A1408 Modbus Gateway Controller Communication Protocol Specification



|  |  |  |
| --- | --- | --- |
| File status:  [√] Draft  [ ] Official release  [ ] Under revision | File ID: |  |
| Current version: | V1.4 |
| Author: |  |
| Review: |  |
| Completion date: |  |
| Scope of application: | **867，865，864，713，712** |

Wuhan Jinfu Technology Co., Ltd.

Version History

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Version/Status | Author | Review | Start and End Date | Notes |
| V1.0 |  |  | 2021-11-01 | Create this document |
| V1.1 |  |  | 2021-12-14 | Add card swipe protocol |
| V1.2 |  |  | 2022-02-01 | Improve the protocol section for other models of locks |

**Contents**

[Contents 3](#_bookmark0)

Overview 5

General Frame Format 5

* 1. Preamble 5
  2. Frame Length 5
  3. Opcode 5
  4. Payload 6
  5. Checksum 6

Opcode Description 6

* 1. Heartbeat packet data (0x01) 7
  2. Unlock command (0x02) 8
  3. User number setting (0x03) 8
  4. Write swipe IC card number (0x04) 9
  5. Read IC card number (0x05) 9
  6. Send password data (0x06) 9
  7. Get password data (0x07) 10
  8. Send fingerprint data (0x08) 10
  9. Get fingerprint data (0x09) 11
  10. Get unlock information in the lock (0x0A) 11
  11. Set lock time (0x10) 14
  12. Get lock time (0x11) 15
  13. Modify lock ID (0x12) 15
  14. Clear the data stored in the lock (0x13) 16
  15. Get lock function information (0x14) 16
  16. Modify device ID (0x15) 17
  17. Poll online locks (0x16) 17
  18. Query lock user information (0x17) 18
  19. Write IC card number to lock (0x18) (for /865/864) 18
  20. Delete IC card number in lock (0x19) (for /865/864) 18
  21. Read card swipe record in lock (0x20) (for /865/864) 19
  22. Read authorized IC card number in lock (0x21) (for /865/864) 19
  23. Unlock enable (0x22) 20
  24. Get unlock enable information (0x23) 20
  25. Single or double user verification selection (0x24) 21
  26. Get single or double user verification information (0x25) 21
  27. Lock enters remote upgrade (0x26) 22
  28. Device enters remote upgrade (0x27) 22
  29. Lock model register (0x28) 22
  30. Get device information (0x29) 23
  31. Set device local IP (0x30) 24
  32. Get device local IP (0x31) 26
  33. Set target IP (0x32) 26
  34. Get target IP (0x33) 27
  35. Set the device target port number (0x34) 27
  36. Get the device port number (0x35) 28
  37. Set subnet mask address (0x36) **Error! Bookmark not defined.**
  38. Get subnet mask address (0x37) **Error! Bookmark not defined.**
  39. Set gateway address (0x38) **Error! Bookmark not defined.**
  40. Get gateway address (0x39) **Error! Bookmark not defined.**
  41. Data exception (0xFF) 28

1. **Overview**

This document provides the network communication protocol of the box controller.

1. **General Frame Format**

A complete protocol includes preamble, frame header, operation code, payload, and checksum. See Table 2-1 General frame format

Table 2-1 General frame format

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Preamble | Frame length | Operation code | Payload | Checksum |
| 2 bytes | 2 bytes | 1 bytes | 0-N bytes | 2 byte |

* 1. **Preamble**

The leading code is a fixed value of 0xAA 0xBB

Table 2-2 Preamble format

|  |  |
| --- | --- |
| Preamble field 1 | Preamble field 2 |
| 1 byte | 1 byte |
| 0xAA(PreCode1) | 0xBB(PreCode1) |

* 1. **Frame Length**

Table 2-3 Frame length format

|  |
| --- |
| Field 1 |
| 2 bytes |
| Frame length (Fram Len) |

Frame length: 2 bytes, the sum of all byte lengths except the preamble and length word, including the checksum.

* 1. **Operation Code**

Table 2-4 Operation code format

1 byte

Operation code field

Operation code (Cmd)

Operation code: Specific command operation instructions, see the following operation code description for details.

**2.4 Payload**

Table 2-5 Payload structure

|  |
| --- |
| Payload field |
| 0-N byte |
| Operation parameters |

Operation parameters: Varies according to the specific operation. Its data length is the frame length - 3; see the operation code for details. section.

