address	Write MemBank

AA AA BB BB CC CC DD DD	C7 B3
Write Data	CRC

Received Command(Write tags successfully):

FF	00	24	00 00	E0 26

Header	Data Length	Command Code	Status Code	CRC

Example 3: Using tag matching filter

```
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
```

Send Command:

FF	1B	24	03 E8	04	00000000	00
Header	Data Length	Command Code	Timeout	Option	Write Address	Write MemBank

CCCCDDDD	00000020	0C	1110	AAAABBBB CCCCDDDD	26 AA
Access Password	Select Address	Select Data Length	Select Data	Write Data	CRC

Example 4: Using tag matching filter

```
Write MemBank=0x03(USER bank)
Write Address=0x00000002
Write Data=0x1111222200000000
Access Password=0x00000000
Select MemBank=0x01 (EPC bank)
Select Data Length (bits)=0x60
Select Data=0x0123456789ABCDEF01234567
```

Send Command:

FF	21	24	03 E8	01	00000002	03	00000000
Header	Data Length	Command Code	Timeout	Option	Write Address	Write MemBank	Access Password

60	0123456789AB CDEF01234567	11112222 00000000	27 03

Select Data Length	Select Data	Write Data	CRC

Example 5:

Assume tag Epc: 0xFFFF FFFF

Select Option = 0x01, matching filter in EPC bank, Access Password = 0x00000000, filter bit length 0x20, filter data 0xFFFFFFFF. Write to the User bank (0x03), starting address 0x00000000, data: 0xBBBBBBBB. Read data from the Tid bank (0x02), starting address 0x00000002, data length 0x02.

Send Command:

FF	1C	24	03 E8	84	01	00000000	03
Header	Data Length	Command Code	Timeout	WriteReadFlag	Option	Write Address	Write bank

00000000	20	FFFFFFFF	BBBBBBBB	02	00000002	02	415F
Access Password	Select Data Length	Select Data	Write Data	Read Bank	Read Address	Read Length	CRC

Received Command:

FF	06	24	00 00	84	01
Header	Data Length	Command Code	Status Code	WriteReadFlag	Option

20 00 FC 02	14 DF
Read DATA	CRC

Example 6:

Assume the tag EPC: 0xFFFF FFFF,

Select Option=0x01, matching filter EPC bank, Access Password=0x11112222, filter bit length 0x20, filter data 0xFFFF FFFF,

Write to USER area (0x03), starting address 0x00000000, data: 0xBBBB BBBB

Read USER area data (0x03), starting address 0x00000000, data length 0x02

Send Command:

FF	1C	24	03 E8	84	01	00000000	03
Header	Data Length	Command Code	Timeout	WriteReadFlag	Option	Write Address	Write bank

11112222	20	FFFFFFFF	BBBBBBBB	03	00000000	02	0BE6
Access Password	Select Data Length	Select Data	Write Data	Read Bank	Read Address	Read Length	CRC

Received Command:

FF	06	24	00 00	84	01
Header	Data Length	Command Code	Status Code	WriteReadFlag	Option

BB BB BB BB	81C7
Read DATA	CRC

Example 7:

Select Option=0x00, write to USER bank (0x03), starting address 0x00000000, data: 0xBBBB BBBB;

Read TID area data (0x02), starting address 0x00000002, data length 0x02

Send Command:

FF	13	24	03 E8	84	00	00000000	03
Header	Data Length	Command Code	Timeout	WriteReadFlag	Option	Write Address	Write bank

BB BB BB BB	03	00000000	02	0BE6
Write Data	Read Bank	Read Address	Read Length	CRC

Received Command:

FF	06	24	00 00	84	00
Header	Data Length	Command Code	Status Code	WriteReadFlag	Option

20 00 77 0B	A8E6
Read DATA	CRC

6.3 Lock Tags (0x25)

Command Description

This command is used to lock or unlock the specified tag memory bank, and the first tag responding from the module will be the one actually operated on.

Command Features

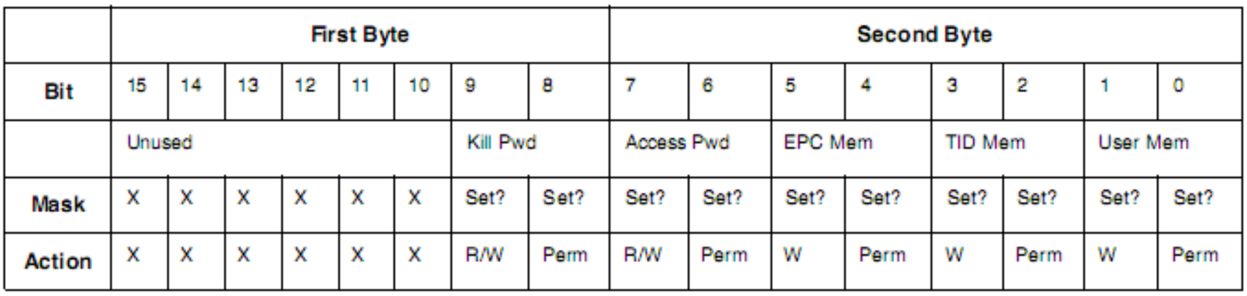
Command Code	Bootloader Command	App Firmware Command	Data Field
0x25	Invalid	Valid	The send command exists, but the receive command does not exist

Send Command in Data Field Format

Lock Tag (0x25) command is accompanied by the Data field when sent. The Data field includes the following fields, as shown in the table:

Field	Byte Length	Description
Timeout	2	Refer to Timeout field description
Option	1	Option field included Select-Option Bits control bit Option=0x05 cannot use in this command
Access Password	4	Tag Access password
Mask Bits	2	See pic 6，When the corresponding bit is set to 1, it indicates the execution of the corresponding

Field	Byte Length	Description
		ACTIONBIT operation. Mask Bits is a term defined in the Class-1 Generation-2 UHF RFID specification. For detailed information, please refer to the Class-1 Generation-2 UHF RFID specification。
Action Bits	2	The bits in ACTIONBIT only take effect when the corresponding MASKBIT bit is set to 1. 0 is unlock, 1 is lock. Action Bits are terms defined in the Class-1 Generation-2 UHF RFID specification. For more detailed information, please refer to the Class-1 Generation-2 UHF RFID specification
Tag Singulation	0/N	Same definition with 0x22 command



	First Byte								Second Byte							
Bit	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
	Unused						Kill Pwd		Access Pwd		EPC Mem		TID Mem		User Mem	
Mask	X	X	X	X	X	X	Set?	Set?	Set?	Set?	Set?	Set?	Set?	Set?	Set?	Set?
Action	X	X	X	X	X	X	R/W	Perm	R/W	Perm	W	Perm	W	Perm	W	Perm

Figure 6

As shown in Figure 6, both the Mask and Action fields are 2 bytes, with the lower 10 bits being valid.

The lower 10 bits of the Mask field correspond to whether the lower 10 bits of the Action field are effective.

R/W: Operations for read/write functions. W: Operations for write functions only. Set to 1 for lock; set to 0 for unlock.

Perm indicates the lock type, with 1 representing a permanent lock, meaning it cannot be unlocked or written to.

The table below describes the Bit values of Mask and Action corresponding to the five operations.

No Act:

0	0
0	0

lock:

1	0
1	0

unlock:

1	0
0	0

Per lock:

1	1
1	1

Per unlock:

1	1
0	1

	Zero-lock / No lock			Not Zero-lock			Non-zero lock (temporary)			Permanent lock			Permanent unlock		
Bank	read	write	lock/unlock	read	write	lock	read	write	unlock	read	write	unlock	read	write	lock
Reserve	✓	✓	✓	✓	✓	Passworded	Passworded	Passworded	Passworded	×	×	×	✓	✓	×
EPC	✓	✓	✓	✓	✓	Passworded	✓	Passworded	Passworded	✓	×	×	✓	✓	×
TID	✓	×	none	✓	×	none	✓	×	none	✓	×	none	✓	×	none
User	✓	✓	✓	✓	✓	Passworded	✓	Passworded	Passworded	✓	×	×	✓	✓	×
Locking steps for blank tag with all-zero password (choose one):															
First, write the access password + write to EPC user bank (order does not matter). Then, use the access password to lock the reserve and EPC user banks (order doesn't matter)															
First, write the access password. Next, use the access password to lock the reserve and EPC user banks. Finally, use the access password to write to the EPC user bank.															

Notes:

- If dynamic Q is configured, the module will use Q=2. If static Q is configured, the module will follow the corresponding setting.
- If Target A-B is configured, the module will use Target A. If Target B-A is configured, the module will use Target B. If static Target is configured, the module will follow the corresponding setting.
- A single operational antenna must be specified first.

Command Example：

Example 1

Filter EPCID=0x111122223333444455556666, access password=0x11223344, enable tag filtering, and lock the EPC bank.

Send Command：

FF	18	25	03 E8	01	1122 3344	00 20	00 20	60	11112222 33334444 55556666	9E 7A
Header	Data Length	Command Code	Timeout	Option	Access Password	Mask Bits	Action Bits	Select Data Length	Select Data	CRC

Example 2

Access password=0x11223344, enable tag filtering with EPCID starting byte 0x11, and lock the EPC bank.

Send Command：

FF	11	25	03 E8	04	1122 3344	00 20	00 20	00 00 00 20	08	11	94 32
Header	Data Length	Command Code	Timeout	Option	Access Password	Mask Bits	Action Bits	Select Address	Select Data Length	Select Data	CRC

Example 3

EPCID=0x111122223333444455556666, access password = 0x11223344, lock the USER bank without using tag filtering

Send Command：

FF	0B	25	03 E8	00	11223344	00 02	00 02	0F A9
Header	Data Length	Command Code	Timeout	Option	Access Password	Mask Bits	Action Bits	CRC

6.4 Kill Tags(0x26)

Command Description

This command invalidates the tag so that it cannot be recognized. The tag of the first responding module will be actually operated on.

Command Features

Command Code	Bootloader Command	App Firmware Command	Data Field
0x26	invalid	valid	Present in the transmitted instruction, absent in the received instruction

Send Command in Data Field Format

Kill Tag (0x26) Command, when sent, includes the Data field, which contains the following fields as shown in the table:

Field	Byte Length	Description
Timeout	2	Refer to Timeout field description。
Option	1	The Option field contains Select-Option Bits control bits. Option = 0x05 cannot be used for this command
Kill Password	4	The kill password of tags.

Field	Byte Length	Description
RFU	1	Reserved, has to be 0x00
Tag Singulation	0/N	Same definition with 0x22 command

Notes:

- If dynamic Q is setted, the module will use Q=2. If static Q is setted, the module will follow the corresponding setting.
- If Target A-B is setted, the module will use Target A. If Target B-A is setted, the module will use Target B. If static Target is setted, the module will follow the corresponding setting.
- A single operational antenna must be specified first.

Command Examples：

Example 1: can’ t use tag filter

Send Command：

FF	08	26	03 E8	00	11223344	00	91 16
Header	Data Length	Command Code	Timeout	Option	Kill Password	RFU	CRC

Example 2: Enable tag filtering, filter bank set to USER.

Send Command：

FF	10	26	03E8	03	1122 3344	00	0000 0000	18	111122	BF 40

Header	Data Length	Command Code	Timeout	Option	Kill Password	RFU	Select Address	Select Data Length	Select Data	CRC

Example 3: Enable tag filtering, filter bank set to EPC

Send Command:

FF	13	26	03E8	01	11112222	00	50	112233445566778899AA	B969
Header	Data Length	Command Code	Timeout	Option	Kill Password	RFU	Select Data Length	Select Data	CRC

6.5 Read Tags Memory Bank (0x28)

Command Description

Read the content of the tag’ s memory bank; the first responding tag will be acted upon.

Command Features

Command Code	Bootloader Command	App Firmware Command	Data Field
0x28	invalid	Valid	There are send commands and receive commands.

Send Command in Data Field Format

The send command to read the tag memory bank (0x28) includes a Data field with the following domains, as shown in the table:

Field	Byte Leength	Description
Timeout	2	Refer to Timeout field description.
Option	1	Option field include Select-Option Bits control bit and Nol-Select-Option Bits-0x28 control bit
Metadata Flags	0/2	This field tells the module the metadata to return. This field exists only when Option BIT4=1
Read MemBank	1	Specify the memory bank to read: RESERVED=0; EPC=1; TID=2; USER=3.

Field	Byte Leength	Description
Read Address	4	Read the starting address, i.e., the block address of the memory bank starting from 0.
Word Count	1	The number of blocks to read, up to a maximum of 96 blocks (192 bytes) at a time.
Access Password	0/4	Same definition with 0x22 command
Tag Singulation	0/N	Same definition with 0x22 command

Receive Command in Data Field Format

The receive command to read the tag memory bank (0x28) includes a Data field.

Field	Byte Length	Description
Option	1	Same as the Option field in the send command.
Metadata Flags	0/2	Same as the Metadata Flags field in the send command. This field exists only when Option BIT4=1.
Metadata	0/N	The length of the Metadata field is determined by the Metadata Flags. This field exists only when Option BIT4=1.
Data Read	N	The data read from the tag memory bank.

Notes:

- If dynamic Q is set, the module will use Q=2. If static Q is set, the module will follow the corresponding setting.
- If Target A-B is set, the module will use Target A. If Target B-A is set, the module will use Target B. If static Target is set, the module will follow the corresponding setting.
- A single operational antenna must be specified first.

- The tag must have the memory bank, the current status must allow reading, and the size must not exceed the memory space.

Command Examples:

Example 1: Disable tag match filter and read 2 blocks from address 1 in the TID bank

Send Command:

FF	09	28	03E8	00	02	00000001	02	C1 F3
Header	Data Length	Command Code	Timeout	Option	Read MemBank	Read Address	Word Count	CRC

Received Command:

FF	05	28	00 00	00	60040135	13 04
Header	Data Length	Command Code	Status Code	Option	Data Read	CRC

Example 2

Enable tag match filter, read 3 blocks from address 1 in the TID bank, with password 0x00000000, match region as TID, starting address 0x10 bit, match length 4 bit, match data 0x60.

Send Command:

FF	13	28	03 E8	02	02	00000001
Header	Data Length	Command Code	Timeout	Option	Read MemBank	Read Address

03	00000000	00000010	04	60	7C91
WordCount	Access Password	Select Address	Select Data Length	Select Data	CRC

Received Command:

FF	07	28	00 00	02	60040135F869	6C29
Header	Data Length	Command Code	Status Code	Option	Data Read	CRC

Example 3

Filter EPCID=0x0123456789ABCDEF01234567, read USER bank, enable tag match filter.

Send Command:

FF	1A	28	03 E8	01	03	00000002
Header	Data Length	Command Code	Timeout	Option	Read MemBank	Read Address

04	00000000	60	0123456789ABCDEF01234567	7AC1
Word Count	Access Password	Select Data Length	Select Data	CRC

Received Command:

FF	09	28	00 00	01	AA BB CC DD 00 00 00 00	E754
Header	Data Length	Command Code	Status Code	Option	Data Read	CRC

Example 4

Read tag data and return tag metadata.

Send Command:

FF	15	28	03 E8	14	00 14	00	00000002
Header	Data Length	Command Code	Timeout	Option	Metadata Flags	Read MemBank	Read Address

02	00000000	00000078	08	34	9C0E
WordCount	Access Password	Select Address	Select Data Length	Select Data	CRC

Received Command:

FF	0C	28	00 00	14	00 14	02	0000 0015	1234 5678	DC 42
Header	Data Length	Command Code	Status Code	Option	Metadata Flags	Antenna ID	Timestamp	Tag Data	CRC

6.6 BlockWrite Tags Memory Bank (0x2D)

Command Description

When the tag supports "BlockWrite", the "Block Write Command" can be used to write a large amount of data into the tag storage area (a whole storage area) at one time more quickly. The tag of the first response module will be actually operated.

