MR79Serial Bluetooth Communication Protocol

V1.13

（2023.01.04）

SHENZHEN MARKTRACE CO., LTD

Index

Change Doc Record 3
1. Scope of protocol 4
2. Required instructions 4
3. Instruction frame format 5
   3.1 Data frame format sent by upper device to MR7901 5
   3.2 Data frame format of MR7901 response to upper device 5
4. Command definition 6
   4.1 Reset the device 0x21 7
   4.2 Get version information 0x22 8
   4.3 Set system configuration parameters 0x13 9
   4.4 Get system configuration parameters 0x14 11
   4.5 Get tag data 0x18 14
   4.6 Set Bluetooth output tag data identification 0x19 16
   4.7 Get Bluetooth output tagl data identification 0x20 17
   4.8 Get the number of tag records 0x25 18
   4.9 Set transmission tag record identification 0x26 19
   4.10 Get transmission tag record identification 0x27 20
   4.11 Get GPRS signal strength 0x0C 21
   4.12 Get antenna information 0x28 22
   4.13 Get device number 0x 24 23
   4.14 Get GPRS module IMEI 0x15 24
   4.15 Set device RTC time 0x16 25
   4.16 Get device RTC time 0x17 26
   4.17 Get the IP and port of the current GPRS connection 0x29 27
   4.18 Get the IP and port of the current LAN connection 0x2B 28
   4.19 Host firmware upgrade 0x31/0x32/0x33 29
   4.20 Tag search 0x2A 32
   4.21 Get device hardware information 0x07 38
   4.22 Set working mode 0x51 40
   4.23 Query the current working mode 0x52 41
   4.24 Query test results 0x53 43
   4.25 Bluetooth password verification 0x0A 47
   4.26 Set APN related parameters 0x62 47
   4.27 Query APN related parameters 0x63 47
5. System configuration parameter format description 63
6. Tag format description 65
   6.1 4bytes Tag format description 65
7. Command summary 67
8. Opcode summary 69
9. Checksum algorithm 69
   9.1 Checksum algorithm 69

1, Change Document Record

SN	Ver	Data	Changes	Compiler
1	Org	2016.11.28	Original To V1.6	Chuangbao Wang
2	V1.7	2020.05.09	English Version	Edward Lee
3	V1.13	20230104	Delete the unsupported Bluetooth commands (such as MQTT related commands, etc.) in the MR7901P V1.50 firmware version	Chuangbao Wang & Edward Lee

1. Scope of protocol

Provide a reference for engineers to complete the communication between MR7901 and Bluetooth app or serial terminal software. (this protocol suites for all MR79xx products, the sample model in this document is MR7901)

2. Required instructions

- Baud rate between MR7901 and Bluetooth is 9600;
- Upper device means Bluetooth APP
- Device/Terminal means RFID reader include MR7901P/MR7901K/MR7902
- The antenna numbers 1, 2, 3, and 4 correspond to the four directions of east, south, west, and north, respectively.

3.Instruction frame format

3.1 Data frame format sent by upper device to MR7901

The instruction frame is composed of frame header, address code (not used), frame length, instruction code, data, and checksum, all expressed in hexadecimal.
The specific structure is defined as follows:

eg: Set time 0A FF 08 16 10 0B 01 02 00 00 BB

sof	addr	len	cmd	data[0]	data[1]	data[2]	data[3]	data[4]	data[5]	checksum
0A	FF	08	16	10	0B	01	02	00	00	BB

sof : 0x0A
addr : 0xFF (not used)
len : 0x08
cmd : 0x16
data : 10 0B 01 02 00 00 (Year, Month, Day, Hour, Second) The corresponding time is 02:00:00 November 1, 2016.
checksum: 0xBB

Explanation:

1. The instruction data length len is composed of cmd, data, checksum;
2. checksum is the sum check of sof + addr + len + cmd + data. For the calculation algorithm, please refer to the checksum of section 9.

3.2 Data frame format of MR7901 response to upper device

The response frame is composed of frame header, instruction code, frame length, operation code, data, and checksum, all expressed in hexadecimal. The specific structure is defined as follows:

eg: Response of Set time 0B 16 02 00 DD

sof	cmd	len	opt	checksum
0B	16	02	00	DD

sof : 0x0B
cmd : 0x16
len : 0x02
opt : 0x00 (The operation is successful, that is, the set time is successful)
data : none
checksum: 0xDD

Explanation:

1. The instruction data length len is composed of cmd, data, checksum;

2. checksum is the sum check of sof + cmd + len + opt + data. For the calculation algorithm, please refer to the checksum of section 9.