**2.5 Check**

Table 2-6 Check structure

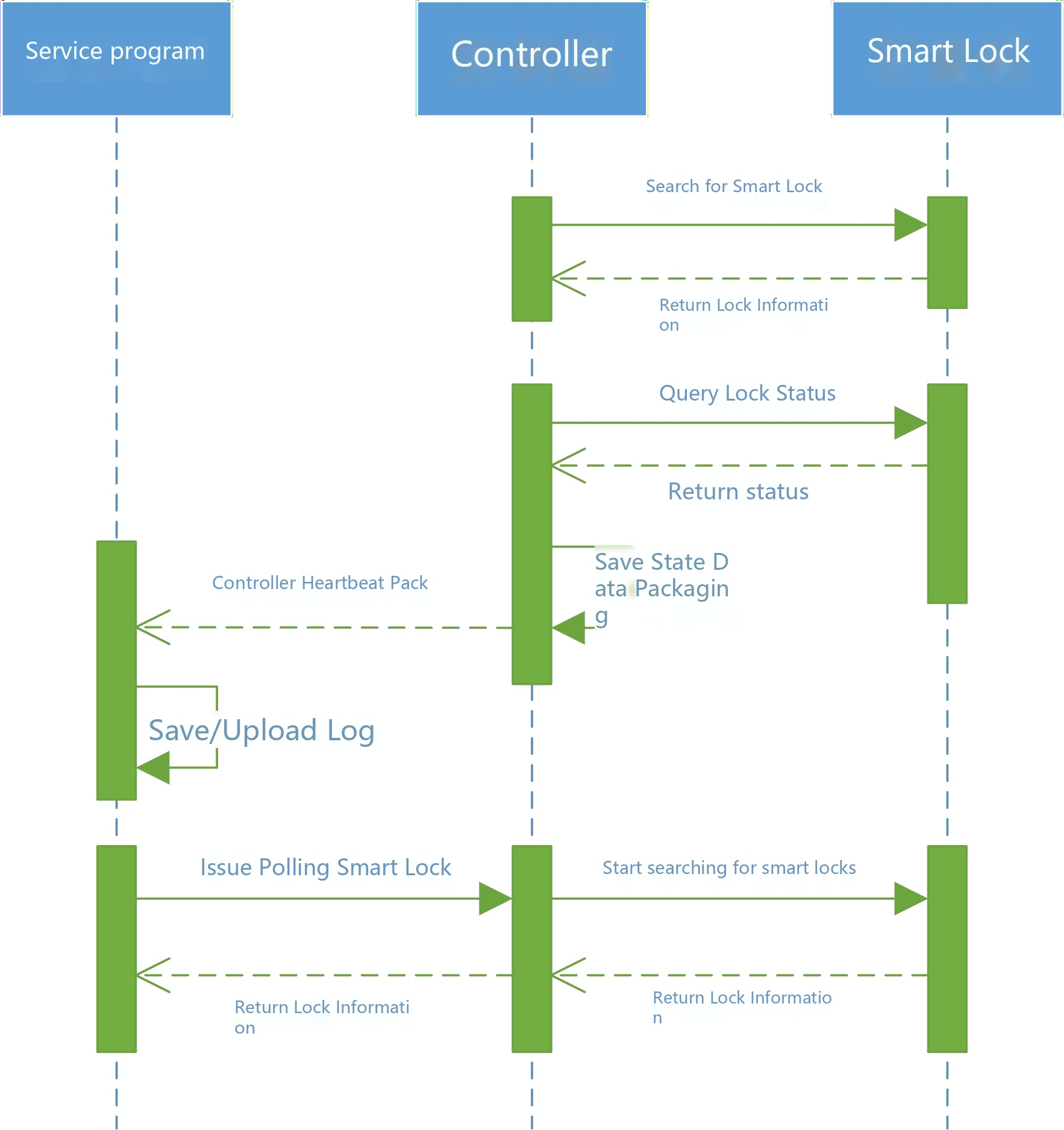
|  |  |
| --- | --- |
| Check field 1 | Check field 2 |
| 1 byte | 1 byte |
| Check value 1 | Check value 2 |

Check: The CRC-16 of all data from the frame header (inclusive) to the payload is the check value; where check value 1 is the CRC-16 low byte, and check value 2 is the CRC-16 high byte.

**3 Operation Code Description**

All operations on the device are distinguished by operation codes. Different operation codes require different operation parameters. This section describes each operation code in detail. The numbers in the following content are all hexadecimal unless otherwise specified. The status byte 0x01 is returned for success, and 0x00 is returned for failure.

Data packets include three types: heartbeat packets, active upload packets, and host query packets. The main workflow of the operation is as follows:



**3.1 Heartbeat Packet Data (0x01)**

This command is used for the device to upload heartbeat packet data to the server. The controller will automatically query the locks on the RS485 bus when it is powered on for the first time. The query interval for each lock is about 200ms. After querying the status 5 times, a heartbeat is sent.

3-1 Heartbeat packet data

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Operation code | Operation parameters | | |  |  |
| 01 | Device ID | Lock ID | Lock status | Temperature | Humidity |
| 4 bytes | 1 byte | 1 byte | 1 byte | 1 byte |

Note: If there is no lock on the bus, the lock ID in the controller's heartbeat packet will reply with FF.

Table 3-2 Lock status

|  |  |  |  |
| --- | --- | --- | --- |
| Lock status | |  |  |
| High byte | Low byte | Temperature | Humidity |
| 1-Door open  0-Door closed | 1-Handle open  0-Handle closed | 1 byte | 1 byte |

Note: Heartbeat packet has no response packet returned:

Table 3-4 Query command

|  |  |  |  |
| --- | --- | --- | --- |
| Operation code | Operation parameters | | |
| 01 | Device ID | Lock ID | Status |
| 4 bytes | 1 byte | 1 byte |

The server actively queries the lock status, sending:

Table 3-3 Query command

|  |  |  |
| --- | --- | --- |
| Operation code | Operation parameter | |
| 01 | Device ID | Lock ID |
| 4 bytes | 1 byte |

Reply:

Table 3-4 Query command

|  |  |  |  |
| --- | --- | --- | --- |
| Operation code | Operation parameter | | |
| 01 | Device ID | Lock ID | Lock status |
| 4 bytes | 1 byte | 1 byte |

**3.2 Unlock Command (0x02)**

This command is used to unlock the device, sending:

Table 3-5 Unlock command

|  |  |  |  |
| --- | --- | --- | --- |
| Operation code | Operation parameter | | |
| 02 | Device ID | Lock ID | Unlock confirmation |
| 4 bytes | 1 byte | 1 byte |

The unlock confirmation is the lock ID. Return:

Table 3-6 Unlock command data return format

|  |  |  |  |
| --- | --- | --- | --- |
| Operation code | Operation parameter | | |
| 02 | Device ID | Lock ID | Reply status |
| 4 bytes | 1 byte | 1 byte |

Description: Command reply status: 01-Unlocked 00-Unlocked

**3.3 User ID Setting (0x03)**

This command is used to set the user number in the electronic lock and send:

Table 3-7 User number setting

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Operation code | Operation parameter | | | |
| 03 | Device ID | Lock ID | Operation function | User number |
| 4 bytes | 1 byte | 1 byte | 2 bytes |

Description: Operation function: 01-Create new user, 02-Delete user, User number: Maximum is 300 Return:

Table 3-8 User number setting return

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Operation code | Operation parameter | | | |
| 03 | Device ID | Lock ID | User number | Setting result |
| 4 bytes | 1 byte | 2 bytes | 1 byte |

Description: Setting result: 01-Success 02-User already exists 03-Failure

* 1. **Write IC Card Number (0x04)**

This command is used to send the IC card number to the device:

Table 3-9 Write IC card number

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Operation code | Operation parameter | | | |
| 04 | Device ID | Lock ID | User number | IC card number |
| 4 bytes | 1 byte | 2 bytes | 4 bytes |

Return:

Table 3-10 Return status information

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Operation code | Operation parameter | | | |
| 04 | Device ID | Lock ID | User number | Status information |
| 4 bytes | 1 byte | 2 bytes | 1 byte |

Description: Status information: 01-successful 00-unsuccessful, if the user number does not exist, the user number returns 0xFF, 0xFF

* 1. **Read IC Card Number (0x05)**

This command is used to read the IC card number in the device

Send: Read number FF FF is to read the current card number.

Table 3-11 Read IC card number

|  |  |  |  |
| --- | --- | --- | --- |
| Operation code | Operation parameter | | |
| 05 | Device ID | Lock ID | User number |
| 4 bytes | 1 byte | 2 bytes |

Return:

Table 3-12 Return IC card number information

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Operation code | Operation parameter | | | |
| 05 | Device ID | Lock ID | User number | IC card number |
| 4 bytes | 1 byte | 2 bytes | 4 bytes |

If the user does not have an IC card number, the IC card number returns empty. If there is no user number, return data abnormal instruction

* 1. **Send Password Data (0x06)**

This command is used to send password data

Send:

Table 3-13 Send password

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Operation code | Operation parameter | | | |
| 06 | Device ID | Lock ID | User number | Password |
| 4 bytes | 1 byte | 2 bytes | 6 bytes |

Return:

Table 3-14 Return status information

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Operation code | Operation parameter | | | |
| 06 | Device ID | Lock ID | User number | Status |
| 4 bytes | 1 byte | 2 bytes | 1bytes |
|  |  |  |  |  |

Description: Setting information: 01-success 00-unsuccessful, if the user number does not exist, the user number returns 0xFF, 0xFF

**3.7 Get Password Data (0x07)**

This command is used to obtain the password data in the lock. Send:

Table 3-15 Get the password in the lock

|  |  |  |  |
| --- | --- | --- | --- |
| Operation code | Operation parameter | | |
| 07 | Device ID | Lock ID | User number |
| 4 bytes | 1 byte | 2 bytes |

Return:

Table 3-16 Password information in the lock

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Operation code | Operation parameter | | | |
| 07 | Device ID | Lock ID | User number | Password |
| 4 bytes | 1 byte | 2 bytes | 6 bytes |

Note: If the user has no password, the password returns empty. If there is no user number, the return data is abnormal. Instruction

**3.8 Send Fingerprint Data (0x08)**

This command is used to send fingerprint data. Send:

Table 3-17 Send fingerprint data

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Operation code | Operation parameter | | | |
| 08 | Device ID | Lock ID | User number | Fingerprint data |
| 4 bytes | 1 byte | 2 bytes | 512 bytes |

Return:

Table 3-18 Return operation parameters

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Operation code | Operation parameters | | |  |
| 08 | Device ID | Lock ID | User number | Status parameters |
| 4 bytes | 1 byte | 2 bytes | 1 byte |

Description: Status parameters: 01-Normal 00-Abnormal, if the user number does not exist, the user number returns 0xFF, 0xFF

**3.9 Get Fingerprint Data (0x09)**

This command is used by the device to obtain fingerprint data and send:

Table 3-19 Get fingerprint data

|  |  |  |  |
| --- | --- | --- | --- |
| Operation code | Operation parameters | | |
| 09 | Device ID | Lock ID | User number |
| 4 bytes | 1 byte | 2 bytes |

Return:

Table 3-20 Return status information

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Operation code | Operation parameters | | | |
| 09 | Device ID | Lock ID | User number | Fingerprint data |
| 4 bytes | 1 byte | 2 bytes | 512 bytes |

Note: If the fingerprint data does not exist, the returned fingerprint data is empty. If there is no such user number, return data exception instruction

**3.10 Get Unlock Information in the Lock (0x0A)**

This command word can also be used to obtain the latest unlocking information in the lock and send:

Table 3-21 Get unlocking information in the lock

|  |  |  |
| --- | --- | --- |
| Operation code | Operation parameters | |
| 0A | Device ID | Lock ID |
| 4 bytes | 1 byte |

Return:

Table 3-22 Return unlocking information in the lock

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Operation code | Operation parameters | | | | |
| 0A | Device ID | Lock ID | Unlocking user number | Time information | Unlocking method |
| 4 bytes | 1 byte | 2 bytes | 6 byte | 1 byte |

Description: Unlock user number (2 bytes) + unlock time (6 bytes, YY MM DD HH mm SS) + unlock method (1 byte, 01-remote 485, 02-swipe card, 03-Bluetooth, 04-switch, 05-fingerprint, 06-password, 07-abnormal), a total of 8 bytes. After each unlock, lift the handle to actively report an unlock information, followed by the heartbeat status.