Command Features

Command Code	**Bootloader Command**	**App Firmware Command**	**Data Field**
0x2D	invalid	valid	Send command available, receive command unavailable

Notes:

- If dynamic Q is configured, the module will use Q=2. If static Q is configured, the module will follow the corresponding configuration.

●If Target A-B is configured, the module will use Target A. If Target B-A is configured, the module will use Target B. If static Target is configured, the module will follow the corresponding configuration.

●A single operation antenna must be specified first.

●The tag must have the specified memory bank, be in a state that allows writing/modification (not permanently locked), and have sufficient memory space to accommodate the data being written.

●The tag must support this feature to function properly.

Send Command in Data format

The block write tag (0x2D) sends a command with a Data field, which includes the following fields, as shown in the table:

Field	Byte Length	Description
Timeout	2	Reder to Timeout field description.
Chip Type	1	0x00
Option	1	The Option field contains the Select-Option Bits control bit, and BIT6=1。
Sub Command write	2	Fixed 0x00C7，BLOCK WRITE。

Field	Byte Length	Description
Access Password	0/4	Same with 0x22 command.
Tag Singulation	0/N	Same with 0x22 command.
Write Flags	1	0x00
Write MemBank	1	Specifying a memory bank：RESERVED=0; EPC=1; TID=2; USER=3
Write Address	4	Write start address, with block addresses starting from 0.
WordCount	1	Number of blocks to write, up to 48 blocks (96 bytes) at a time.
Data	2*WordCount	The data written is WordCount*2 bytes.

Command Example：

Example 1：enable selection match filter functions：

Send Command:

FF	19	2D	03 E8	00	44	00 C7
Header	Data Length	Command Code	Timeout	Chip type	Option	Sub Command write

1122 3344	0000 0078	08	34	00	00	0000 0000	01	00 00	90 E3
Access password	Select Address	Select data length	Select data	Write Flag	Write MemBank	Write Address	Word count	Data	CRC

Received Command:

FF	00	2D	00 00	710F
Header	Data Length	Command Code	Status Code	CRC

Example 2: don’t enable selection match filter functions.

Send Command:

FF	15	2D	03 E8	00	40	00 C7
Header	Data Length	Command Code	Timeout	Chip type	Option	Sub Command write

00	03	0000 0000	04	11112222 33334444	8D2D
Write Flags	Write MemBank	Write Address	Word Count	Data	CRC

Received Command:

FF	00	2D	00 00	710F
Header	Data Length	Command Code	Status Code	CRC

7 Setting Commands

The set command is used to configure configurable values in the firmware. Since these values are not stored in the module's Flash, they will reset to default values upon restarting the application firmware. The set command follows the general command communication protocol format.

Overview of set commands

Command	Command Code	Description
Set Antenna Ports	0x91	Configure antenna ports. Configurable items include the antenna used for tag access operations, the antenna used for inventory operations, and the module's transmit power.
Set the Current Tag protocol	0x93	Set the tag protocol for operations.
Set frequency hopping	0x95	Set the frequency hopping table and regulatory hopping time。
Set GPIO	0x96	Set and get the status of GPIO pins.
Set the current working area	0x97	Set the module's current operating area.
Set unique configuration	0x9A	Set the module's unique configuration options.

Command	Command Code	Description
Set Tag Protocol Configuration	0x9B	Set protocol-specific configuration parameters for tags.

7.1 Set power/enable antenna ports(0x91)

Command Description

This command uses the concept of logical antenna numbers. Logical antennas are divided into antennas used for transmission and antennas used for reception.
The logical antenna number used for transmission is called the TX Logical Antenna Number.
The logical antenna number used for reception is called the RX Logical Antenna Number.
The mode adopts a transceiver-integrated configuration, meaning that when an antenna port is operating, it both transmits and receives signals.
When multiple antennas are set to operate, the working sequence of the antennas follows the order from physical antenna port 1 -> 2 -> ... -> 32.

TX ANT NUM (Logical number)	RX ANT NUM (Logical number)	Actual physical antenna port
0x01	0x01	ANT 1
0x02	0x02	ANT 2

…	…	…
0x20	0x20	ANT 32

By default, antenna 1 is enabled when the module is powered on. After powering on, the antennas to be used need to be configured according to section 2.3. When enabling antennas, the new configuration will overwrite the old configuration. For example, in a four-antenna module, the following instructions are executed:

The first instruction enables antennas 1, 2, and 3 (antenna 4 will be disabled, i.e., antenna 4 will not be used for inventory).

The second instruction enables antennas 1 and 4 (antennas 2 and 3 will be disabled, i.e., antennas 2 and 3 will not be used for inventory).

Enabled antennas are used for inventory instructions (e.g., 22 and AA48). If all antennas are to be disabled, simply disable inventory.

The default initial transmit power is the module's maximum power. Configuring the power will not affect the enabled antennas.

Command Features

Command Code	Bootloader Command	App Firmware Command	Data Field
0x91	invalid	valid	Send command available, receive command unavailable.

Send Command in Data Field Format

Option	Definition
none	Enable single antenna operation
0x00	Enable single antenna operation
0x01	Option 1 is not supported

0x02	Enable single antenna or multiple antennas operation
0x03	Set transmit and receive power
0x04	Set transmit and receive power + antenna stabilization time

The antenna setup command has two formats (enable and configure).

If you want to enable the working antennas, then Option is either absent, or equal to 0 or 2. In this case, the Data field contains the following fields:

Field	**Byte Length**	**Description**
Option	0/1	When setting a single antenna port, Option can be absent or = 0 or = 2. When setting multiple antenna ports, Option must exist and is fixed to 2.
TX, RX Logical Antenna Number pairs	N*2(Note: N∈[1,32])	N*2 bytes TX, RX antenna number, the first byte is TX, the second byte is RX. It depends on the number of antenna ports of the module and the number of antennas to be enabled. The antenna numbers can be in any order in the command.

If you want to configure antenna power and stabilization time, then Option=3 or=4. In this case, the Data field contains the following fields:

Field	Byte Length	Description
Option	1	0x03, set only the antenna transmit and receive power; 0x04, set transmit and receive power + stabilization time (invalid).
TX Logical Antenna Number	1	Antenna number, such as 1, such as 4.
Read Power	2	Read the transmit power of related operations in units of 0.01dBm with an actual accuracy of 1dBm.
Write Power	2	Write the transmit power of related operations in units of 0.01dBm with an actual accuracy of 1dBm.
Setting Time	0/2	When the antenna is switched, it is used to configure the stabilization time required for the antenna, in μs (invalid). This field exists only when Option=0x04
Repeat the above four fields.	N*5 or N*7	As described above

Command Examples:

Example 1: Set antenna port 1 as the antenna used for tag access operations.

Enable only antenna 1 (Option=0x00).

Send Command:

FF	03	91	00	01	01	6287
Header	Data Length	Command Code	Option	TX Logical Antenna Number	RX Logical Antenna Number	CRC

Example 2: Set antenna ports 1 and 4 as the antennas used for tag inventory.

Enable antennas 1 and 4 (Option=0x02).

Send Command:

Impinj RFID Series Protocol Document

FF	05	91	02	01	01	04	04	2BC6
Header	Data Length	Command Code	Option	TX Logical Antenna Number	RX Logical Antenna Number	TX Logical Antenna Number	RX Logical Antenna Number	CRC

Example 3: Set the antenna power. Set the power of physical antenna ports 2 and 3 to 30dBm (Option=0x03).

Send Command:

FF	0B	91	03	02	03 E8	0B B8	03	03 E8	0B B8	F2F5
Header	Data Length	Command Code	Option	TX Logical Antenna Number	Read Power	Write Power	TX Logical Antenna Number	Read Power	Write Power	CRC

7.2 Set Protocol: GEN2(0x93)

Command Description

Set the tag protocol used for the operation. All modules support only the GEN2 (18000-6C) protocol. When the module is powered on, the GEN2 (18000-6C) protocol is used by default, so you do not need to use this command.

Command Features

Command Code	Bootloader Command	App Firmware Command	Data Field
0x93	invalid	valid	There’ s sending commands, but there’ s not received commands.

Send Command in Data Field Format

Set the current tag protocol (0x93) to send a command with the Data field. The Data field contains the following fields:

Field	Byte Length	Description
Current Protocol	2	0x0005 all of the modules only support GEN2(18000-6C) protocol, this field has to be 0x0005.

Command Example：

Send Command:

FF	02	93	00 05	51 7D

Header	Data Length	Command Code	Current Protocol	CRC

7.3 Set the frequency hopping table, antenna dwell time, and duty cycle(0x95)

Command Description

This Command could set the module’ s hopping table.

This command can set the antenna dwell time for the module.
This value limits the maximum operating time for each antenna.
The antenna switching logic: If no more tags are inventoried or the dwell time is reached, the module will switch to the next antenna for reading.

This command can set the duty cycle parameters for the module (requires firmware version 20240606 or later).
●After only enable single antenna, the "duty cycle operation mode" is only supported in AA48 mode.。
●After configuring the reference time and full load working time, you need to configure BIT0~BIT3 in the high byte of Search Flags of AA48 to enable the "duty cycle working mode".

Command Features

Command Code	**Bootloader Command**	**App Firmware Command**	**Data Field**
0x95	invalid	valid	There’ s sending commands, but there’ s not received commands.

Send Command in Data Field Format

When setting the frequency hopping table, the command is sent with the Data field, which contains the following fields:

Field	Byte Length	Description
frequencies	N*4	N frequencies (within the operating region band), each frequency occupies 4 bytes. The maximum number of frequencies (N) is 50. Only frequencies within the "current region band" can be set; refer to Appendix 2 for the frequency hopping table. After using the 0x97 command, the working frequency hopping table will be restored to the default, which includes all frequency points in the current region band. Only standard modules for China support frequency setting; versions for other regions are not supported.

When setting the frequency hopping time or antenna dwell time, the command is sent with the Data field, which contains the following fields:

Field	Byte Length	Description
Option	1	0x01 is the frequency hopping time, which is meaningless. 0x02 is the antenna dwell time (if it is 0, the default is 4 seconds).
Timeout	4	The unit is ms, and the value range is 20-60000, which means the maximum value is one minute.

When setting the duty cycle parameters, the command is sent with the Data field, which contains the following fields:

Field	Byte Length	Description
Option	1	It has to be 0x11
Time1	2	Full-load working time before entering duty cycle mode, in milliseconds (ms). If the value is less than 50ms, it will be treated as 0ms.
Time2	2	Duty cycle reference time, the working cycle of duty cycle mode, in milliseconds (ms). For example, inventory for 600ms and stop for 400ms per second. 600 + 400 = 0x03E8. If the value is less than 50ms, it will be treated as 1000ms.

Send Command (Set the frequency hopping table and configure two frequencies：903250kHz 和 926750kHz)：

FF	08	95	00 0D C8 52	00 0E 24 1E	F8A5
Header	Data Length	Command Code	903250kHz	926750kHz	CRC

Send Command (Set the antenna dwell time to 5 seconds)：

FF	05	95	02	00001388	D5AB
Header	Data Length	Command Code	Option	Timeout	CRC

Send Command (Set the duty cycle parameters to 5 seconds on and 1 second off.)：

FF	05	95	11	1388	03E8	9958
Header	Data Length	Command Code	Option	Time1	Time2	CRC

7.4 Set GPOGPO(0x96)

Command Description

This command has two formats for setting gpo and getting gpo status. Different reader types have different number of gpio. This series of modules supports 2 output.

Command Features

Command Code	Bootloader Command	App Firmware Command	Data Field
0x96	Invalid	valid	When used to set the function, there' s sending commands, and there' s not receiving commands. When used to obtain the function, there' s not sending commands, and there' s receiving commands.

Send Command in Data Field Format

When the 0x96 command is used for setting, the Data field is included when sending the command. At this time, the Data field contains the following fields, as shown in the table:

Field	Byte Length	Description
GPO Number and Status pairs	N*2	N GPO number and state pairs, each pair is 2 bytes (the first byte is the GPO number, the second byte is the state)

Received Command in Data Format

When the 0x96 command is used for acquisition, it has a Data field when receiving the command. At this time, the Data field contains the following fields:

Field	Byte Length	Description
Status of GPO pins	N	Returns the status of all GPO in numerical order. Each pin state is a byte, 0 is low level, 1 is high level.

Command Examples:

Example 1: Set GPO

Send Command:

FF	04	96	01	01	02	00	2F 68
Header	Data Length	Command Code	Output #1	Status of Output #1	Output #2	Status of Output #2	CRC

Example 2: Get last time GPO status

Received Command:

FF	02	96	00 00	01	00	28E1
Header	Data Length	Command Code	Status Code	Status of Output #1	Status of Output #2	CRC

7.5 Set the Current Working Area(0x97)

Command Description

Each country has its legal work area

Command Features

Command Code	Bootloader Command	App Firmware Command	Data Field
0x97	invalid	valid	There' s sending commands, but there' s not receiving commands.

Send Command in Data Field Format

Set the working area (0x97) with the Data field when sending the command. At this time, the Data field contains the following fields, as shown in the table:

Field	Byte Length	Description
Region Code	1	refer to appendix 2

Notes:

●When using the 0x95 command to set the frequency, you can only set the frequency in the frequency hopping table corresponding to the frequency band area in which the module is currently set to work.

●After the setting is completed, the working frequency hopping table will be restored to the default, that is, all the frequencies in the current frequency band area.

Command Examples:

Example 1: Set the working area to North America.

Send Command:

FF	01	97	01	4B BC
Header	Data Length	Command Code	Region Code	CRC

Received Command:

FF	00	97	00 00	77 9E
Header	Data Length	Command Code	Status	CRC

Example 2: Set working area to China 1 frequency band.

Sending Commands:

FF	01	97	06	4B BB
Header	Data Length	Command Code	Region Code	CRC

Received Command:

FF	00	97	00 00	77 9E
Header	Data Length	Command Code	Status	CRC

7.6 Set Standby Low Power Mode(0x98)

Command Description

This command is used to set the standby low power strategy (requires firmware version 202405023 or later).
Each time the RF circuit is activated, it consumes a certain amount of time. Therefore, if power consumption is not a critical concern, it is not recommended to enable this feature.
This mode is suitable for scenarios where there are strict requirements for standby power consumption or temperature, but no strict timing constraints on module wake-up.
After enable this functions:
After completing an inventory or operation command, the module will shut down the RF hardware circuit (takes about 50 ms).
When the RF hardware circuit is turned off, sending an inventory or operation command will require restarting the RF hardware circuit.
Under normal conditions, restarting the RF hardware circuit takes about 30 ms, but in abnormal cases, it may take up to 150 ms.
After the previous inventory or operation command returns, if the next command is sent immediately, it will take approximately 80–200 ms to restart the RF hardware circuit.
Commands such as carrier modulation AA31, AA4B, AA54 can only be executed when Power mode is set to 0 or 1.

Command Features

Command Code	Bootloader Command	App Firmware Command	Data field
0x98	invalid	valid	There' s sending commands, but didn' t received commands.

Send Command in Data Field Format

Set work area (0x98) Send commands with a Data field that contains the following

fields, as shown in the table:

Field	Byte Length	Description
Power Mode	1	0、1=regular low power consumption mode 2、3=the lowest power consumption mode.

Command Example：

Example 1： Set as the lowest power consumption mode.

Send Command：

FF	01	98	03	44 BE
Header	Data Length	Command Code	Power Mode	CRC

Received Commands：

FF	00	98	00 00	86 71
Header	Data Length	Command Code	Status Code	CRC

7.7 Set Unique Configuration Parameters (0x9A)

Command Description

This command is used to set the module's unique configuration option.

Command Features

Command Code	Bootloader Command	App Firmware Command	Data Field
0x9A	invalid	valid	There’ s sending commands, but didn’ t received commands.

Send Command in Data Field Format

0x9A command, sent this with a Data field, in which case the Data field contains the following fields, as below table：

Field	Byte Length	Description
Option	1	Must be 0x01
Key	1	For a detailed description of the value of the settings items, see below, Key Value Description Table.