4. Command definition

4.1 Reset the device 0x21

Reset the device

Note：

Before resetting the device, the tag records in the cache will be saved to external flash (supported by V2.9 or above).

4.1.1 Command frame definition

Reset device command.

cmd： 0x21

data： none

eg：0A FF 02 21 D4

sof	addr	len	cmd	checksum
0A	FF	02	21	D4

sof : 0x0A

addr : 0xFF

len : 0x02

cmd : 0x21

data : none

checksum: 0xD4

4.1.2 Response frame definition

After receiving this command, the device restarts immediately.

cmd : 0x21

data : none

eg： 0B 21 02 00 D2

sof	cmd	len	opt	checksum
0B	21	02	00	D2

sof : 0x0B

cmd : 0x21

len : 0x02

opt : 0x00 (Successful operation)

data : none

checksum: 0xD2

4.2 Get version information 0x22

Read device firmware version information

4.2.1 Command frame definition

Obtain the firmware version and time information of firmware release.

cmd： 0x22

data： none

eg：0A FF 02 22 D3

sof	addr	len	cmd	checksum
0A	FF	02	22	D3

sof : 0x0A

addr : 0xFF

len : 0x02

cmd : 0x22

data : none

checksum: 0xD3

4.2.2 Response frame definition

cmd : 0x22

data : Firmware version + time of firmware release

eg： 0B 22 18 00 02 07 4A 61 6E 20 31 31 20 32 30 31 37 2C 31 34 3A 34 31 3A 30 36 5D

sof	cmd	len	opt	data[0] version(M)	data[1] version(S)			
0B	22	18	00	2	7	4A('J')	61('a')	6E('n')
20(' ')	31('1')	31('1')	20(' ')	32('2')	30('1')	31('1')	37('7')	2C(',')
								checksum
31('1')	34('4')	3A(':')	34('4')	31('1')	3A(':')	30('0')	36('6')	5D

sof : 0x0B

cmd : 0x22

len : 0x18

opt : 0x00 (Successful operation)

data : 02 07 Firmware version V2.7 (master version number 2, slave version 7)

4A 61 6E 20 31 31 20 32 30 31 37 2C 31 34 3A 34 31 3A 30 36

Firmware release time Jan 11 2017, 14:41:06

checksum: 0x5D

4.3 Set system configuration parameters 0x13

Configure the system parameters of MR7901.

4.3.1 Command frame definition

After receiving this command, the device saves the configuration parameters, and then resets and restarts.

Note：

Before the device restarts, it will clear the tags saved in the external flash (V2.9 version or above).

cmd ： 0x13

data ： System configuration parameters

eg： 0A FF B8 13 55 01 02 09 01 00 B4 00 34 33 35 35 31 30 33 30 30 33 45 30 30 33 39 00 00 00 01 C0 A8 01 C7 FF FF FF 00 C0 A8 01 01 64 00 32 31 38 2E 31 37 2E 31 35 37 2E 32 31 34 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 F8 11 32 31 38 2E 31 37 2E 31 35 37 2E 32 31 34 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 F8 11 00 51 7F 3E 00 39 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 06 01 06 01 06 FF FF 10 4D 52 37 39 30 31 2D 30 30 33 45 30 30 33 39 00 A8 A8 A8 A8 1F 1F 1F 1F 00 A1 00 05 00 00 10

sof	addr	len	cmd	data[0] initial flag		checksum
0A	FF	B8	13	55	…	10

sof : 0x0A

addr : 0xFF

len : 0xB8

cmd : 0x13

data : none

data : （Please refer to Table 1 for specific format description）

55 : 1. The 5th byte in the frame, the parameter characteristic value, when reading the configuration parameter, it is fixed at 0x55

01 : 2. The 6th byte in the frame, the working mode is: GPRS transmission, and the tag records are transmitted to the platform. (Definition of the lower four digits: 0x01: GPRS 0x02: LAN)

02 09 : 3. Starting from the 7th byte in the frame, firmware version V2.9 (main version number 2, from version 9)

01 : 4. The 9th byte in the frame, buzzer identification, turn on the buzzer (0x00: off, 0x01: on)