**Issue Lock Unlock Time Period Permission (0x0B)**

This command word can also be used to send the lock unlocking time period authority:

Table 3-21 Send lock unlocking time period authority

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Operation code | Operation parameters | | | | | |
| 0B | Device ID | Lock ID | User number | Sequence number | Start time | End time |
| 4 bytes | 1 byte | 2 bytes | 2bytes | 6 bytes | 6 bytes |

Description: The time period sequence number: the current 10 periods, 0-9 periods, the time format is: YY MM DD HH mm SS, BCD format, delete the time period directly write 00, modify the time period directly overwrite the data. Delete the user, you can directly delete all time periods. AA BB 00 18 0B 01 02 03 04 01 00 01 00 01 23 06 19 15 47 00 23 06 20 15 47 00 04 EB

Return:

Table 3-10 Return status information

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Operation code | Operation parameters | | | |
| 0B | Device ID | Lock ID | User number | Status information |
| 4 bytes | 1 byte | 2 bytes | 1 byte |

Description: Status information: 01- Success 00- Unsuccessful, if the user number does not exist, the user number returns 0xFF, 0xFF, AA BB 00 0B 0B 01 02 03 04 01 00 01 01 42 1E

**Get Lock Unlock Time Period Record (0x0C)**

This command is used to read the lock unlocking time period record in the device and send:

Table 3-11 Read IC card number

|  |  |  |  |
| --- | --- | --- | --- |
| Operation code | Operation parameters | | |
| 0C | Device ID | Lock ID | User number |
| 4 bytes | 1 byte | 2 bytes |

AA BB 00 0A 0C 01 02 03 04 01 00 01 05 2F

Return:

Table 3-12 Return IC card number information

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Operation code | Operation parameters | | | | |
| 0C | Device ID | Lock ID | User number | Start time | End time |
| 4 bytes | 1 byte | 2 bytes | 6 bytes | 6 bytes |

If there is no such user number, return data exception instruction

This command is used to perform normally closed or normally open operations on the lock. Send:

Table 3-47 Unlock enable and disable operations

|  |  |  |  |
| --- | --- | --- | --- |
| Operation code | Operation parameters | | |
| 0D | Device ID | Lock ID | Operation parameters |
| 4 bytes | 1 byte | 1 byte |

Description: The operation parameters are as follows

00: Normally open AA BB 00 09 0D 01 02 03 04 01 00 7F DE

01: Normally closed AA BB 00 09 0D 01 02 03 04 01 01 5E CE

Return:

Table 3-48 Unlock enable command data return information

|  |  |  |  |
| --- | --- | --- | --- |
| Operation code | Operation parameters | | |
| 0D | Device ID | Lock ID | Status information |
| 4 bytes | 1 byte | 1 byte |

Description: Status: 01- Success 00- Unsuccessful

**Get Lock Normally Closed or Normally Open (0x0E)**

This command is used to perform normally closed or normally open operations on the lock. Send:

Table 3-47 Unlock enable and disable operations

|  |  |  |
| --- | --- | --- |
| Operation code | Operation parameters | |
| 0E | Device ID | Lock ID |
| 4 bytes | 1 byte |

AA BB 00 08 0E 01 02 03 04 01 BC E0

Return:

Table 3-48 Unlock enable command data return information

|  |  |  |  |
| --- | --- | --- | --- |
| Operation code | Operation parameters | | |
| 0E | Device ID | Lock ID | Status information |
| 4 bytes | 1 byte | 1 byte |

Description: The operating parameters are as follows AA BB 00 09 0E 01 02 03 04 01 00 FD 06

00: Normally open

01: Normally closed

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Operation code | Operation parameters | | | |  |  |  |  |
| 0B | Device ID | Lock ID | Event | Handle/door status  Status | Lock number  Number | User number  Number | Card number/password  Code/fingerprint | Time |
| 4 bytes | 1 byte | 2 bytes | 2byte | 8 byte | 2 bytes | 6 byte | 6byte |

Description: User is 00 when there is no user 00: Card number/password/fingerprint: Card number: 00 00 +4 bytes, write 00 if no card number,

Password: 6 bytes, write 00 if no password, Fingerprint: 00 00 00 00 00 +1 byte. Write 00 if no fingerprint, write 1 if fingerprint;

Event type:

|  |  |  |
| --- | --- | --- |
| 00 | 01 | Remote unlock success event |
| 00 | 02 | Card unlock success event |
| 00 | 03 | Bluetooth unlock success event |
| 00 | 04 | Switch unlock success event |
| 00 | 05 | Fingerprint unlock success event |
| 00 | 06 | Password unlock success event |
| 00 10 | | Lock closed event |
| 00 11 | | Lock opened event |
| 00 12 | | Door closed event |
| 00 13 | | Door opened event |
| 00 | 82 | Invalid card unlock failure event |
| 00 | 83 | Card invalid time period unlock failure |
| 00 | 84 | Invalid password unlock failure event |
| 00 | 85 | Password invalid time period unlock failure |
| 00 | 86 | Invalid fingerprint unlocking failure event |
| 00 | 87 | Unlocking failure during invalid fingerprint time period |

**3.11 Set Lock Time (0x10)**

This command is used to set the lock's own time to send:

Table 3-23 Set lock time

|  |  |  |  |
| --- | --- | --- | --- |
| Operation code | Operation parameter | | |
| 10 | Device ID | Lock ID | Time information |
| 4 bytes | 1 byte | 6 bytes |

Description: Modify the internal time of the lock, according to the lock reply and write format: YY MM DD HH mm SS, BCD format.