Field	Byte Length	Description
Value	1	For a detailed description of the value of the settings items, see below, Key Value Description Table.

Key Value Description Table

Key	Value	Description
0x00: Use the antenna port number as one of the unique identifiers for the tag buffer entry.	0x00	The antenna port is one of the unique identifiers for the tag buffer entry.For the same EPCID tag, if detected by different antennas, multiple entries will be generated (default value after power-on).
	0x01	The antenna port is not one of the unique identifiers for the tag buffer entry.For the same EPCID tag, if detected by different antennas, only one entry will be generated, recording only the latest antenna port.
0x06: Record the maximum RSSI seen	0x00	For the same EPCID tag, if detected multiple times, only the latest RSSI value will be recorded (default value after power-on).
	0x01	For the same EPCID tag, if detected multiple times, the maximum observed RSSI value will be recorded.
0x08: append the data as one of the unique identifiers of the tag buffer entry	0x00	The additional data is one of the unique identifiers for the tag buffer entry.If tags with the same EPCID but different additional data are detected, multiple entries will be generated (entries with empty additional data will also be considered separate entries).
	0x01	The additional data is not one of the unique identifiers for the tag buffer entry.If tags with the same EPCID but different additional data are detected, only one entry will be generated, recording only the latest additional data (default value after power-on).

Command Examples：Set the antenna ports to be one of the unique identifiers for the tag buffer entry.

Send Command：

FF	03	9A	01	00	01	AF 5C
Header	Data Length	Command Code	Option	Key	Value	CRC

Received Command：

FF	00	9A	00 00	A6 33
Header	Data Length	Command Code	Status Code	CRC

7.8 Set Protocol Comfigration Parameters (0x9B)

Command description: This command is used to set protocol-specific set parameters.

Command Features

Command Code	Bootloader Command	App Firmware Command	Data Field
0x9B	invalid	valid	There’ s send commands, but there’ s not received commands.

Send Command in Data Field Format

Set Tag Protocol Configuration (0x9B), the command includes the Data field, which contains the following fields:

Field	Byte Length	Description
Protocol Value	1	Must be 0x05. Now all modules only support Gen2 protocol.

Field	Byte Length	Description
Parameter	1	Protocol parameters.
Option	0/1	An option of parameter. For some parameters, this field is not available.
Value	0/1	Settings’ value. For some parameters, this field is not available.

Protocol Parameters Tables

Parameter	Option	Value
0x00: Session	there’ s not this field	0x00~0x03: Session 0~3(default 0)
0x01: Target	0x01: static Target	0x00: Target A (default value)
		0x01: Target B
	0x00：dynamic Target。	0x00: A-B. Start from A and store until the label is not found, then switch to B.
		0x01: B-A. Start from B and store until the label is not found, then switch to A.
0x02: RFMODE	there’ s not this field	Send value as shown in the figure below. (default ID=7)
0x12: Q value	0x00: Dynamic Q (dynamically adjusts Q based on inventory status, default value)	No such field
	0x01: Static Q value	0x00~0x0F(1 Byte，Q value)

Notes:

- Dynamic Q and Dynamic Target apply only to 22 and AA48.

- Only one row (one RF MODE) can be set at a time; individual parameters (e.g., Tari) cannot be configured.
- The table below shows the mapping between old and new mode IDs. The values in red indicate the command values used for RF MODE configuration.
- If the current chip does not support the specified RF MODE (e.g., E310 set to New MODE ID=103), it will still return status code 0000, but will actually revert to the default RF MODE 7. It is recommended to use command 6B again to confirm the current RF MODE.

Command send value (HEX)	Command send value (DEC)	Mode ID	E710 Chip Sensitivity Spec (dBm)	Typical Optimized Read Rate (tags/s)	Forward Link Modulation	Tari (µs)	PIE	BLF (kHz)	Reverse Link Modulation	Supported SKUs		
CB	203	103	-78	1,000+	DSB	6.25	1.5	640	FM0	E710		
6F	111	11	-78	800+	PR	7.5	2	640	FM0			
DC	220	120	-81	700+	DSB	6.25	1.5	640	M=2		E510	
65	101	1	-81	550+	PR	7.5	2	640	M=2			
2D	45	345	-84	400+	PR	7.5	1.5	640	M=4			
73	115	15	-84	400+	PR	7.5	2	640	M=4			
70	112	12	-84	300+	PR	15	2	320	M=2			E310
67	103	3	-84	250+	PR	20	2	320	M=2			
69	105	5	-87	200+	PR	20	2	320	M=4			
6B	107	7	-88	150+	PR	20	2	250	M=4			
71	113	13	-93	50+	PR	20	2	160	M=8			

Example 1: Set Session 1, send command:

FF	03	9B	05	00	01	DCE9
Header	Data Length	Command Code	Protocol Value	Parameter	Value	CRC

Example 2: Set Target B, send command:

FF	04	9B	05	01	01	01	A2FC
Header	Data Length	Command Code	Protocol Value	Parameter	Option	Value	CRC

Example 3: Set old RF MODE ID to 11, send command:

FF	03	9B	05	02	6F	DE87
Header	Data Length	Command Code	Protocol Value	Parameter	Value	CRC

Example 4: Set static Q value to 3, send command:

FF	04	9B	05	12	01	03	80AC
Header	Data Length	Command Code	Protocol Value	Parameter	Option	Value	CRC

8 Get Commands

The get commands listed in the following table are used to get parameters, options and working status from the module. The get commands follow the general command communication protocol format.

Get commands overview

Commands	Command Code	Description
Get antenna port configuration	0x61	Get the configuration of the antenna port (the antenna for tag access operations, the antenna used for inventory, and the transmit power of the antenna port, etc.)
Get read power transmission information	0x62	Get the default power and power range
Get the current tag protocol	0x63	Get the current tag operation protocol
Get frequency hopping settings	0x65	Get the frequency hopping table and regulatory frequency hopping time
Get GPI	0x66	Get the status of the GPI PIN

Commands	Command Code	Description
Get the current working range	0x67	Get the current module working area
Get available working range	0x71	Get module support work area
Get module configuration	0x6A	Get the module configuration
Get tag protocol configuration	0x6B	Get tag protocol configuration
Get the current temperature	0x72	Get the current temperature of the module

8.1 Get antenna port configuration (0x61)

Command description

This command returns the antenna configuration of the module, including which antennas are used for transmission and reception, the transmit power of the antenna port, etc.

Command attributes

Command Code	Bootloader command	App Firmware command	Datafield
0x61	NO	YES	Send command Yes, receive command Yes

Sending command Data field format

Get antenna port configuration (0x61). The command is sent with the Data field.

The Data field contains the following fields:

Field	Byte length	Description
Option	1	See the table below for detailed instructions

Option value	Description
0x00	Returns the antenna for tag access operations (the antenna with the smallest logical number, among enabled antennas). Not commonly used, it is recommended to use Option=2.

Option value	Description
0x02	If the enabled antenna has been configured using command 91, the enabled antenna will be returned. If the enabled antenna has not been configured using command 91, the default enabled antenna will be returned. Among them, the default enabled antenna of the module is antenna 1. This value can be modified using permanent save.
0x03	Get the read and write transmit power of all logical antenna ports.
0x04	Get the read and write transmit power and antenna setup time for all logical antenna ports.
0x05	For multi-port modules, obtain the connection status of all logical antenna ports. The module uses the switch level status to determine whether there is an antenna connection, and can only determine the closed-loop antenna. Single-port modules do not support this function.

Receive command Data format

Get Antenna Port Configuration (0x61) The receiving command contains the Data field. The Data field varies according to the Option value, as shown in the table：

Option value	Byte length	description
00	2	1 pair of antenna configuration information. The first byte is the TX Logical Antenna Number, and the second byte is the RX Logical Antenna Number.
02	2*N	N pairs of antenna configuration information.

Option value	**Byte length**	**description**
03	5*N	N pairs of antenna power information, the antenna power information is composed in the following order: 1 byte Logical Antenna, 2 bytes Read Power, 2 bytes Write Power
04	7*N	N pairs of antenna power time information, the antenna power time information is composed in the following order: 1 byte Logical Antenna, 2 bytes Read Power, 2 bytes Write Power, 2 bytes Setting Time. Note: Time has no actual meaning.
05	2*N	N pairs of antenna connection status information. The antenna connection status information is composed in the following order: 1 byte Logical Antenna, 1 byte connection status, 1 for connection status and 0 for disconnected status.

Command example：

Example 1: Get the antenna of the tag access operation.

Send command：

FF	01	61	00	BD BD
Header	Data Length	Command Code	Option	CRC

Receive command：

FF	02	61	00 00	03	03	4C 20
Header	Data Length	Command Code	Status Code	TX Logical Antenna Number	RX Logical Antenna Number	CRC

Example 2: Get the antenna used in the inventory

Impinj RFID Series Protocol Document

Send command:

FF	01	61	02	BD BF
Header	Data Length	Command Code	Option	CRC

Receive command:

FF	05	61	0000	02	03	03	04	04	7439
Header	Data Length	Command Code	Status Code	Option	TX Logical Antenna Number	RX Logical Antenna Number	TX Logical Antenna Number	RX Logical Antenna Number	CRC

Example 3: Get the read and write transmit power of all antenna ports, assuming it is 30dBm

Send command:

FF	01	61	03	BD BE
Header	Data Length	Command Code	Option	CRC

Receive command:

FF	15	61	0000	03	01	0BB8	0BB8	02	0BB8	0BB8
Header	Data Length	Command Code	Status Code	Option	TX Logical Antenna Number	Read Power	Write Power	TX Logical Antenna Number	Read Power	Write Power

03	0BB8	0BB8	04	0BB8	0BB8	F76F
TX Logical Antenna Number	Read Power	Write Power	TX Logical Antenna Number	Read Power	Write Power	CRC

Example 4: Get the read/write transmit power and setup time of all antenna ports, assuming 30dBm

Send command:

FF	01	61	04	BD B9
Header	Data Length	Command Code	Option	CRC

Receive command:

FF	1D	61	0000	04	01	0BB8	0BB8	01F4	02	0BB8	0BB8	01F4	03	0BB8	0BB8	01F4	04	0BB8	0BB8	01F4	2527
Header	Data Length	Command Code	Status Code	Option	TX Logical Antenna Number	Read Power	Write Power	Setting Time	TX Logical Antenna Number	Read Power	Write Power	Setting Time	TX Logical Antenna Number	Read Power	Write Power	Setting Time	TX Logical Antenna Number	Read Power	Write Power	Setting Time	CRC

Example 5: Get the connection status of all logical antenna ports

Send command:

FF	01	61	05	BD B8
Header	Data Length	Command Code	Option	CRC

Receive command(Only antenna 4 and 8 are connected):

FF 11 61 00 00 05 01 00 02 00 03 00 04 01 05 00 06 00 07 00 08 01 9C E2

8.2 Get transmit power information (0x62)

Command description

Get the module's default transmit power, maximum transmit power, and minimum transmit power when powered on.

Command attributes

Command Code	Bootloader command	App Firmware command	Data field
0x62	NO	YES	Send command YES, Receive command YES

Send command Data field format

Get read transmit power information (0x62). This command is sent with a Data field, which includes the following fields, as shown in the table:

Field	Byte length	Description
Option	1	0 returns the default transmit power at power on. 1 returns the default transmit power at power on, maximum transmit power, minimum transmit power.

Receive command Data field format

Get the read transmit power information (0x62). This command is received with the Data field, which includes the following fields, as shown in the table:

Field	Byte length	Description
Option	1	Same as Send command。
Read TX power	2	The default transmit power is read after power on. The unit is dBm. This value is not recommended. To obtain the current actual transmit power value, refer to the 0x61 command.
Max TX power	0/2	When Option is 1, it exists and indicates the maximum transmit power of the module, in units of 0.01dBm.
Min TX power	0/2	When Option is 1, it exists and indicates the minimum transmit power of the module, in units of 0.01dBm.

Command example：

Send command：

FF	01	62	01	BE BC
Header	Data Length	Command Code	Option	CRC

Receive command：

FF	07	62	00 00	01	0C E4
Header	Data Length	Command Code	Status Code	Option	Read TX power
0C E4	00 00	06 EF			
Max TX power	Min TX power	CRC			

8.3 Get the current tag protocol(0x63)

Command Description

Get the tag protocol during the operation. All Impinj E series modules only support the GEN2 (18000-6C) protocol. When the module is powered on, the GEN2 (18000-6C) protocol is used by default, so you do not need to use this command.

Command attributes

Command Code	Bootloader command	App Firmware command	Data field
0x63	NO	YES	Send command NO, Receive command YES

Receive command Data Field Format

Get the current protocol (0x63). When receiving this command, it contains the Data field, which includes the following fields, as shown in the table.:

Field	Byte length	Description
Current Protocol	2	All modules only support GEN2 (18000-6C) protocol, this field must be 0x0005.

8.4 Get frequency hopping table/antenna dwell time/duty cycle(0x65)

Command Description

This command is used to obtain the frequency hopping table/antenna dwell time/duty cycle. This command has two formats.

Command attributes

Command Code	Bootloader command	App Firmware command	Data field
0x65	NO	YES	None when sending a command to obtain the frequency hopping table. Yes when sending a command to obtain the frequency hopping time, antenna dwell time or duty cycle. Yes when receiving command.

Send command Data Field Format

The 0x65 command is sent to obtain the frequency hopping time or antenna dwell time with the Data field, which includes the following fields：

Field	Byte length	Description
Option	1	0x01 is frequency hopping time, this value is meaningless. 0x02 is the antenna dwell time (if it is 0, the default is 4 seconds). 0x11 is the duty cycle parameter.

There is no Data field when the 0x65 command is sent to obtain the frequency hopping table.

Receive command Data Field Format

When the 0x65 instruction obtains the frequency hopping table, the command is received with the Data field. At this time, the Data field contains the following fields：

Field	Byte length	Description
frequencies	4*M	M frequencies, each frequency is 4 Bytes long.

0x65 command frequency hopping time or antenna dwell time or duty cycle, the command is received with the Data field：

Field	Byte length	Description
Option	1	Same as the send command Option
Hop time	4	Refer to 0x95 setting command

Command example：

Send command(Get frequency hopping table)**：**

FF	00	65	1D 6A
Header	Data Length	Command Code	CRC

Receive command：

FF	0C	65	00 00	00 0D F9 26	00 0D C8 52	00 0E 24 1E	2C B5
Header	Data Length	Command Code	Status Code	915250 kHz	903250 kHz	926750 kHz	CRC

Send command(Get antenna dwell time)：FF 01 65 02 B9 BF

Receive command (need 6 second to get)：FF 05 65 00 00 02 00 00 17 70 04 DC

Send command(Get duty cycle parameters)：FF 01 65 11 B9 AC

Receive command(The results are five seconds and one second.)：FF 05 65 00 00

11 13 88 03 E8 4C D7

8.5 Get GPI(0x66)

Command Description

This command gets the status of all GPI pins of the module.

Command attributes

Command Code	Bootloader command	App Firmware command	Data field
0x66	NO	YES	Send command NO, Receive command YES

Receive command Data Field Format

Get GPI (0x66) receive command with Data field, at this time the Data field contains the following fields, as shown in the table:

Field	Byte length	Description
Status of GPI pins	N	The status of all GPI pins of the module are arranged in numerical order. Each GPI pin occupies one byte. This series of modules has a total of 2 input GPIO ports.

Command example:

Send command:

FF	00	66	1D 69
Header	Data Length	Command Code	CRC

Receive command: Assume input GPIO #1 is 0 and GPIO #2 is 1

FF	02	66	00 00	00	01	CAB2
Header	Data Length	Command Code	Status Code	Input #1	Input #2	CRC

8.6 Get the work area code(0x67)

Command Description

Get the current working area code.

Command attributes

Command Code	Bootloader command	App Firmware command	Data field
0x67	NO	YES	Send command NO, Receive command YES

Receive commandDataField Format

Get the current working area (0x67) , receive command with Data field, which contains the following fields:

field	Byte length	Description
Region Code	1	Refer to Appendix 2

Command example：

Send command：

FF	00	67	1D 68
Header	Data Length	Command Code	CRC

Receive command：

FF	01	67	00 00	01	B480
Header	Data Length	Command Code	Status Code	Region Code	CRC

8.7 Get low power consumption in standby(0x68)

Command Description

This command is used to obtain the standby low power consumption strategy configuration.

Command attributes

Command Code	Bootloader command	App Firmware command	Data field
0x68	NO	YES	Send command NO, Receive command YES

Receive command Data Field Format

Get the current working area (0x67), the Receive command has a Data field, which contains the following fields:

Field	Byte length	Description
Power Mode	1	0, 1 = normal low power mode; 2, 3 = lowest power mode.

Command example:

Example 1: Set to the lowest power mode

Send command:

FF	00	68	1D67
Header	Data Length	Command Code	CRC

Receive command:

FF	01	68	00 00	03	8671
Header	Data Length	Command Code	Status Code	Power Mode	CRC

8.8 Get unique configuration(0x6A)

Command Description

This command is used to obtain the unique configuration of the module.

Command attributes

Command Code	**Bootloader command**	**App Firmware command**	**Data field**
0x6A	NO	YES	Send command YES， Receive command YES

Send command Data Field Format

Get the module's unique configuration (0x6A), Send command with Data field, including the following fields, as shown in the table：

Field	**Byte length**	**Description**
Option	1	Must be 0x01
Key	1	For detailed configuration information, please refer to the key value Description table.

Receive command Data Field Format

Get the module's unique configuration (0x6A). The Receive command contains the Data field, which includes the following fields, as shown in the table：

Field	**Byte length**	**Description**
Option	1	Must be 0x01
Key	1	Configuration items, please refer to the 9A key value Description table for detailed description
Value	1	The value of the configuration item. For detailed description, please refer to the 9A key value Description table

Command example：

Receive command(Get antenna uniqueness: If a tag is stored by multiple antennas, only one piece of information is generated)**:**

FF	03	6A	00 00	01	00	01	3E45
Header	Data Length	Command Code	Status Code	Option	Key	Value	CRC

8.9 Get protocol configuration parameters(0x6B)

Command Description

This command is used to obtain the configuration parameters of a specific label protocol.

Command attributes

Command Code	**Bootloader command**	**App Firmware command**	**Data field**
0x6B	NO	YES	Send command NO, Receive command YES

Send command Data Field Format

Get tag protocol configuration (0x6B), Send command with Data field, which contains the following fields:

Field	Byte length	Description
Protocol Value	1	Must be 0x05. Currently all modules only support Gen2 protocol.
Parameter	1	Protocol parameters, for detailed description please refer to the protocol parameter option table.

Receive command Data Field Format

Get tag protocol configuration (0x6B), receive command with Data field, the Data field contains the following fields：

Field	Byte length	Description
Protocol Value	1	Must be 0x05. Currently all modules only support Gen2 protocol.
Parameter	1	Protocol parameters. For detailed description, please refer to the protocol parameter option table.
Option	0/1	An option for a parameter. For some parameters, this field is not available. For detailed description, please refer to the protocol parameter option table.

Field	Byte length	Description
Value	0/1	The value of the Option parameter. For some parameters, this field is not available. For detailed description, please refer to the Protocol Parameter Option Table.

Command example：

Get the Session configuration is Session0

Send command：

FF	02	6B	05	00	3A6F
Header	Data Length	Command Code	Protocol Value	Parameter	CRC

Receive command：

FF	03	6B	00 00	05	00	00	0874
Header	Data Length	Command Code	Status Code	Protocol Value	Parameter	Value	CRC

Get Target configuration is TargetA

Send command：

FF	02	6B	05	01	3A6E
Header	Data Length	Command Code	Protocol Value	Parameter	CRC

Receive command：

FF	04	6B	0000	05	01	01	00	2C68
Header	Data Length	Command Code	Status Code	Protocol Value	Para meter	Opt ion	Val ue	CRC

8.10 Get available tag protocols(0x70)

Command Description

This command is used to obtain the supported tag protocols. There is only GEN2, i.e. 18000-6C protocol. When the module is powered on, the GEN2 (18000-6C) protocol is used by default, so you do not need to use this command.

Command attributes

Command Code	Bootloader command	App Firmware command	Data field
0x70	NO	YES	Send command NO, Receive command YES

Receive command Data Field Format

The 0x70 command is received with a Data field. The Data field contains the following fields, as shown in the table.:

Field	Byte length	Description
Current Protocol	2	All modules only support the GEN2 (18000-6C) protocol, and this field must be 0x0005.

8.11 Get the available frequency regions(0x71)

Command Description

This command is used to obtain the supported working frequency table.

The Chinese version module has four frequency tables available: North American band, Chinese band, CE_LOW, and full band;

Others can only use the frequency band of the corresponding region.

Command attributes

Command Code	Bootloader command	App Firmware command	Data field
0x71	NO	YES	Send command NO, Receive command YES

Receive command Data Field Format

(0x71) instruction, Receive command with Data field, at this time the Data field contains the following fields, as shown in the table：

Field	Byte length	Description
Regions	1*N	Available region codes

Command example：

Send command:

FF	00	71	1D 7E
Header	Data Length	Command Code	CRC

Receive command:

FF	04	71	00 00	01	06	08	FF	DB40
Header	Data Length	Command Code	Status Code	NA	CN	Eu	Full Frequency	CRC

8.12 Get module temperature(0x72)

Command Description

The maximum operating temperature supported by the module is about 90°C.

When the temperature exceeds this value, the module will report an error.

Command attributes

Command Code	Bootloader command	App Firmware command	Data field
0x72	NO	YES	Send command NO, Receive command YES

Receive command Data Field Format

Get module temperature (0x72), Receive command with Data field, the Data field contains the following fields, as shown in the table:

Field	Byte length	Description
Temperature	1	Temperature value, 1 byte, signed number.

Note:

- SIMX600 series modules do not have temperature detection function; such as SIM7600, SIM5600, etc.

Command example：

Send command：

FF	00	72	1D 7D
Header	Data Length	Command Code	CRC

Receive command： Get temperature is 39℃

FF	01	72	0000	27	4820
Header	Data Length	Command Code	Status Code	Temperature	CRC

9 Command for permanently saving configuration parameters(0xAA40)

Unlike ordinary setting commands, this type of configuration command for modifying power-on default values can achieve permanent storage.

Permanent storage configuration commands follow the extended command communication protocol format.

Command attributes

SubCommand Code	Bootloader command	App Firmware command	Subcommand Data
0xAA40	NO	YES	Send command YES, Receive command YES

Send command SubData field format

0xAA40Send command is with SubData field，At this time, the SubData field contains the following fields, as shown in the table：

Field	Byte length	Description
KEY	1	Indicates which parameters to obtain or configure
GETORSET	1	0 means get function, 1 means set function
KEYDATA	N	Parameter content, the length and composition of KEYDATA are determined by KEY.

9.1 The working antenna and power are enabled by default at power-on

9.1.1 Get the default working antenna and power enabled at power-on

Send command SubData field format

field	Byte length	Description
KEY	1	0x91
GETORSET	1	0x00
KEYDATA	0	There is no such field

Receive command SubData field format

Field	Byte length	Description
KEY	1	0x91
GETORSET	1	0x00
KEYDATA	1/(4+7*N)	If 1 byte 0x5A is returned, it means that the working antenna and power have not been configured, and the default is used.

Field	Byte length	Description
		If 4+7*N (N is the number of antenna ports of the module) is returned, 4 bytes of Antusenum, BIT0 represents antenna 1, and BIT31 represents antenna 32. If the bit corresponding to the antenna is set to 1, it means that the antenna is enabled, and if it is set to 0, it means that the antenna is not enabled. 7 bytes of antenna information: 1 byte antenna logical ID; 2 bytes read power, unit 0.01dBm; 2 bytes write power, unit 0.01dBm; 2 bytes Setting Time is invalid. If all are FFFFFFFFFFFF, it means that the logical antenna has not been configured with power.

9.1.2 Set the default working antenna and power at power-on

Send command SubData field format

Field	Byte length	Description
KEY	1	0x91
GETORSET	1	0x01
KEYDATA	1/N	When restoring the factory default value, KEYDATA=0x5A. When setting the specified value, KEYDATA is the part of the 91 command except "FF and CRC". That is, KEYDATA includes the Data Length field, the Command Code field,

Field	Byte length	Description
		and the Data field. The DataField Format refers to the 0x91 command Send commandData format. (Note that only the format when Option=2 or Option=4 is supported).

Receive command SubData field format

Field	Byte length	Description
KEY	1	0x91
GETORSET	1	0x01
KEYDATA	0	There is no such field

Command example：

Configure the power of antennas 1, 2, 3, and 4 to 3300 each

Send command：

FF	2F	AA	4D 6F 64 75 6C 65 74 65 63 68	AA 40	91	01

Header	Data Length	Command Code	Sub command Marker (Moduletech)	Sub command Code	KEY	GETORSET

1D 91 04 01 0C E4 0C E4 00 00 02 0C E4 0C E4 00 00 03 0C E4 0C E4 00 00 04 0C E4 0C E4 00 00	B8	BB	CEFB
KEYDATA	SubCRC	Terminator	CRC

Receive command:

FF	0E	AA	0000	4D 6F 64 75 6C 65 74 65 63 68	AA 40	91	01	545F
Header	Data Length	Command Code	Status Code	Subcommand Marker (Moduletech)	Subcommand Code	KEY	GETORSET	CRC

9.2 Default working frequency and frequency hopping time at power-on

9.2.1 Get the default working frequency at power-on

Send command SubData field format

Field	Byte length	Description
KEY	1	0x95
GETORSET	1	0x00
KEYDATA	0/1	Get the working frequency, there is no this field; when getting the frequency hopping time, 1 byte, 0x01.

Receive command SubData field format

Field	Byte length	Description
KEY	1	0x95
GETORSET	1	0x00
KEYDATA	1/4*N/5	If 1 byte 0x5A is returned, it means that the default value has not been configured. When obtaining the working frequency, it is N*4 bytes, N is the number of frequencies set to work, each frequency is 4 bytes, the high byte is in front, the unit is kHz; When obtaining the frequency hopping time, it is 0x01+HOPTIME, HOPTIME is the 4-byte frequency hopping time, the unit is milliseconds.

9.2.2 Set the default working frequency at power on

Send command SubData field format

Field	Byte length	Description
KEY	1	0x95
GETORSET	1	0x01
KEYDATA	1/N	When restoring the factory default value, KEYDATA=0x5A. When setting the specified value, KEYDATA is the part of the 95 instruction except "FF and CRC". That is, KEYDATA includes the Data Length field, Command Code field and Data field of the 0x95 instruction frame. The DataField Format refers to the Send commandData format of the 95 instruction (note that when setting the frequency hopping time, the frequency hopping time setting range is 20ms~4000ms, and this setting value is invalid).

Receive command SubData field format

Field	Byte length	Description
KEY	1	0x95
GETORSET	1	0x01
KEYDATA	0	There is no such field

Notes:

●This command can only be used for the Chinese version module

●If the frequency band in which the module works has been set, you can only set part of the frequency or all of the frequencies in the frequency band to work. The frequency hopping table is shown in Appendix 2. If the working frequency band is set using the 0x97 command, all default frequencies will be selected.

●After using this command to set, the current frequency will be used immediately, and the set frequency will be used by default after each subsequent power-on.

When using this command to restore to factory default:

If the default working frequency band is modified, the current power-on default working frequency band saved will be used immediately;

If the power-on default working frequency band has not been configured, the current module will work according to the factory default power-on frequency band; and the device will be restored to factory default after powering on.

●The default power-on working frequency area must have been set before this command can be used to set the frequency, that is, the default power-on working frequency area must be set using the 0x97 command that saves the configuration before it can be set.

9.3 Default working frequency region at power-on

9.3.1 Get the default working frequency region when powering on

Send command SubData field format

Field	**Byte length**	**Description**
KEY	1	0x97
GETORSET	1	0x00
KEYDATA	0	There is no such field

Receive command SubDatafield format

Field	**Byte length**	**Description**
KEY	1	0x97
GETORSET	1	0x00
KEYDATA	1	1 byte, working frequency region code. If 0x5A is returned, it means that it has not been configured and the default is used.

9.3.2 Set the default working frequency region at power-on

Send command SubData field format

Field	Byte length	Description
KEY	1	0x97
GETORSET	1	0x01
KEYDATA	1	1 byte, working frequency region code. When restoring to factory defaults, KEYDATA = 0x5A.

Receive command SubDatafield format

域	Byte length	Description
KEY	1	0x97
GETORSET	1	0x01
KEYDATA	0	No such field

Note:

●This command can only be used for the Chinese version of the module

●The factory default working frequency band of the Chinese module is North America, and the modules in other regions are the frequency bands of the corresponding regions.

●After using this command to set, the module will immediately use the set frequency band to work, and will use the set frequency band by default every time it is powered on again. If it has not been configured or restored to the factory default, it will work according to the original default of the module.

9.4 Default is unique when powering on

9.4.1 Get the default unique value when power on

Send command SubDatafield format

Field	Byte length	Description
KEY	1	0x9A
GETORSET	1	0x00
KEYDATA	2	1 byte OPTION, 1 byte KEY, please refer to 9A

Receive command SubData field format

Field	Byte length	Description
KEY	1	0x9A
GETORSET	1	0x00
KEYDATA	1/3	1 byte OPTION, 1 byte KEY, 1 byte VALUE, refer to 9A. If 1 byte 0x5A is returned, it means that the default value is used without configuration.

9.4.2 Set the default unique setting at power on

Send command SubDatafield format

Field	Byte length	Description
KEY	1	0x9A
GETORSET	1	0x01
KEYDATA	1/3	1 byte OPTION, 1 byte KEY, 1 byte VALUE. Please see 9A for the corresponding relationship (OPTION can only be 0x01). When restoring the factory default value, KEYDATA=0x5A.

Receive command SubData field format

Field	Byte length	Description
KEY	1	0x9A
GETORSET	1	0x01
KEYDATA	0	No such field

9.5 Default protocol at power on

9.5.1 Get default protocol at power on

Send command SubData field format

Field	Byte length	Description
KEY	1	0x9B
GETORSET	1	0x00
KEYDATA	2	1-byte Protocol Value, 1-byte Parameter. Please refer to Part 9B to set the protocol configuration command.

Receive command SubData field format

Field	Byte length	Description
KEY	1	0x9B
GETORSET	1	0x00
KEYDATA	3/4	Specifically, it depends on which parameter is obtained, which is composed of Protocol Value, Parameter, Option, and Value. For the corresponding relationship, please see part 9B: Set protocol configuration command. If 1 byte 0x5A is returned, it means that it has not been configured and the default is used.

9.5.2 Set the default protocol at power on

Send command SubData field format

Field	Byte length	Description
KEY	1	0x9B
GETORSET	1	0x01
KEYDATA	1/3/4	3 or 4 bytes, depending on the parameter being set, consisting of Protocol Value, Parameter, Option, and Value. Please see 9B for the corresponding relationship. When restoring the factory default value, KEYDATA=0x5A.

Receive command SubData field format

Field	Byte length	Description
KEY	1	0x9B
GETORSET	1	0x01

9.6 Whether to run to APP when power on

9.6.1 Get whether to run to APP when powered on

Send command SubData field format

Field	Byte length	Description
KEY	1	0x04
GETORSET	1	0x00

Receive command SubData field format

域	Byte length	Description
KEY	1	0x04
GETORSET	1	0x00
KEYDATA	4	If it is 0xA5A55A5A, it means that after power-on, it will immediately run to the APP layer. If it is other values, after power-on, it will stay in the BOOT layer.