Return:

Table 3-24 Return information

|  |  |  |  |
| --- | --- | --- | --- |
| Operation code | Operation parameter | | |
| 10 | Device ID | Lock ID | Return status |
| 4 bytes | 1 byte | 1 byte |

Description: Return status: 01- Success 00- Unsuccessful

* 1. **Get Lock Time (0x11)**

This command is used to get the lock time send:

Return:

Table 3-25 Get device time command

|  |  |  |
| --- | --- | --- |
| Operation code | Operation parameter | |
| 11 | Device ID | Lock ID |
| 4 bytes | 1 byte |

Table 3-26 Get device time return

|  |  |  |  |
| --- | --- | --- | --- |
| Operation code | Operation parameter | | |
| 11 | Device ID | Lock ID | Time information |
| 4 bytes | 1 byte | 6 bytes |

Description: Time information is replied and written in the format of the lock: YY MM DD HH mm SS, BCD format.

* 1. **Modify Lock ID (0x12)**

This command is used to modify the ID number (station number) of a single lock. Send:

Table 3-27 Modify lock ID

|  |  |  |  |
| --- | --- | --- | --- |
| Operation code | Operation parameter | | |
| 12 | Device ID | Lock ID | Lock new ID |
| 4 bytes | 1 byte | 1 byte |

Return:

Table 3-28 Modify lock ID Return

|  |  |  |
| --- | --- | --- |
| Operation code | Operation parameter | |
| 12 | Device ID | Lock new ID |
| 4 bytes | 1 byte |

After modification, the lock needs to communicate according to the new ID (station number)

* 1. **Clear the Data Stored in the Lock (0x13)**

This command is used to clear various types of stored data in the lock send:

Table 3-29 Clear stored data in the lock

|  |  |  |  |
| --- | --- | --- | --- |
| Operation code | Operation parameter | | |
| 13 | Device ID | Lock ID | Storage data type |
| 4 bytes | 1 byte | 2 bytes |

Storage data type description:

1. Clear all unlock records: 00 01
2. Clear all card numbers in the lock: 00 02
3. Clear all passwords in the lock: 00 03
4. Clear all fingerprints in the lock: 00 04
5. Clear all users in the lock: 00 06

(5) is used for 867, (2)(3) is used for other models of smart locks Return:

Table 3-30 Clear the stored data in the lock Return value

|  |  |  |  |
| --- | --- | --- | --- |
| Operation code | Operation parameter | | |
| 13 | Device ID | Lock ID | Status information |
| 4 bytes | 1 byte | 1 byte |

Description: Status information: 01- Success 00- Unsuccessful

* 1. **Get Lock Function Information (0x14)**

This command is used to obtain the function information in the lock and send:

Table 3-31 Get lock function information

|  |  |  |
| --- | --- | --- |
| Operation code | Operation parameter | |
| 14 | Device ID | Lock ID |
| 4 bytes | 1 byte |

Description: Status information: 01- Success 00- Unsuccessful Return:

Table 3-32 Get lock function information Return

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Operation code | Operation parameter | | | | |
| 14 | Device ID | Lock ID | Hardware version number | Software version number | Lock function information |
| 4 bytes | 1 byte | 2 bytes | 2 bytes | 2 bytes |

Description:

Hardware version number: The high byte is used as the integer version number, and the low byte is used as the decimal version number. Software version number: The high byte is used as the integer version number, and the low byte is used as the decimal version number. Lock function information: The high byte is reserved

Low byte: 0 Bit: 485 Function

1. Bit: Card swipe function
2. Bit: Bluetooth function
3. Bit: Switch function
4. Bit: Fingerprint function
5. Bit: Password function

5th position: wifi function

Parameter bit 0---not available 1 Available

* 1. **Modify Device ID (0x15)**

This command is used to modify the device ID number. Send:

Table 3-33 Modify lock ID

|  |  |  |
| --- | --- | --- |
| Operation code | Operation parameter | |
| 15 | Device ID | New device ID |
| 4 bytes | 4 bytes |

Return:

Table 3-34 Modify lock ID information return

|  |  |  |
| --- | --- | --- |
| Operation code | Operation parameter | |
| 15 | New device ID | Status information |
| 4 bytes | 1 byte |

Description: Status information: 01- Success 00- Unsuccessful

* 1. **Poll Online Locks (0x16)**

This command is used to add a new lock to the bus, and the device actively polls the locks in the bus to send:

Table 3-35 Start polling

|  |  |  |
| --- | --- | --- |
| Operation code | Operation parameter | |
| 16 | Device ID | Operation information |
| 4 bytes | 1 byte |

Description: Operation information: 0x01 Return:

Table 3-36 Polling return information

|  |  |  |
| --- | --- | --- |
| Operation code | Operation parameter | |
| 16 | Device ID | Status information |
| 4 bytes | 1 byte |

Description: Status information: 01- Success 00- Unsuccessful

* 1. **Query Lock User Information (0x17)**

This command is used to query whether the user information already exists in the lock.

User group: If the number of users exceeds 200, they need to be grouped. Otherwise, they are processed as one group. For example, if the number of users is 180, it is one group. If the number of users is 300, it is divided into two groups, with 150 users in each group. The first group is 1-150, and the second group is 151-300.

Table 3-37 Query the user information in the lock

|  |  |  |  |
| --- | --- | --- | --- |
| Operation code | Operation parameter | | |
| 17 | Device ID | Lock ID | User group |
| 4 bytes | 1 byte | 1 byte |

Return:

Table 3-38 Query the user information in the lock

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Operation code | Operation parameter | | |  |
| 17 | Device ID | Lock ID | User group | User information |
| 4 bytes | 1 byte | 1 byte | 150 bytes |

Note: In the reply data, 1 byte in the user information represents one user, and 150 bytes represent 150 user information. Data 00 represents that the user does not exist, and 01 represents that the user number exists.