9.6.2 Set whether to run to APP when powered on

Send command SubData field format

Field	Byte length	Description
KEY	1	0x04

Field	Byte length	Description
GETORSET	1	0x01
KEYDATA	4	If it is 0xA5A55A5A, it means that after power-on, it will immediately run to the APP layer. If it is other values, after power-on, it will stay in the BOOT layer.

Receive command SubData field format

Field	Byte length	Description
KEY	1	0x04
GETORSET	1	0x01
KEYDATA	0	No such field

Note:

- After configuring "Power on to APP", if you switch to BOOT layer 09 command during operation, it will immediately return to APP. If you need to stay in the BOOT layer, you need to send AB to prepare for upgrade first, and then send 09
- The factory default of the module is to stay in the BOOT layer after power on.

Command example:

Send command:

FF	14	AA	4D 6F 64 75 6C 65 74 65 63 68	AA 40	04	01	A5 A5 5A 5A	ED	BB	12 39
Header	Data Length	Command Code	Subcommand Marker (Moduletech)	Subcommand Code	KEY	GETORSET	KEYDATA	Sub CRC	Terminator	CRC

Receive command:

FF	0E	AA	00 00	4D 6F 64 75 6C 65 74 65 63 68	AA 40	04	01	C1 5F
Header	Data Length	Command Code	Status Code	Subcommand Marker (Moduletech)	Subcommand Code	KEY	GETORSET	CRC

9.7 Default baud rate at power on

9.7.1 Get the default baud rate at power-on

Send command SubData field format

Field	Byte length	Description
KEY	1	0x06
GETORSET	1	0x00
KEYDATA	0	No such field

Receive command SubData field format

Field	Byte length	Description
KEY	1	0x06
GETORSET	1	0x00
KEYDATA	4	The module defaults to a baud rate value when powered on, which is one of 9600, 19200, 38400, 57600, 115200, 230400, 460800, and 921600.

Command example: Get the current baud rate

Send command:

FF	10	AA	4D 6F 64 75 6C 65 74 65 63 68	AA 40	06	00	F0	BB	A0 51

Header	Data Length	Command Code	Subcommand Marker (Moduletech)	Subcommand Code	KEY	GETORSET	Sub CRC	Terminator	CRC

Receive command:

FF	12	AA	0000	4D 6F 64 75 6C 65 74 65 63 68	AA40	06	00	00 0E 10 00	9C 5F
Header	Data Length	Command Code	Status Code	Subcommand Marker (Moduletech)	Subcommand Code	KEY	GETORSET	KEYDATA	CRC

9.7.2 Set the default baud rate at power on

Send commandSubDatafield format

Field	Byte length	Description
KEY	1	0x06
GETORSET	1	0x01
KEYDATA	4	The module defaults to a baud rate value when powered on, which is one of 9600, 19200, 38400, 57600, 115200, 230400, 460800, and 921600.

Receive command SubData field format

Field	Byte length	Description
KEY	1	0x06
GETORSET	1	0x01

Command example: **Send command:**

FF	14	AA	4D 6F 64 75 6C 65 74 65 63 68	AA 40	06	01	00 0E 10 00	0F	BB	79 9F

Header	Data Length	Command Code	Subcommand Marker (Moduletech)	Subcommand Code	KEY	GETORSET	KEYDATA	Sub CRC	Terminator	CRC

Receive command:

FF	0E	AA	0000	4D 6F 64 75 6C 65 74 65 63 68	AA 40	06	01	C3 5F
Header	Data Length	Command Code	Status Code	Subcommand Marker (Moduletech)	Subcommand Code	KEY	GETORSET	CRC

●When the module is powered on, the serial port will be initialized according to the previously configured and saved baud rate. The factory default is 115200

●After receiving the correct response from the module after using this command setting, the module currently uses the set baud rate to work, and each subsequent power-on will also use the set baud rate to initialize the serial port.

9.8 Restore factory default settings

After using this command to reset the module to save the configuration parameters to the default factory configuration, the factory default configuration is used immediately and the previously configured and saved "permanently saved configuration parameters" are cleared. For specific parameters to be cleared, see Chapter 9 (including baud rate, whether to run to APP when powered on, excluding module hardware version, excluding serial number). The module will work according to the factory default until the module is reconfigured. After the execution is completed (the command is received), it is recommended to power on the module again.

Send command SubData field format

Field	Byte length	Description
KEY	1	0xAA
GETORSET	1	0x01

Receive command SubData field format

Field	Byte length	Description
KEY	1	0xAA

Field	Byte length	Description
GETORSET	1	0x01

Command example：

Send command：

FF	10	AA	4D 6F 64 75 6C 65 74 65 63 68	AA 40	AA	01	95	BB	8D 63
Header	Data Length	Command Code	Subcommand Marker (Moduletech)	Subcommand Code	KEY	GETORSET	Sub CRC	Terminator	CRC

Receive command：

FF	0E	AA	0000	4D 6F 64 75 6C 65 74 65 63 68	AA40	AA	01	6F 5F
Header	Data Length	Command Code	Status Code	Subcommand Marker (Moduletech)	Subcommand Code	KEY	GETORSET	CRC

9.9 Prepare to upgrade the firmware command

This command is for preparing upgrade. Because the "Run to APP at power-on" function may be set, the host computer needs to send this command before each upgrade.

After sending this command, as long as you receive a reply from the module (no need to pay attention to the status code), you can continue to upgrade the module.

Send command SubData field format

Field	Byte length	Description
KEY	1	0xAB
GETORSET	1	0x01

Receive command SubData field format

Field	Byte length	Description
KEY	1	0xAB
GETORSET	1	0x01

Command example:

Send command:

FF	10	AA	4D 6F 64 75 6C 65 74 65 63 68	AA 40	AB	01	96	BB	BD52
Header	Data Length	Command Code	Subcommand Marker (Moduletech)	Subcommand Code	KEY	GETORSET	Sub CRC	Terminator	CRC

Receive command:

FF	0E	AA	00 00	4D 6F 64 75 6C 65 74 65 63 68	AA 40	AB	01	6E 5F
Header	Data Length	Command Code	Status Code	Subcommand Marker (Moduletech)	Subcommand Code	KEY	GETORSET	CRC

10 Other commands

10.1 Standing wave detection(0xAA4A)

command Description

The standing wave check command is used to detect the antenna standing wave value. The smaller the value, the better the antenna matching. It should usually be less than 7. Otherwise, the antenna may not match, or the antenna contact is poor, or the antenna is damaged, or the antenna is not connected.

This command complies withthe extended command communication protocol format.

commands attributes

SubCommand Code	Bootloader commands	App Firmware Commands	SubData
0xAA4A	No	Yes	Send command Yes, receive command Yes

Send command SubData field format

0xAA4A sends a command with the SubData field, which contains the following fields, as shown in the table:

Field	Byte length	Description
data	5+3*N	First Byte: specifies the high Byte of the detection power value; Second Byte: specifies the low Byte of the detection power value, unit 0.01dBm; (Invalid, 20dBm will be used in the module) The third Byte: specifies the logical antenna number; The fourth Byte: specifies the frequency band; the Chinese module can specify four frequency bands: China, North America, CE_LOW, and full frequency band; other regions can only specify the frequency band of the corresponding region; The fifth Byte: specifies the number of frequencies N to be tested, which is divided into two cases: N=0 means all M frequencies in the test frequency band (modules in all regions are available). N>0 means N frequencies in the test frequency band (only Chinese modules can be used). Subsequent Bytes:

Field	Byte length	Description
		3*N Bytes: Each frequency is represented by 3 Bytes, with the high Byte first. If a frequency band is set, only the corresponding frequency in the frequency band can be set;

Receive command SubData field format

0xAA4A receives the command with the SubData field, which contains the following fields, as shown in the table:

Field	Byte length	Description
data	5+4*M Or 5+4*N	First Byte: specifies the high Byte of the detection power value; Second Byte: specifies the low Byte of the detection power value (unit: 0.01dBm, invalid); Third Byte: specifies the logical antenna number; Fourth Byte: specifies the frequency band; the Chinese module can specify four frequency bands: China, North America, CE_LOW, and full frequency band; other regions can only specify the frequency band of the corresponding region; The fifth Byte: specifies the number of frequencies N to be tested. This value cannot exceed the maximum number of frequencies contained in the specified frequency band. Only Chinese modules can specify individual frequencies within the frequency band for testing. The value of modules in other regions must be 0. Subsequent Bytes: N=0 means all M frequencies in the test frequency band, and the field length is 5+4*M Bytes;

Field	Byte length	Description
		N>0 means N frequencies in the test frequency band, and the field length is 5+4*N Bytes; The test result of each frequency consists of 4 Bytes, the upper 3 Bytes are the frequency (kHz), and the lowest Byte is return loss. Return loss value = transmission power value - reflection power value, unit is0.1dB。

Note:

●If this command is in accordance with the FCC standard, it will take about 25 seconds to detect once. Areas with similar FCC standards will take a long time. It is recommended to set the timeout period for waiting for a reply after sending this command to 30 seconds.

Impinj RFID Series Protocol Document

command Examples： Antenna 1 power is 3000, detecting echo values of all frequencies in North America.

Sending commands:

FF	13	AA	4D 6F 64 75 6C 65 74 65 63 68	AA 4A	0B B8 01 01 00
Header	Data Length	Command Code	Subcommand Marker (Moduletech)	Subcommand Code	data

B9	BB	BD 67
SubCRC	Terminator	CRC

Analysis: data = 0BB8 01 01 00: power 3000 (invalid), logical antenna 1, frequency band North America, all frequencies.

Receiving commands:

FF	D9	AA	00 00	4D 6F 64 75 6C 65 74 65 63 68	AA 4A
Header	Data Length	Command Code	Status Code	Subcommand Marker (Moduletech)	Subcommand Code

0BB80101000DF732780DC65E820E26126E0DF926780DC852820E241E6E0DDBDA780E02EA6E0E16726E0DD022820DFB1A6E0DE792780E0EA26E0DEF62780DD40A820DF34A780DDFC2780E06D26E0E1A5A6E0DCC3A820DFF026E0DEB7A780E128A6E0E0ABA6E0DD7F2820DF53E780DE1B6780E08C66E0E1C4E6E0DCE2E820DED6E780DD9E6820E00F66E0E147E6E0DE3AA780E1E426E0DE59E780E0CAE6E0E20366E0DD216820DF156780DDDCE780E04DE6E0E18666E0DCA46820DFD0E780DE986780E10966E0E222A6E0DD5FE82	BD 67
data	CRC

Analysis:

0BB8 01 01 00： Power 3000 (invalid), logical antenna 1, frequency band North America, all frequencies

0DF732 78：

Frequency 0x0DF732=915250kHz

VL=0x78=120.

RL=10 to the power of (VL/10/20)=3.9810.

The standing wave VSWR calculation formula is: VSWR=(RL+1)/(RL-1)=1.67.

Therefore, the standing wave of the first frequency 915250kHz is 1.67.

10.2 Multi-label matching filter (0xAA4C)

command Description

Match filtering supports up to 16 rules, and the maximum length of each rule is 255 bits (Option BIT5=0).

This command complies with extended command communication protocol format.

command attributes

SubCommand Code	Bootloader command	App Firmware command	SubData
0xAA4C	No	Yes	Send command yes, receive command no

Send command SubData field format

0xAA4C sends a command with the SubData field, which contains the following fields, as shown in the table:

Field	Byte length	Description
SELFLAG	2	When the matching filter tag data can be sent with only one command, SELFLAG=0xFFFF; When the matching filter tag data requires two commands to send, the first SELFLAG=0x0000, the second SELFLAG=0x00FF; When the matching filter tag data requires three or more commands to

Field	Byte length	Description
		send, the first SELFLAG=0x0000, the middle SELFLAG=0xFF00; the last SELFLAG=0x00FF;
SELTAGCNT	1	The number of matching filter rules in each command
SELTAGDATAN	N*SELTAGCNT	SELTAGDATAN is the data for each filter tag.

The SELTAGDATAN field contains the following fields, as shown in the table:

Field	Byte length	Description
selLEN	1	The length of the entire SELTAGDATAN field in Bytes
selBANK	1	Filter label BANK, value 1-3， EPC=1; TID=2; USER=3
selADDR	4	Filter bit address;
selbitsLEN	1	Filter bit length;
selDATA	N	Data to be compared with the tag data specified in the bank. Note that N = Select Data Length/8, then rounded up

Note:

●When using the 0x22 command and the 0xAA48 asynchronous inventory command to perform tag inventory, if the lower 3 bits of OPTION are all 1, it means that the multi-tag matching and filtering function is enabled. At this time, only the lower 4 bits of OPTION are valid;

●BIT3=0 means: a tag will be counted as long as it meets any rule.

●BIT3=1 means: a tag will not be counted as long as it meets any rule.

If a tag wants to be inventoried, all banks of the tag must perfectly circumvent (not comply with) every rule.

When BIT3=1 is compared to BIT3=0, for each label, the logic of "whether it can be inventoried" will be reversed.

(If BIT3=0, the tag will be counted, but if BIT3=1, the tag will not be counted, and vice versa)

●If you use multi-label matching filter Option=7, but "multi-label matching filter" has not been set, the execution fails.

●As long as the "Multi-label matching filtering rules" are configured and the module has always been at the APP layer, the rules will be retained and used until new AA4C rules are sent.

Commad example:

Filter rule 1: EPCID starts with E20081818116025310 40AF36
Filter rule 2: EPCID starts with 4298
Filter rule 3: EPCID starts with 112210000000000002001000

Send command:

FF	40	AA	4D 6F 64 75 6C 65 74 65 63 68	AA 4C	FFFF	03
Header	Data Length	Command Code	Subcommand Marker (Moduletech)	Subcommand Code	SELFLAG	SELTAGCNT

13	01	00 00 00 20	60	E2 00 81 81 81 16 02 53 10 40 AF 36
selLEN	selBANK	selADDR	selbitsLEN	selDATA
09	01	00 00 00 20	10	42 98
selLEN	selBANK	selADDR	selbitsLEN	selDATA
13	01	00 00 00 20	60	11 22 10 00 00 00 00 00 02 00 10 00
selLEN	selBANK	selADDR	selbitsLEN	selDATA

8D	BB	4E77
SubCRC	Terminator	CRC

Receiving commands:

FF	0C	AA	00 00	4D 6F 64 75 6C 65 74 65 63 68	AA 4C	0F27
Header	Data Length	Command Code	Status Code	Subcommand Marker (Moduletech)	Subcommand Code	CRC

10.3 Private Yichain Temperature Label(0xAA50)

Commad Description

The special read tag storage bank is shown in Figure 7, which obtains the tag temperature command. This command complies withExtended command communication protocol format.

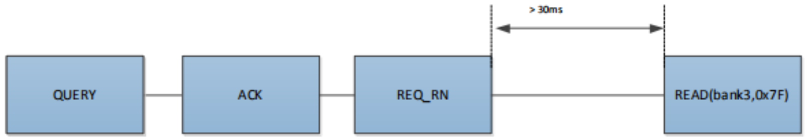


Figure 7

Commad attributes

SubCommand Code	Bootloader command	App Firmware commad	SubData
0xAA50	No	Yes	Send command Yes, receive command Yes

Send command SubData field format

The 0xAA50 command is sent with the SubData field, which contains the following fields, as shown in the table

Field	Byte length	Description
TIMEALL	2	Total command execution time (TIMESELWAIT + TIMEREADWAIT + tag reading time), in milliseconds. The tag reading time is the value defined in the Timeout field.
TIMESELWAIT	2	When using matching filtering, set the waiting time after sending matching filtering data. The unit is milliseconds, the maximum value is 300, and it can be 0 when not used.
TIMEREADWAIT	2	Specifies the time to wait before reading memory contents. The unit is milliseconds, the maximum value is 300, and it can be 0 when not used.

Field	Byte length	Description
Option	1	The meaning is the same as command 0x28.
Metadata Flags	0/2	The meaning is the same as command 0x28.
Read MemBank	1	The meaning is the same as command 0x28.
Read Address	4	The meaning is the same as command 0x28.
Word Count	1	The meaning is the same as command 0x28.
Access Password	0/4	The meaning is the same as command 0x28.
Tag Singulation	0/N	The meaning is the same as command 0x28.

Receive command SubData field format

The private iLian temperature tag (0xAA50) command contains the SubData field when it is received.

Field	Byte length	Description
Option	1	The same as the Option field of the send command.
Metadata Flags	0/2	Same as the Metadata Flags field in the send command.当 This field exists only when BIT4 of Option=1.
Metadata	0/N	The length of the Metadata field is determined by Metadata Flags. This field exists only when BIT4 of Option=1.
Data Read	N	The read tag storage bank data. This field exists only when BIT4 of Option=0.
EPC Length	1	It is the Byte length of PC+EPCID+TagCRC.

Field	Byte length	Description
PC Word	2	The PC field in the EPC bank.
EPCID	N	EPCID
TagCRC	2	TagCRC

Note:

●Temperature tag temperature range determination method (PC)
The current temperature measurement ranges are -30~97 degrees, 0~120 degrees, and -40~120 degrees. Before calculating the temperature, the chip temperature measurement range can be determined by reading the PC value in the EPC bank of the tag. Different temperature measurement ranges use corresponding temperature calculation methods.

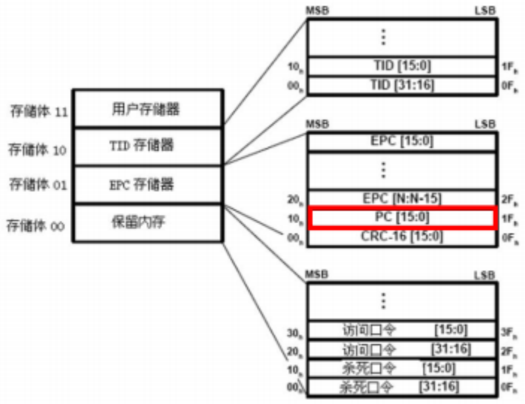


图 6.17 逻辑内存映象

If the PC value ends with 78 (i.e. 0xXX78), it is considered to be a -40~120 degree temperature measurement tag.
If the PC value ends with 00 (i.e. 0xXX00), it is considered to be a -30~97 degree temperature measurement tag.
If the PC value ends with 48 (i.e. 0xXX48), it is considered to be a 0~120 degree temperature measurement tag.
The temperature data is two Bytes [Byte1, Byte2], Byte1 is the integer part and Byte2 is the decimal part.
For -40~120 degree tags, the calculation method after reading the temperature data is: subtract 45 from the integer part and *100/256 from the decimal part.
For -30~97 degree tags, the calculation method after reading the temperature data is as follows: the highest bit of the integer part is the sign bit,
If it is a positive number, "integer minus 30, decimal * 100/256",
If it is a negative number, "invert the integer and subtract 30; invert the decimal and add 1 and then * 100/256".
For 0~120 degree tags, the calculation method after reading the temperature data is: the integer part remains unchanged, and the decimal part*100/256.

Command example: Filter TID, start from address 0, filter data E2008; read Yilian temperature tag.

Send command:

FF	29	AA	4D 6F 64 75 6C 65 74 65 63 68	AA 50	044C	00 00
Header	Data Length	Command Code	Subcommand Marker (Moduletech)	Subcommand Code	TIMEALL	TIMESELWAIT

00 64	12	00 0F	03	0000007F	01
TIMEREADWAIT	Option	Metadata Flags	Read MemBank	Read Address	Word Count

00000000	00000000	14	E20080	C8	BB	6CB6
Access Password	Select Address	Select Data Length	Select Data	Sub CRC	Terminator	CRC

10.4 Private iLian light tag (0xAA51)

Command Description

Light up the LED on the iLian tag. This command complies with the extended command communication protocol format.

Command attributes

SubCommand Code	Bootloader command	App Firmware command	Subcommand Data
0xAA51	No	Yes	Send command Yes, receive command Yes when single tag is on, no when multiple tags are on at the same time

Send command SubData field format

The 0xAA51 command is sent with the SubData field. At this time, the SubData field contains the following fields, as shown in the table:

Field	Byte length	Description
Timeout	2	Refer to the Timeout field description. If BIT7 of Option=1, the high Byte of timeout is the duration of lighting the light, and the low Byte of timeout is the time to remove the inventory tag, in units of 100 milliseconds*. If the Select-Option Bits of Option = 0x07, the low Byte of timeout must be 0xFF*.

Field	Byte length	Description
Option	1	Option field contains the Select-Option Bits control bits.If BIT7=1, the definition of the Timeout field will be changed. If Select-Option Bits=0x07, the function of lighting up multiple tags at the same time is realized.
Metadata Flags	0/2	The meaning is the same as command 0x22.
Tag Singulation	0/N	The meaning is the same as command 0x22.

Receive command SubData field format

iLian tag lights up (0xAA51) command received with SubData field

Field	Byte length	Description
Option	1	The same as the Option field of the send command.
Metadata Flags	0/2	Same as the Metadata Flags field in the send command.当 This field exists only when BIT4 of Option is 1=1.
Metadata	0/N	The length of the Metadata field is determined by Metadata Flags. This field exists only when BIT4 of Option is 1=1.

Field	Byte length	Description
PC Word	2	The PC field in the EPC bank.
EPC ID	N	Tags EPC
Tag CRC	2	Tags CRC

Note:

- ●This command is only available for the Chinese version module.

●When the highest bit in the Option field is 1, it is used to turn on the light.

The high Byte of timeout is the duration of lighting the light, and the low Byte is the time to remove the inventory tag.

For example, FF 11 AA 4D 6F 64 75 6C 65 74 65 63 68 AA 51 40 05 80 C0 BB CC CF

It represents the counting time 0x05=500ms. When the LED tag is counted, the lighting time is 0x40=6400ms.

When this function is used, the return time after a successful command is the sum of the above two times. After the above example succeeds, the maximum return time is about 6.9 seconds.

●When the lower 3 bits of the Option field are all 1, multi-label filtering function is enabled (without password field).

The low Byte of timeout is fixed to FF and cannot be 0. The multi-tag lighting command does not need to count the tags, so this time value is actually invalid. After the command is executed, only operation failure or success will be returned.●

The corresponding BIT and actual effect of the Option domain are shown in the table below. Option=0x87 is more commonly used.

[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	彎湛	璓ケ	孜晒獤	[illegible]	庍袑蒲空	庍袑[illegible]	[illegible]	谿狒
鐿	鐿 を 劝 偶	鐿	鐿 桑 壬 ┐	[illegible]	を	簖ケ	[illegible]	薋笙鄠粇	慌瑮鄠粇晒獤	簖ケ[illegible]	桑	桑
嗉虗婊 沈惫 劝偶 盼嶕		劝偶 学嵃 [illegible] [illegible]		[illegible]	[illegible]	簖ケ[illegible]晼瘿	[illegible]	薋笙鄠粇	慌瑮鄠粇晒獤	簖ケ[illegible]	薕	
				[illegible]	[illegible]	簖ケ[illegible]晼瘿	[illegible]	薋笙鄠粇	慌瑮鄠粇晒獤	簖ケ[illegible]	薕	
				[illegible]	[illegible]	簖ケ[illegible]晼瘿	[illegible]	薋笙鄠粇	慌瑮鄠粇晒獤	簖ケ[illegible]	薕	
				[illegible]	[illegible]	簖ケ[illegible]晼瘿	[illegible]	薋笙鄠粇	慌瑮鄠粇晒獤	簖ケ[illegible]	薕	
鐿		鐿		[illegible]	塀虗婊	鐱晼瘿	墀偛[illegible]	桑壬[illegible]	[illegible]	桑[illegible]	桑	
鐿		鐿		[illegible]	を	簖ケ	鎢[illegible]	孜[illegible]笙鄠粇	孜[illegible]瑮鄠粇	簖ケ[illegible]	桑	
嗉虗婊 沈惫 劝偶 盼嶕	珋 锐 芀	劝偶 学嵃 [illegible] [illegible]		[illegible]	[illegible]	簖ケ[illegible]晼瘿	鎢[illegible]	孜[illegible]笙鄠粇	孜[illegible]瑮鄠粇	簖ケ[illegible]	薕	
				[illegible]	[illegible]	簖ケ[illegible]晼瘿	鎢[illegible]	孜[illegible]笙鄠粇	孜[illegible]瑮鄠粇	簖ケ[illegible]	薕	
				[illegible]	[illegible]	簖ケ[illegible]晼瘿	鎢[illegible]	孜[illegible]笙鄠粇	孜[illegible]瑮鄠粇	簖ケ[illegible]	薕	
				[illegible]	[illegible]	簖ケ[illegible]晼瘿	鎢[illegible]	孜[illegible]笙鄠粇	孜[illegible]瑮鄠粇	簖ケ[illegible]	薕	
鐿		鐿		**[illegible]**	**竱虗娟**	**鍲晹檏**	**[illegible]**	**仔[illegible]**	**仔苫獛**	**丧[illegible]**	**丧**	

Command example: The light lasts for 4 seconds, and multiple tags can be lit at the same time (multi-tag filtering AA4C must be configured first)

Send command:

FF	11	AA	4D 6F 64 75 6C 65 74 65 63 68	AA 51	28FF	87

Header	Data Length	Command Code	Subcommand Marker (Moduletech)	Subcommand Code	Timeout	option

A9	BB	1B E8
SubCRC	Terminator	CRC

Receiving commands:

FF	0C	AA	00 00	4D 6F 64 75 6C 65 74 65 63 68	AA 51	0F 3A
Header	Data Length	Command Code	Status Code	Subcommand Marker (Moduletech)	Subcommand Code	CRC

10.5 Configure antenna and power for carrier modulation (0xAA04)

Command Description

Before sending the carrier modulation signal (AA31), the test antenna and power need to be set.

This command complies with the extended command communication protocol format.

Command attributes

SubCommand Code	**Bootloader command**	**App Firmware command**	**Subcommand Data**
0xAA04	No	Yes	Send command yes, receive command no

Note:

- The power value must be within the range allowed by the certification bank. For example, if the certification bank is FCC, the maximum power can only be 30dBm.
- When sending the AA31 command, the power supply capacity must be guaranteed to be sufficient to transmit the currently configured power.
- The configured antenna port needs to be connected to an antenna or spectrum analyzer. If no antenna is connected, the AA31 command will return an error code.

Send command SubData field format

0xAA04 sends a command with the SubData field, which contains the following fields, as shown in the table:

Field	Byte length	Description
ENGTESTSUBCMD	1	0x0C
ARG0	4	Set the antenna for the test, for example, antenna 2 is 00000002
ARG1	4	Set the power of the test antenna (unit: 0.01dBm)

Command example:

Send command (set test antenna 1 power to 2400):

FF	17	AA	4D 6F 64 75 6C 65 74 65 63 68	AA 04	0C 00000001 00000960
Header	Data Length	Command Code	Subcommand Marker (Moduletech)	Subcommand Code	SubData

24	BB	A4DE
SubCRC	Terminator	CRC

Send command (set test antenna 2 power to 2000):

FF	17	AA	4D 6F 64 75 6C 65 74 65 63 68	AA 04	0C 00000002 000007D0
Header	Data Length	Command Code	Subcommand Marker (Moduletech)	Subcommand Code	SubData

93	BB	79D8

SubCRC	Terminator	CRC

10.6 Configure the frequency of carrier modulation(0xAA27)

Command Description

Before sending the carrier modulation signal (AA31), you need to set the test frequency. The configured frequency needs to be in the "frequency band of the currently configured working bank". This command complies with the extended command communication protocol format.

Command attributes

SubCommand Code	Bootloader command	App Firmware command	Subcommand Data
0xAA27	No	Yes	Send command yes, receive command no

Send command SubData field format

0xAA27 sends a command with a SubData field, which contains the following fields, as shown in the table:

Field	Byte length	Description
RESERVED	4	Reserved, temporarily 00000000
FREQ	4	The unit is kHz. For example, 915250kHz is 000DF732

Send command (set frequency to 915250kHz):

FF	16	AA	4D 6F 64 75 6C 65 74 65 63 68	AA 27	00000000 000DF732

Header	Data Length	Command Code	Subcommand Marker (Moduletech)	Subcommand Code	SubData

07	BB	612F
SubCRC	Terminator	CRC

Receiving command:

FF	0C	AA	00 00	4D 6F 64 75 6C 65 74 65 63 68	AA 27	0F4C
Header	Data Length	Command Code	Status Code	Subcommand Marker (Moduletech)	Subcommand Code	CRC

10.7 Transmit carrier wave and modulation(0xAA31)

Command Description

Check the module's RF performance. This command complies with the extended command communication protocol format.

The carrier wave is used to observe the spectrum characteristics and frequency stability of the pure carrier signal.

Transmitting modulated waves (Modulation) is used to observe the spectrum characteristics of the modulated signal, occupied bandwidth, etc.

Note: E series, Fudan and R2000 all support carrier.

Note: Only the E series supports modulation waves, while Fudan and R2000 do not support modulation waves (after setting the frequency, AA48 can be used instead).

Testing Process

①Use the standard demo of Ex10 series initialization to check whether the certification bank of the module is the actual bank used. If not, you can use the demo to modify it, and then power on the module again. (Optional)

②97 configures the working frequency band (China modules can use four frequency bands, and modules in other regions can only use the corresponding frequency bands). (Optional)

③FF00651D6A obtains available frequencies (frequency hopping table). (Optional)

④AA04 and AA27 configure "antenna and power" and "frequency in the frequency hopping table".

⑤Carrier AA3101+stop AA3100 (after the test is completed, you need to stop manually and start the next test command).

⑥Modulate AA31AA+stop AA3100 (after the test is completed, you need to stop manually and start the next test command).

⑦Repeat ⑤ or ⑥. (Optional)

⑧After the test is completed, 97 configures the working frequency band to restore all selected frequencies in the frequency band. (Optional, you can also power on again)

Command attributes

SubCommand Code	Bootloader command	App Firmware command	Subcommand Data
0xAA31	No	Yes	Send command yes, receive command no

Send command SubData field format

0xAA31 sends a command with a SubData field, which contains the following fields, as shown in the table:

Field	Byte length	Description
data	1	00 = stop transmitting carrier and modulation, 01 = transmit carrier, AA = transmit modulation

Command example:

Send command (stop carrier and modulation):

FF	0F	AA	4D 6F 64 75 6C 65 74 65 63 68	AA 31	00
Header	Data Length	Command Code	Subcommand Marker (Moduletech)	Subcommand Code	data

DB	BB	31A8
SubCRC	Terminator	CRC

Receiving command:

FF	0C	AA	00 00	4D 6F 64 75 6C 65 74 65 63 68	AA 31	0F5A
Header	Data Length	Command Code	Status Code	Subcommand Marker (Moduletech)	Subcommand Code	CRC

Send command (transmit carrier signal):

FF	0F	AA	4D 6F 64 75 6C 65 74 65 63 68	AA 31	01
Header	Data Length	Command Code	Subcommand Marker (Moduletech)	Subcommand Code	data

DC	BB	2689
SubCRC	Terminator	CRC

Send command (transmit modulated signal):

FF	0F	AA	4D 6F 64 75 6C 65 74 65 63 68	AA 31	AA
Header	Data Length	Command Code	Subcommand Marker (Moduletech)	Subcommand Code	data

85	BB	7B08
SubCRC	Terminator	CRC

10.8 Set RSSI filter threshold(0xAA5B)

Command Description

This command complies with the extended command communication protocol format(Need to update the firmware 202404024 or later).

This command is used to configure the RSSI filtering function, the purpose of which is to ignore some tag data with too weak signal strength.

In the firmware, when the signal strength of the read tag is weaker than a certain value, the tag data is not uploaded (ignored).