* 1. **Write IC Card Number to Lock (0x18) (for /865/864)**

This command is used to add IC card number, send:

Table 3-39 Write IC card number

|  |  |  |  |
| --- | --- | --- | --- |
| Operation code | Operation parameter | | |
| 18 | Device ID | Lock ID | IC card number |
| 4 bytes | 1 byte | 4 bytes |

Return:

Table 3-40 Return status information

|  |  |  |  |
| --- | --- | --- | --- |
| Operation code | Operation parameter | | |
| 18 | Device ID | Lock ID | Status information |
| 4 bytes | 1 byte | 1 byte |

Description: Status information: 01- Success 00- Unsuccessful

* 1. **Delete IC Card Number in Lock (0x19) (for /865/864)**

This command is used to delete IC card number, send:

Table 3-41 Delete IC card number

|  |  |  |  |
| --- | --- | --- | --- |
| Operation code | Operation parameters | | |
| 19 | Device ID | Lock ID | IC card number |
| 4 bytes | 1 byte | 4 bytes |

Table 3-42 Return status information

|  |  |  |  |
| --- | --- | --- | --- |
| Operation code | Operation parameters | | |
| 19 | Device ID | Lock ID | Status information |
| 4 bytes | 1 byte | 1 byte |

Description: Status information: 01- Success 00- Unsuccessful

* 1. **Read the Card Swipe Record in the Lock (0x20) (for /865/864)**

This command is used to read the card swipe record in the lock, send:

Table 3-43 Query the card swipe record in the lock

|  |  |  |
| --- | --- | --- |
| Operation code | Operation parameters | |
| 20 | Device ID | Lock ID |
| 4 bytes | 1 byte |

Return:

Table 3-44 Return status information

|  |  |  |  |
| --- | --- | --- | --- |
| Operation code | Operation parameters | | |
| 20 | Device ID | Lock ID | Data information |
| 4 bytes | 1 byte | 120 bytes |

Note: Each record consists of the card swipe sequence number (2 bytes) + IC card number (4 bytes), a total of 20 records, of which the latest one is at the front, and the rest are in the same order.

* 1. **Read the Authorized IC Card Number in the Lock (0x21) (for /865/864)**

This command is used to read the authorized IC card number in the lock, send:

Table 3-45 Query the user information of the lock

|  |  |  |
| --- | --- | --- |
| Operation code | Operation parameters | |
| 21 | Device ID | Lock ID |
| 4 bytes | 1 byte |

Return:

Table 3-46 Return status information

|  |  |  |  |
| --- | --- | --- | --- |
| Operation code | Operation parameters | | |
| 21 | Device ID | Lock ID | Data information |

|  |  |  |  |
| --- | --- | --- | --- |
|  | 4 bytes | 1 byte | 80 bytes |

Description: The data is: 20 4-byte IC card numbers. If the card number is less than 20, the extra data is 0xFF 0xFF 0XFF 0xFF

* 1. **Unlock Enable (0x22)**

This command is used to unlock, enable and disable the lock, send:

Table 3-47 Unlock enable and disable operations

|  |  |  |  |
| --- | --- | --- | --- |
| Operation code | Operation parameters | | |
| 22 | Device ID | Lock ID | Operation parameters |
| 4 bytes | 1 byte | 1 byte |

Description: The operation parameters are as follows

Enable: 01 The lock can be operated normally at this time

Disable: 00 At this time, the lock cannot be operated normally and can only be opened by a mechanical key. Return:

Table 3-48 Unlock enable command data return information

|  |  |  |  |
| --- | --- | --- | --- |
| Operation code | Operation parameters | | |
| 22 | Device ID | Lock ID | Status information |
| 4 bytes | 1 byte | 1 byte |

Description: Status: 01- Success 00- Unsuccessful

* 1. **Get Unlock Enable Information (0x23)**

This command is used to query the enable and disable status of the lock, send:

Table 3-49 Get unlock enable and disable status

|  |  |  |
| --- | --- | --- |
| Operation code | Operation parameters | |
| 23 | Device ID | Lock ID |
| 4 bytes | 1 byte |

Return:

Table 3-50 Unlock enable disable status return information

|  |  |  |  |
| --- | --- | --- | --- |
| Operation code | Operation parameters | | |
| 23 | Device ID | Lock ID | Status information |
| 4 bytes | 1 byte | 1 byte |

Description: The status information is as follows

Enable: 01 The lock can be operated normally at this time

Disable: 00 At this time, the lock cannot be operated normally and can only be opened by a mechanical key

* 1. **Single or Double User Verification Selection (0x24)**

This command is used to select single or double user authentication for the lock. Single user means that the lock can be unlocked after one user's permission is authenticated. Double user means that the lock can be unlocked after two users' permission are authenticated at the same time.

Send:

Table 3-51 Single and Double User Verification Selection

|  |  |  |  |
| --- | --- | --- | --- |
| Operation Code | Operation Parameters | | |
| 24 | Device ID | Lock ID | Select Parameters |
| 4 bytes | 1 byte | 1 byte |

Description: The selection parameters are as follows

Single User: 00 Dual User: 01 Multi-factor: 02

Return:

Table 3-52 Single and Double User Verification Command Data Return Information

|  |  |  |  |
| --- | --- | --- | --- |
| Operation Code | Operation Parameters | | |
| 24 | Device ID | Lock ID | Status |
| 4 bytes | 1 byte | 1 byte |

Description: Status: 01- Success 00- Unsuccessful

* 1. **Get Single or Double User Verification Information (0x25)**

This command is used to obtain single and double user verification operations on the device, send:

Table 3-53 Get Single and Double User Verification Information

|  |  |  |
| --- | --- | --- |
| Operation Code | Operation Parameters | |
| 25 | Device ID | Lock ID |
| 4 bytes | 1 byte |

Return:

Table 3-54 Get Single and Double User Verification Command Data Return Information

|  |  |  |  |
| --- | --- | --- | --- |
| Operation Code | Operation Parameters | | |
| 25 | Device ID | Lock ID | Data Information |
| 4 bytes | 1 byte | 1 byte |

Description: The data information is as follows

Single User: 00 Dual User: 01

Multi-factor: 02

* 1. **Lock Enters Remote Upgrade (0x26)**

This command is used to enter the IAP upgrade operation of the lock, send:

Table 3-55 Enter remote upgrade

|  |  |  |  |
| --- | --- | --- | --- |
| Operation Code | Operation Parameters | | |
| 26 | Device ID | Lock ID | Operation information |
| 4 bytes | 1 byte | 1 byte |

Description: The operation information is: enter IAP mode is 01, exit IAP mode is 02. Return:

Table 3-56 Enter remote upgrade command data return format

|  |  |  |  |
| --- | --- | --- | --- |
| Operation Code | Operation Parameters | | |
| 26 | Device ID | Lock ID | Status information |
| 4 bytes | 1 byte | 1 byte |

Description: Status information: 01- Success 00- Unsuccessful

* 1. **Device Enters Remote Upgrade (0x27)**

This command is used to enter the IAP upgrade operation of the device, send:

Table 3-57 Enter remote upgrade

|  |  |  |
| --- | --- | --- |
| Operation Code | Operation Parameters | |
| 27 | Device ID | Operation information |
| 4 bytes | 1 byte |

Description: The operation information is: enter IAP mode is 01. Return:

Table 3-58 Enter remote upgrade command data return format

|  |  |  |
| --- | --- | --- |
| Operation Code | Operation Parameters | |
| 27 | Device ID | Status information |
| 4 bytes | 1 byte |

Description: Status information: 01- Success 00- Unsuccessful

* 1. **Lock Model Register (0x28)**

This command is used to obtain the lock model, send:

Table 3-59 Get lock model

|  |  |  |
| --- | --- | --- |
| Operation Code | Operation Parameters | |
| 28 | Device ID | Lock ID |
| 4 bytes | 1 byte |

Return:

Table 3-60 Get lock model command data return information

|  |  |  |  |
| --- | --- | --- | --- |
| Operation Code | Operation Parameters | | |
| 28 | Device ID | Lock ID | Data |
| 4 bytes | 1 byte | 2 bytes |

Data: Read according to the BCD code of the lock model

DS865：08 65

DS864：08 64

DS867：08 67

DS713：07 13

DS712：07 12

DS403：04 03

DS887：08 07

DS888：08 08

* 1. **Get Device Information (0x29)**

This command is used to obtain the function information in the device and send:

Table 3-61 Get device function information

|  |  |
| --- | --- |
| Operation Code | Operation Parameters |
| 29 | Device ID |
| 4 bytes |

Return:

Table 3-62 Get device function information return

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Operation Code | Operation Parameters | | | |
| 29 | Device ID | Hardware version number | Software version number | Reserved bytes |
| 4 bytes | 2 bytes | 2 bytes | 2 bytes |

Return:

Hardware version number: high byte as integer version number, low byte as decimal version number  
Software version number: high byte as integer version number, low byte as decimal version number

* 1. **Device Parameter Setting (0X2A)**

Send:

Table 3-81 Parameter setting

Operation Parameters

Operation Code

|  |  |  |  |
| --- | --- | --- | --- |
| 2A | Device ID | Heartbeat time | Polling lock maximum station number |
| 4 bytes | 2 byte | 1 bytes |

Description: Heartbeat time: minimum unit s, default is 60s, hexadecimal transmission, such as 60s, send 0x00, 0x3c; Polling lock maximum station number: the number of polled devices, the default is 254, the maximum is 254;

Return:

Table 3-82 Parameter setting

|  |  |  |
| --- | --- | --- |
| Operation Code | Operation Parameters | |
| 2A | Device ID | Status information |
| 4 bytes | 1 bytes |

Description: Status information: 01-success 00-unsuccessful;

**3.31 Unlock duration setting (0X2B)**

Send:

Table 3-81 Parameter setting

|  |  |  |  |
| --- | --- | --- | --- |
| Operation Code | Operation Parameters | | |
| 2B | Device ID | Lock ID | Unlock duration |
| 4 bytes | 1 byte | 2byte |

Description: Heartbeat time: minimum unit s, default is 10s, hexadecimal sending, such as 10s, send 0x0A; return:

Table 3-82 Parameter setting

|  |  |  |  |
| --- | --- | --- | --- |
| Operation Code | Operation Parameters | |  |
| 2B | Device ID | Lock ID | Status information |
| 4 bytes | 1 byte | 1 bytes |

Description: Status information: 01-success 00-unsuccessful;

**3.31 Alarm duration setting (0X2C)**

Send:

Table 3-81 Parameter setting

|  |  |  |  |
| --- | --- | --- | --- |
| Operation Code | Operation Parameters | | |
| 2B | Device ID | Lock ID | Alarm duration |
| 4 bytes | 1 byte | 2byte |

Description: Heartbeat time: minimum unit s, default is 10s, hexadecimal sending, such as 10s, send 0x0A;

Return:

Table 3-82 Parameter setting

|  |  |  |  |
| --- | --- | --- | --- |
| Operation Code | Operation Parameters | |  |
| 2B | Device ID | Lock ID | Status information |
| 4 bytes | 1 byte | 1 bytes |

Description: Status information: 01-success 00-unsuccessful;

**3.31 Buzzer Switch Setting (0X2D)**

Send:

Table 3-81 Parameter setting

|  |  |  |  |
| --- | --- | --- | --- |
| Operation Code | Operation Parameters | | |
| 2B | Device ID | Lock ID |  |
| 4 bytes | 1 byte |  |