Command attributes

SubCommand Code	Bootloader command	App Firmware command	Subcommand Data
0xAA5B	No	Yes	Send command Yes, receive command Yes

Send command SubData field format

0xAA5B sends a command with the SubData field, which contains the following fields, as shown in the table:

Field	Byte length	Description
data	1/4	If the data length is 1 Byte: 00 Get the current status and setting value. If the data length is 4 Bytes: 01000000 Cancel RSSI filtering function.

Field	Byte length	Description
		If the data length is 4 Bytes: 01AACE00 Enable RSSI filtering = -50。

Receive command SubData field format

0xAA5B receives the command with the SubData field, which contains the following fields, as shown in the table:

Field	Byte Length	Description
data	4/1	If the command sent is "Get": 1. If the data length is 4 Bytes: 00000000 RSSI filtering function is not enabled. 2. If the data length is 4 Bytes: 00AACE00 RSSI filtering is enabled = -50. If the command sent is "Enable or Cancel": The data length is 1 Byte: 01.

Command Examples：

Send command (get current status and setting value)：

FF	0F	AA	4D 6F 64 75 6C 65 74 65 63 68	AA 5B	00
Header	Data Length	Command Code	Subcommand Marker (Moduletech)	Subcommand Code	data

05	BB	0B49
SubCRC	Terminator	CRC

Receive command (get RSSI filtering function is not enabled)：

FF	10	AA	00 00	4D 6F 64 75 6C 65 74 65 63 68	AA 5B	0000 0000	E27C
Header	Data Length	Command Code	Status Code	Subcommand Marker (Moduletech)	Subcommand Code	data	CRC

Receive command (get to enable RSSI filtering function, tags with RSSI < -40

will be ignored)：

FF	10	AA	00 00	4D 6F 64 75 6C 65 74 65 63 68	AA 5B	00AA D800	2EDC
Header	Data Length	Command Code	Status Code	Subcommand Marker (Moduletech)	Subcommand Code	data	CRC

Send command (cancel RSSI filtering function)：

FF	12	AA	4D 6F 64 75 6C 65 74 65 63 68	AA 5B	0100 0000
Header	Data Length	Command Code	Subcommand Marker (Moduletech)	Subcommand Code	data

06	BB	1DAB
SubCRC	Terminator	CRC

Send command (enable RSSI filtering function, tags with RSSI < -40 will be ignored)：

FF	12	AA	4D 6F 64 75 6C 65 74 65 63 68	AA 5B	01AA D800
Header	Data Length	Command Code	Subcommand Marker (Moduletech)	Subcommand Code	data

88	BB	7578
SubCRC	Terminator	CRC

10.9Temperature and humidity LED tag(0xAA5A)

Command Description

This command complies with the extended command communication protocol format. This command is used to take inventory of various temperature and humidity labels, light up LED labels, etc.

Currently only 3 types of Intel, NXP U8/U8M, and SCR409 are supported. Only the certification bank is China.

Command attributes

SubCommand Code	Bootloader command	App Firmware command	Subcommand Data
0xAA5A	No	Yes	Send command Yes, receive command Yes

Send command SubData field format

0xAA5A sends a command with the SubData field, which contains the following fields, as shown in the table:

Field	Byte length	Description
TAGTYPE	2	0001: Inno Temperature Tag NMV2D_V1.1_0512 0002: Yuehe Temperature Tag LTU32 0003: Fudan Micro Temperature Tag FM13DT160 0004: Caravelle LED Tag KX2005X-BL 0005: E-MAN EWIZ TAG 266B01 Ink Screen Tag 0006: FUJITSU MB97R8110 Ink Screen Tag: 0007: NXP U8/U8M 0008: Tag with authentication function, EPC V2.0 Authenticate command 0009: SCR409 Temperature Tag
CMDDATAS	M	Different types of tags have different command data, see below for details

Description of various tags

- Inno Temperature Tag: After counting the tags, the BANK bank must be read and written repeatedly to obtain temperature related information;

- Yuehe Temperature Scale: A SELECT command in a specific format is sent to indicate that the temperature is to be acquired. When the tag inventory is subsequently taken, the temperature data will be returned together with the EPC, and the temperature calculation parameters embedded in the read BANK bank must also be used.
- Fudan Micro Temperature Standard: Customized commands need to be sent. To obtain temperature information, two commands, start and get, need to be sent.
- Caravelle LED tag: Just read the address 4 length 1 in the RESERVE bank to light up the LED;
- Ink screen tag: It is necessary to provide an interface to keep the tag powered on after inventorying it, and then listen to the commands sent to perform multiple read and write operations on the tag;
- With authentication function tag, EPC V2.0 Authenticate command;
- SCR409 temperature tag;

Receive command SubData field format

0xAA5A receives the command with the SubData field, which contains the following fields, as shown in the table:

Field	Byte length	Description
TAGTYPE	2	Tag type identification (same as above)
CMDRESULTDATAS	M	Operation Results

When the status code is failure, you do not need to pay attention to the entire data field. You only need to confirm what kind of failure the status code reflects.

10.9.1 TAGTYPE=0001：Inno Temperature

Sending CMDDATAS is explained as follows:

Field	Byte length	Description
Timeout	2	Command execution time, in milliseconds.
RFU	4	Reserved for future use. The value is 00000000.
Select Option	1	For Select Options in Tag Singulation, see Section 5.1.1.
Access Password	0/4	The meaning is the same as command 0x28.
Tag Singulation	N	The meaning is the same as command 0x28.

The details of receiving CMDRESULTDATAS are as follows:

Field	**Byte length**	**Description**
RSSI	1	The signal strength detected by the tag, in dBm, signed single Byte.
Frequency	3	The frequency being panned, in kHz.
PHASE	2	The high Byte is the starting phase value, and the low Byte is the ending phase value. The way to convert phase data to degrees is: (phase value/256)*360(degrees)
EPC Length	1	It is the Byte length of PC+EPCID+TagCRC.
PC Word	2	The PC field in the EPC bank.
EPC ID	N	EPCID
CRC-16	2	TagCRC
A	2	CALIBRATED PARAMETERS A
B	2	CALIBRATED PARAMETERS B
C	2	CALIBRATED PARAMETERS C
N1	2	The lower 12 bits are valid, which is a set of N values for obtaining the temperature tag.
N2	2	The lower 12 bits are valid, which is a set of N values for obtaining the temperature tag.
N3	2	The lower 12 bits are valid, which is a set of N values for obtaining the temperature tag.
N4	2	The lower 12 bits are valid, which is a set of N values for obtaining the temperature tag.
N5	2	The lower 12 bits are valid, which is a set of N values for obtaining the temperature tag.

Field	Byte length	Description
N6	2	The lower 12 bits are valid, which is a set of N values for obtaining the temperature tag.
N7	2	The lower 12 bits are valid, which is a set of N values for obtaining the temperature tag.
N8	2	The lower 12 bits are valid, which is a set of N values for obtaining the temperature tag.
N9	2	The lower 12 bits are valid, which is a set of N values for obtaining the temperature tag.
N10	2	The lower 12 bits are valid, which is a set of N values for obtaining the temperature tag.

Note: To calculate the temperature value, you need to read 10 sets of N values, remove the maximum and minimum values and take the average value. Please refer to the temperature tag information for details.

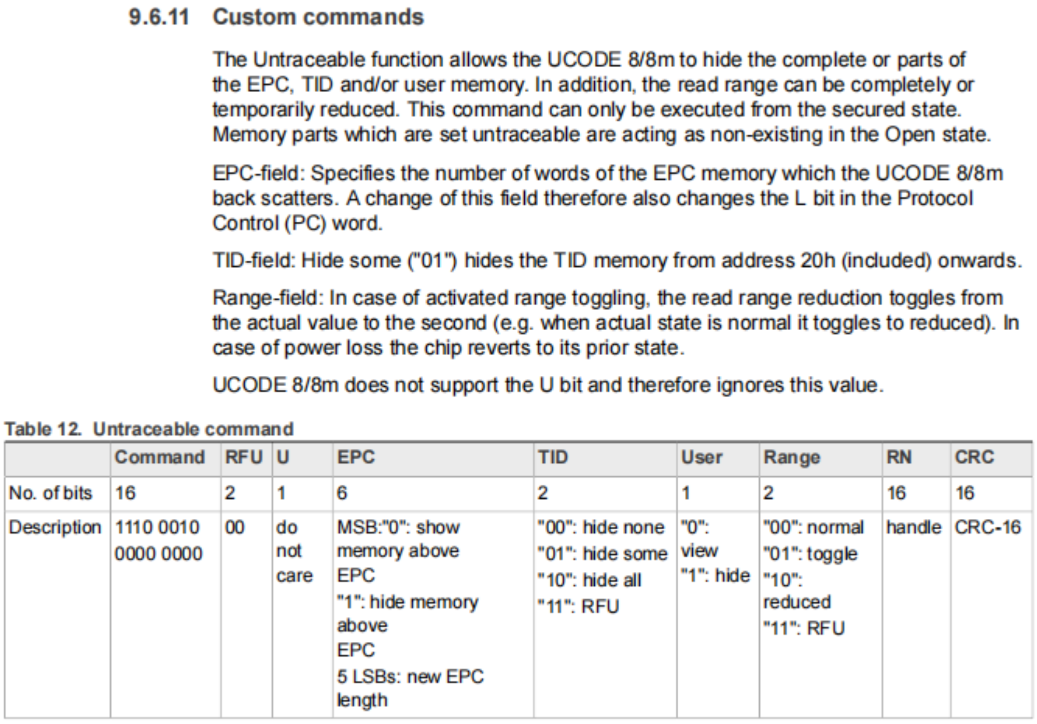
10.9.2 TAGTYPE=0007： NXP U8/U8M

Sending CMDDATAS is explained as follows:

Field	Byte length	Description
Timeout	2	command execution time, in milliseconds.
NXPcmd	2	Currently only 0001, custom commands for NXP U8/8M are supported.
NXPcmddata	2	Corresponding data of NXPcmd command. When NXPcmd = 0001, NXPcmddata is 2 Bytes, see below.
Select Option	1	For Select Options in Tag Singulation, see Section 5.1.1.
Access Password	0/4	The meaning is the same as command 0x28.
Tag Singulation	N	The meaning is the same as command 0x28.

NXPcmddata explains:

Control BIT	BIT length	Description	Example value (binary)	Example NXPcmdData Value
0/1	2	Range	01(toggle)	Hexadecimal: 04F1 Binary: 1 00111 10 0 01
2	1	User	0(view)	
3/4	2	TID	10(hide all)	
5~9	5	EPC	00111(new EPC Length)	
10	1	EPC	1(show)	



9.6.11 Custom commands

The Untraceable function allows the UCODE 8/8m to hide the complete or parts of the EPC, TID and/or user memory. In addition, the read range can be completely or temporarily reduced. This command can only be executed from the secured state. Memory parts which are set untraceable are acting as non-existing in the Open state.

EPC-field: Specifies the number of words of the EPC memory which the UCODE 8/8m back scatters. A change of this field therefore also changes the L bit in the Protocol Control (PC) word.

TID-field: Hide some ("01") hides the TID memory from address 20h (included) onwards.

Range-field: In case of activated range toggling, the read range reduction toggles from the actual value to the second (e.g. when actual state is normal it toggles to reduced). In case of power loss the chip reverts to its prior state.

UCODE 8/8m does not support the U bit and therefore ignores this value.

Table 12. Untraceable command

	Command	RFU	U	EPC	TID	User	Range	RN	CRC
No. of bits	16	2	1	6	2	1	2	16	16
Description	1110 0010 0000 0000	00	do not care	MSB:"0": show memory above EPC "1": hide memory above EPC 5 LSBs: new EPC length	"00": hide none "01": hide some "10": hide all "11": RFU	"0": view "1": hide	"00": normal "01": toggle "10": reduced "11": RFU	handle	CRC-16

The details of receiving CMDRESULTDATAS are as follows:

Field	Byte length	Description
RSSI	1	The signal strength detected by the tag, in dBm, signed single Byte.
Frequency	3	The frequency being panned, in kHz.
PHASE	2	The high Byte is the starting phase value, and the low Byte is the ending phase value. The way to convert phase data to degrees is: (phase value/256)*360(degrees)
EPC Length	1	It is the Byte length of PC+EPCID+TagCRC.
PC Word	2	The PC field in the EPC bank.
EPC ID	N	EPCID
CRC-16	2	TagCRC

Impinj RFID Series Protocol Document

10.9.3 TAGTYPE=0009： SCR409 Temperature

Sending CMDDATAS is explained as follows:

Field	Byte length	Description
Timeout	2	Command execution time, in milliseconds.
RFU	4	Reserved, 0x00 00 00 00
Select Option	1	For Select Options in Tag Singulation, see Section 5.1.1.
Access Password	0/4	The meaning is the same as command 0x28.
Tag Singulation	N	The meaning is the same as command 0x28.

Receiving CMDRESULTDATAS is explained as follows：

Field	Byte length	Description
RSSI	1	The signal strength detected by the tag, in dBm, signed single Byte.
Frequency	3	The frequency being panned, in kHz.
PHASE	2	The high Byte is the starting phase value, and the low Byte is the ending phase value. The way to convert phase data to degrees is: (phase value/256)*360(degrees)
EPC Length	1	It is the Byte length of PC+EPCID+TagCRC.
PC Word	2	The PC field in the EPC bank.
EPC ID	N	EPCID
CRC-16	2	TagCRC
0X92 DATA	2	The value of address 0X92 in the USER bank, with high Byte first.

Field	Byte length	Description
0X93 DATA	2	The value of address 0X93 in the USER bank, with high Byte first.
0X94 DATA	2	The value of USER bank address 0X94, high Byte first.
0X95 DATA	2	The value of USER bank address 0X95, high Byte first.
0X97 DATA	2	The value of USER bank address 0X97, high Byte first.

Command example:

Send command (SCR409 temperature, read time 1000ms)： FF 17 AA 4D 6F 64 75 6C 65 74 65 63 68 AA 5A 00 09 03 E8 00 00 00 00 00 F8 BB 69 28

Receiving command:FF 2F AA 00 00 4D 6F 64 75 6C 65 74 65 63 68 AA 5A 00 09 C8 0D F7 32 E6 E6 10 30 00 55 66 77 88 99 00 11 22 33 44 55 66 A2 2C 40 08 17 98 4B 54 34 BC 0C 28 F4 22

即:-56dBm,915250kHz,Phase:E6E6,EPC:556677889900112233445566,28.19℃

Receiving command:FF 2F AA 00 00 4D 6F 64 75 6C 65 74 65 63 68 AA 5A 00 09 DE 0E 26 12 AA AA 10 34 00 00 00 00 00 00 00 00 00 00 00 00 01 E0 29 40 12 17 98 4B 54 34 BC 0C 64 1B 75

That is: -34dBm, 927250kHz, Phase: AAAA, EPC: 000000000000000000000001, 25.78℃

Receiving command:FF 0C AA 04 23 4D 6F 64 75 6C 65 74 65 63 68 AA 5A D0 65

That is: 0423 error (out of label range)

10.10 Flip the S2 channel of the tag to side A(0xAA4D)

Command Description

This command complies with the extended command communication protocol format. This command can only be used for Chinese conventional modules.This command will try to flip the Session2 channel of all tags within the antenna range to side A for inventory again.

When using this command, it is recommended to send it three times, namely the "maximum/middle/minimum" frequency points in the frequency hopping table.

Command attributes

SubCommand Code	**Bootloader command**	**App Firmware command**	**Subcommand Data**
0xAA4D	No	Yes	Send command yes, receive command no

Send command SubData field format

0xAA4D sends a command with the SubData field, which contains the following fields, as shown in the table:

Field	**Byte length**	**Description**
AntFlag	2	Enabled antennas, BIT0 for antenna 1, BIT15 for antenna 16. These antennas must exist and be correctly connected. For example, 0x4001 for antennas 1 and 15.

Field	Byte length	Description
Freq	4	The specified frequency (in the frequency hopping table), for example 902750 is 0x000DC65E.
Power	2	The transmit power used this time, for example 30dBm is 0x0BB8.

Command Examples：

Send command (antenna 1, transmit power 33dBm, frequency 902750)：

FF16AA4D6F64756C6574656368AA4D0001000DC65E0CE419BB06AA

Send command (antenna 1 and 3, transmit power 32dBm, frequency 926250)：

FF16AA4D6F64756C6574656368AA4D0005000E222A0C80E2BBB44F

Receive command (sent correctly)：

FF0CAA00004D6F64756C6574656368AA4D0F26

Receive command (error such as antenna not connected)：

FF0CAAAA4D4D6F64756C6574656368AA4DB930

Appendix

Appendix 1 Status Code

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

Status code description table

Status Code	Description
0x0000	Success
0x0100	The actual length of the Data is different from the value of the Data Length field.
0x0101	The command is unavailable. This is usually caused by unstable module power supply, which leads to module soft reset.
0x0105	Parameter value not available
0x010A	Parameter value not available
0x010B	Unavailable region selection
0x0200	App Firmware layer program CRC is incorrect
0x0302	Flash undefined error, flash write failed
0x0400	Tag not found, usually due to insufficient power or filter mismatch
0x0402	Protocol not available
0x0404	Write success when embedded in read, but read failure
0x040A	General tag errors (read/write lock, kill command)
0x040B	The read memory bank exceeds the limit (for example, only 96 blocks can be read at a time)
0x040C	Unavailable Destroy Password

Status Code	Description
0x0420	GEN2 protocol error
0x0423	Memory bank out of bounds, wrong PC
0x0424	Locked storage bank
0x042B	Lack of energy
0x042F	Non-specific error
0x0430	Unknown error
0x0500	Frequency value not available
0x0504	Temperature is too high
0x0505	Excessive return loss is common in metal reflection environments, and rarely occurs due to frequency, antenna, etc.
0x7F00	The system is not aware of the error, serious error. The RF hardware circuit failed to start
0x500F	iLian temperature label detected temperature is out of range
0x50FF	iLian temperature tag detects unstable temperature
0xAA02	Failed to write OEM register
0xAA03	Failed to read OEM register
0xAA04	The command failed to execute
0xAA2A	OEM formatting failed
0xAA31	The carrier opening or closing operation failed (the antenna is not connected). You need to connect an antenna or a spectrum analyzer
0xAA40	Indicates that the save configuration command failed to write the OEM register

Status Code	Description
0xAA4A	If the standing wave detection fails, you may need to check the hardware problem
0xAA4B	Indicates that the reset or power on/off operation failed
0xAA4C	Indicates that there is no valid setting for multi-tag matching filtering data
0xAA4D	Indicates that the setting of Session2/Session3 and Target A failed
0xAA55	User-defined storage bank command, read and write execution failed
0xAA56	Failed to configure or read the user-defined command
0xEE01	The chip did not execute to the application layer error
0xEE02	Chip firmware switch upgrade failed
0xEE03	Chip firmware continues to upgrade failed
0xEE04	Chip firmware upgrade failed
0xFF11	FLASH initialization failed
0xFF12	GPIO initialization failed
0xFF13	Timer initialization failed
0xFF14	SPI initialization failed
0xFF15	Antenna control initialization failed
0xFF16	Band initialization failed
0xFF17	EX10 initialization failed
0xFF1F	Firmware abnormality

Status Code	Description
0xFFFF	The hardware version number is wrong, the hardware version needs to be written
Other non-0	Command execution failed

Appendix 2 Regions and Regional Frequency Table

Work Area

The relationship between the setting value and the corresponding frequency bank of the Chinese version module (certified for China) is as follows:

Bank Name	Area Code
North America (902~928)	0x01
China 1 (920~925)	0x06
CE_LOW (865~867)	0x08
Full Frequency Band(860~960)	0xFF

The relationship between the setting values of other regional modules (non-China certified regions) and the corresponding frequency regions is as follows. Only the corresponding frequency bands can be set.:

Bank Name	Area Code
North America (902~928)	0x01
China 1 (920~925)	0x06
CE_LOW (865~867)	0x08
KOREA	0x09
JAPAN (NO LBT 4FRE)	0x0B
JAPAN2 (LBT 6FRE)	0x1F
JAPAN3 (NO LBT 19FRE,MAX power 24dBm)	0x20
CE_HIGH (916~919)	0x0C
HK	0x0D
TAIWAN	0x0E
MALAYSIA	0x0F
SOUTH_AFRICA	0x10
BRAZIL	0x11
THAILAND	0x12
SINGAPORE	0x13
AUSTRALIA	0x14
INDIA	0x04
URUGUAY	0x16
VIETNAM	0x17
ISRAEL	0x18
PHILIPPINES	0x19
INDONESIA	0x1A

Bank Name	Area Code
NEW_ZEALAND	0x1B
PERU	0x1C
RUSSIA	0x1D

Regional frequency table

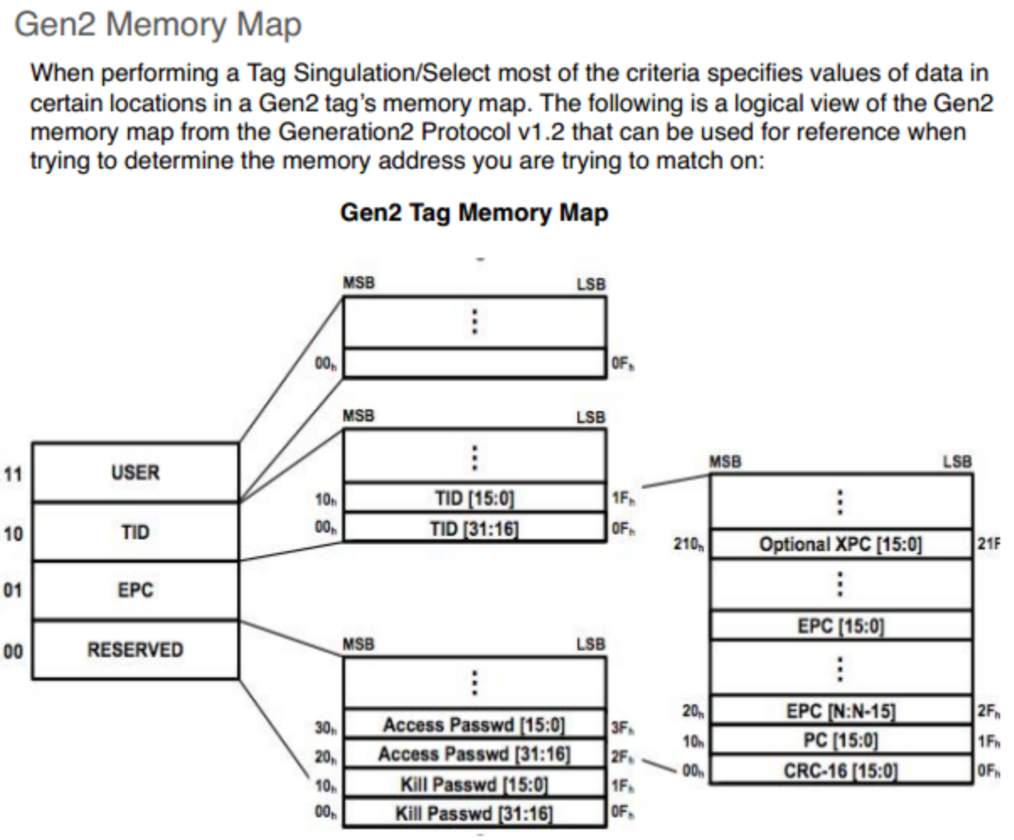
The command to set the frequency hopping table can only select the frequencies that belong to the current working bank of the module.
After executing the command to set the current working bank, the frequencies in the frequency table are the default hopping table for each bank.

Bank	Frequency(kHz)
North America (902~928)	915250,902750,927250,915750,903250,926750,908250,918250,923250,905250,916250,911250,921250,913250,906250,914250,909250,919250,924250,904250,917250,912250,922250,920250,907250,914750,909750,919750,924750,904750,912750,907750,917750,922750,910250,925250,910750,920750,925750,905750,913750,908750,918750,923750,903750,916750,911750,921750,926250,906750
China 1 (920~925)	922125,920625,924375,922375,920875,924125,922625,921125,923875,921875,923625,922875,921375,923125,921625,923375
CE_LOW (865~867)	865700,866300,866900,867500
Full Frequency Band (860~960)	860000,870000,880000,890000,900000,910000,920000,930000,940000,950000,960000
Japan (no LBT, 916~921)	916800,918000,919200,920400
Japan 2 (with LBT, 916~921)	916800,918000,919200,920400,920600,920800
Japan 3 (without LBT, 916~924)	916800,918000,919200,920400,920600,920800,921000,921200921400,921600,921800,922000,922200,922400,922600,922800923000,923200,923400
South Korea (917~921)	917300,917900,918500,919100,919700,920300
CE_HIGH (916~919)	916300,917500,918700
Hong Kong (920~925)	920250,920750,921250,921750,922250,922750,923250,923750,924250,924750

Bank	Frequency(kHz)
Taiwan (920~927)	920750,921250,921750,922250,922750,923250,923750,924250,924750,925250,925750,926250,926750,927250
MALAYSIA (919~923)	919250,919750,920250,920750,921250,921750,922250,922750
SOUTH_AFRICA (915~918)	915600,915800,916000,916200,916400,916600,916800,917000,917200,917400,917600,917800,918000,918200,918400,918600,918800
BRAZIL(902~907.5,915~928)	902750,903250,903750,904250,904750,905250,905750,906250,906750,907250,915250,915750,916250,916750,917250,917750,918250,918750,919250,919750,920250,920750,921250,921750,922250,922750,923250,923750,924250,924750,925250,925750,926250,926750,927250
THAILAND (920~925)	920250,920750,921250,921750,922250,922750,923250,923750,924250,924750
SINGAPORE (920~925)	920250,920750,921250,921750,922250,922750,923250,923750,924250,924750
AUSTRALIA (920~925)	920250,920750,921250,921750,922250,922750,923250,923750,924250,924750
INDIA (865~867)	865100,865700,866300,866900
URUGUAY (916~927)	916250,916750,917250,917750,918250,918750,919250,919750,920250,920750,921250,921750,922250,922750,923250,923750,924250,924750,925250,925750,926250,926750,927250
VIETNAM (918~922)	918750,919250,919750,920250,920750,921250,921750,922250
ISRAEL (916)	916250
PHILIPPINES (918~920)	918250,918750,919250,919750
INDONESIA (917~922)	917250,920750,921250,921750
NEW_ZEALAND (922~927)	922250,922750,923250,923750,924250,924750,925250,925750,926250,926750
PERU (916~927)	916250,916750,917250,917750,918250,918750,919250,919750,920250,920750,921250,921750,922250,922750,923250,923750,924250,924750,925250,925750,926250,926750,927250

Bank	Frequency(kHz)
RUSSIA (916~920)	916200,917400,918600,919800

Appendix 3 Gen2 Tag Memory Structure



Gen2 Memory Map

When performing a Tag Singulation/Select most of the criteria specifies values of data in certain locations in a Gen2 tag's memory map. The following is a logical view of the Gen2 memory map from the Generation2 Protocol v1.2 that can be used for reference when trying to determine the memory address you are trying to match on:

Gen2 Tag Memory Map

Serial number	BANK	Description (1 block = 2 Bytes = 16 bits) (block address starts from 0)
0	Reserved Area	Blocks 0 to 1 are the Kill passwords. Blocks 2 to 3 are the Access passwords.
1	EPC	The 0th block is TagCRC_EPCCRC, the 1st block is PC, and the following blocks are EPCID.

2	TID	The block address starts from 0, and the first block is block 0.
3	USEER	The block address starts from 0, and the first block is block 0.

Appendix 4 C language example of command CRC

Sending commands:

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

Receiving commands:

FF	14	03	00 00	22 02 11 00
Header	Data Length	Command Code	Status Code	BootLoader Version
32 00 00 00	20 23 09 03	23 09 03 00	00 00 00 10	63 5C
Hardware Version	Firmware Date	Firmware Version	Supported Protocol	CRC

```c
#include<stdio.h>
unsigned short CalcCRC(unsigned char *msgbuf,unsigned char msglen)
{
    unsigned short calcCrc=0xFFFF;
    unsigned char xorFlag;
    for(unsigned char i=1;i<msglen;i++)//Starting from index 1, the actual 0xFF is not included in the calculation
        for(char dcdBit=7;dcdBit>=0;dcdBit--)
        {
            xorFlag=calcCrc>>15;
            calcCrc=calcCrc<<1|msgbuf[i]>>dcdBit&1;
            if(xorFlag)calcCrc^=0x1021;
        }
    return calcCrc;
}
int main()
{
    //Test sending command FF00031D0C
    //unsigned char sendata[]={0xFF,0x00,0x03};//不填入 CRC
    //Test receiving command FF140300002202110032000000202309032309030000000010635C
    unsigned char sendata[]={0xFF,0x14,0x03,0x00,0x00,0x22,0x02,0x11,0x00,0x32,0x00,0x00,0x00,0x20,0x23,0x09,0x03,0x23,0x09,0x03,0x00,0x00,0x00,0x00,0x10};//Do not fill in CRC
    //The address of the frame header 0xFF and the length of the command without CRC are passed in.
    unsigned short crc=CalcCRC(sendata,sizeof(sendata));
    printf("CRC16:%02X%02X\n",(crc>>8)&0xFF,crc&0xFF);
    return 0;
}
```

Appendix 5 C language example of TagCRC_EPCCRC

```c
#include<stdio.h>
unsigned short ISO6Ccrc16(unsigned short seed,unsigned char len,unsigned
 char *data)
{
    unsigned char mask;
    unsigned short crcVal;
    crcVal=seed;
    for(;len;len--,data++)
    {
        for(mask=0x80;mask;mask>>=1)
        {
            if(crcVal&0x8000)
            {
                crcVal=crcVal<<1;
                crcVal^=0x1021;
            }
            else
                crcVal=crcVal<<1;
            if(*data&mask)
                crcVal^=0x1021;
        }
    }
    return ~crcVal;
}
int main()
{
    //unsigned char PCEPC[]={0x10,0x00,0x01,0x23,0x45,0x67};//AC31 1000
01234567000000000000000000
    unsigned char PCEPC[]={0x30,0x00,0x05,0x00,0x00,0x00,0x00,0x00,0x00,
0x00,0x00,0x00,0x23,0x54};//4AC8 3000 0500000000000000000002354
    //The frame header PC and EPCID are passed in.
    unsigned short TagCRC=ISO6Ccrc16(0xFFFF,sizeof(PCEPC),PCEPC);
    printf("TagCRC_EPCCRC:%02X%02X\n",(TagCRC&0xff00)>>8,TagCRC&0x00ff);
    return 0;
}
```

Appendix 6 SubCRC C language example

Sending commands:

FF	10	AA	4D 6F 64 75 6C 65 74 65 63 68	AA 40	AA	01	95	BB	8D 63
Header	Data Length	Command Code	Subcommand Marker (Moduletech)	Subcommand Code	KEY	GETORSET	SubCRC	Terminator	CRC

```
#include<stdio.h>
unsigned char GetSubcrc(unsigned char*data,unsigned char len)
{
    unsigned char i,temp=0;
    for(i=0;i<len;i++)
        temp+=data[i];
    return temp;
}
int main()
{
    unsigned char opdata[]={0xAA,0x40,0xAA,0x01};//The result is 95 followed by BB
    //The part passed in is the part after Subcommand Code (inclusive) until SubCRC (exclusive)
    unsigned char SubCRC=GetSubcrc(opdata,sizeof(opdata));
    printf("SubCRC:%02X\n",SubCRC);
}
```