Description: Heartbeat time: minimum unit s, default is 10s, hexadecimal sending, such as 10s, send 0x0A; return:

Table 3-82 Parameter setting

|  |  |  |  |
| --- | --- | --- | --- |
| Operation Code | Operation Parameters | |  |
| 2B | Device ID | Lock ID | Status information |
| 4 bytes | 1 byte | 1 bytes |

Description: Status information: 01-success 00-unsuccessful;

**3.31 LED Switch Setting (0X2E)**

Send:

Table 3-81 Parameter setting

|  |  |  |  |
| --- | --- | --- | --- |
| Operation Code | Operation Parameters | | |
| 2B | Device ID | Lock ID |  |
| 4 bytes | 1 byte |  |

Description: Heartbeat time: minimum unit s, default is 10s, hexadecimal sending, such as 10s, send 0x0A; return:

Table 3-82 Parameter setting

|  |  |  |  |
| --- | --- | --- | --- |
| Operation Code | Operation Parameters | |  |
| 2B | Device ID | Lock ID | Status information |
| 4 bytes | 1 byte | 1 bytes |

Description: Status information: 01-success 00-unsuccessful;

* 1. **Set Device Local IP (0x30)**

This command sets the local IP of the device, the default IP is 192.168.1.254 Send:

Table 3-63 Set local IP

|  |  |  |
| --- | --- | --- |
| Operation Code | Operation Parameters | |
| 30 | Device ID | Local IP |
| 4 bytes | 4 bytes |

Description: The local IP information uses hexadecimal, such as 192.168.1.254. Return:

Table 3-64 Return status information

|  |  |  |
| --- | --- | --- |
| Operation Code | Operation Parameters | |
| 30 | Device ID | Status information |
| 4 bytes | 1 byte |

Description: Status information: 01- Success 00- Unsuccessful

* 1. **Get Device Local IP (0x31)**

This command gets the local IP of the device, the default IP is 192.168.1.254 Send:

Table 3-65 Get local IP

|  |  |  |
| --- | --- | --- |
| Operation Code | Operation Parameters | |
| 31 | Device ID | Operation Parameters |
| 4 bytes | 1 byte |

Description: Operation parameter 01 returns:

Table 3-65 Return local IP information

|  |  |  |
| --- | --- | --- |
| Operation Code | Operation Parameters | |
| 31 | Device ID | Local IP |
| 4 bytes | 4 bytes |

Note: Local IP information uses hexadecimal.

* 1. **Set Target IP and Port (0x32)**

This command sets the target IP of the device, the default IP is 192.168.1.201 Send:

Table 3-67 Set target IP

|  |  |  |  |
| --- | --- | --- | --- |
| Operation Code | Operation Parameters | |  |
| 32 | Device ID | Target IP | Target port number |
| 4 bytes | 4 bytes | 2 bytes |

Note: Target IP information uses hexadecimal. For example, 192.168.1.201. Return:

Table 3-68 Return status information

|  |  |  |
| --- | --- | --- |
| Operation Code | Operation Parameters | |
| 32 | Device ID | Status information |
| 4 bytes | 1 byte |

Description: Status information: 01- Success 00- Unsuccessful

* 1. **Get Target IP (0x33)**

This command gets the device target IP, the default IP is 192.168.1.201 Send:

Table 3-69 Get target IP

|  |  |  |
| --- | --- | --- |
| Operation Code | Operation Parameters | |
| 33 | Device ID | Operation Parameters |
| 4 bytes | 1 byte |

Description: Operation parameter 01 returns:

Table 3-70 Return local IP information

|  |  |  |
| --- | --- | --- |
| Operation Code | Operation Parameters | |
| 33 | Device ID | Target IP |
| 4 bytes | 4 bytes |

Note: The target IP information is in hexadecimal.

* 1. **Set the Device Target Port Number (0x34)**

This command sets the target port number of the device. The default port number is 8234. Send:

Table 3-71 Set target IP

|  |  |  |
| --- | --- | --- |
| Operation Code | Operation Parameters | |
| 34 | Device ID | Target port number |
| 4 bytes | 2 bytes |

Description: The target port information is in hexadecimal. For example, 8234, the data is 20 2A. Return:

Table 3-72 Return status information

Operation Parameters

Operation Code

|  |  |  |
| --- | --- | --- |
| 34 | Device ID | Status information |
| 4 bytes | 1 byte |

Description: Status information: 01- Success 00- Unsuccessful

* 1. **Get Device Port Number (0x35)**

This command obtains the target port number of the device. The default port number is 8234. Send:

Table 3-73 Get device port number

|  |  |  |
| --- | --- | --- |
| Operation Code | Operation Parameters | |
| 35 | Device ID | Operation Parameters |
| 4 bytes | 1 byte |

Description: Description: Operation parameter 01

Table 3-74 Return port number information

|  |  |  |
| --- | --- | --- |
| Operation Code | Operation Parameters | |
| 35 | Device ID | Target port number |
| 4 bytes | 2 bytes |

Description: The target port information is in hexadecimal. For example, 8234, the data is 20 2A. Return:

**3.41 Data Abnormality (0xFF)**

This command is used to send data. When the lock return format is incorrect or the data is abnormal, the return data is returned:

Table 3-83 Data abnormality

|  |  |  |  |
| --- | --- | --- | --- |
| Operation Code | Operation Parameters | | |
| FF | Device ID | Lock ID | Error message |
| 4 bytes | 1 byte | 2 bytes |

Description: Error information is 0xFF, 0xFF 0xFF 0X01: Data exception

0xFF 0X02: User password/card number already exists

0xFF 0X03: No user

0xFF 0X04: Data out of range

0xFF 0X05: Data timeout