01 : 5. The 10th byte in the frame, reserved 1

B4 00 : 6. Starting at the 11th byte in the frame, the tag filter time is 0x00B4, which is 180 seconds. (Low byte first, high byte second), Judgment time for leaving base station in V3.0 and above

34 33 35 35 31 30 33 30 30 33 45 30 30 33 39 00 : 7. Starting at the 13th byte in

the frame, the device ID, "4355103003E0039"

00 00 : 8. Starting at the 29th byte in the frame, the 0x0000 base station stay timing reporting function is disabled (V3.3 version)

01 : 9. The 31st byte in the frame, DHCP is enabled (0x00: off, 0x01: on, for LAN)

C0 A8 01 C7 : 10. Starting at the 32nd byte in the frame, LAN local IP, 192.168.1.199

FF FF FF 00 : 11. Starting at the 36th byte in the frame, LAN subnet mask 255.255.255.0

C0 A8 01 01 : 12. Starting at the 40th byte in the frame, the LAN gateway 192.168.1.1

64 00 : 13. Starting at the 44th byte in the frame, LAN local IP port 0x0064, which is 100 (low byte first, high byte second)

32 31 38 2E 31 37 2E 31 35 37 2E 32 31 34 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 : 14. Starting at the 46th byte in the frame, the IP of GPRS server 1, "218.17.157.214", platform IP (balanced server address)

F8 11 : 15. Starting at the 78th byte in the frame, the port of GPRS server 1, 0x11F8 is 4600 (low byte first, high byte second), platform port

32 31 38 2E 31 37 2E 31 35 37 2E 32 31 34 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 : 16. Starting at the 80th byte in the frame, the IP of LAN server 1, "218.17.157.214", platform IP (balanced server address)

F8 11 : 17. Starting at the 112th byte in the frame, the port of LAN server 1, 0x11F8, which is 4600 (low byte first, high byte second)

00 51 7F 3E 00 39 : 18. Starting at the 114th byte in the frame, LAN local MAC address 00-51-7F-3E-00-39

00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 : 19. Starting at the 120th byte in the frame, reserved 3

01 06 01 06 01 06 FF FF : 20. Starting from the 148th byte in the frame, the antenna firmware version corresponds to the firmware version of antennas 1 to 4 respectively. Each antenna version occupies 2 bytes. When it is FF FF, it means that reading the antenna version failed. That is, the firmware versions of antennas 1 to 4 are: V1.6, V1.6, V1.6, none (Failed to read antenna 4, the antenna may not be connected to channel 4)

10 : 21. The 156th byte in the frame, GPRS signal strength 0x10 (16)

4D 52 37 39 30 31 2D 30 30 33 45 30 30 33 39 00: 22. Starting at the 157th byte in the frame, the device number is "MR7901-003E0039"

A8 A8 A8 A8 : 23. Starting at the 173rd byte in the frame, the rssi filtering thresholds for antennas 1, 2, 3, and 4 are -88dBm, -88dBm, -88dBm, -88dBm

1F 1F 1F 1F : 24. Starting at the 177th byte in the frame, the gains of antennas 1, 2, 3, and 4 are 31 dBm, 31 dBm, 31 dBm, and 31 dBm, respectively

00 : 25. The 181st byte in the frame, the Bluetooth output tag flag, 0x00 does not output the tag, 0x01 outputs the tag

A1 : 26. The 182th byte in the frame, the communication connection status, 0xA1: the device has established a communication connection with the platform through GPRS (if it is 0xA2: the device and the platform have established a communication connection through the LAN, 0xA3: the device and the platform communicate through GPRS and LAN connection)

00 : 27. The 183th byte in the frame, turn off tag direction judgment filtering

05 : 28. The 184th byte in the frame, the filter interval for tag direction judgment is 5 seconds

00 00 : 29. Starting at the 185th byte in the frame, reserve 4

checksum : 0x10

4.3.2 Response frame definition

After receiving this command, the device restarts immediately.

cmd : 0x13

data : none

eg: 0B 13 02 00 E0

sof	cmd	len	opt	checksum
0B	13	02	00	E0

sof : 0x0B

cmd : 0x13

len : 0x02

opt : 0x00 (Successful operation, Failure is 0x80)

data : none

checksum: 0xE0

4.4 Get system configuration parameters 0x14

Get device system parameters.

4.4.1 Command frame definition

Get device system parameters.

cmd : 0x14

data : none

eg: 0A FF 02 14 E1

sof	addr	len	cmd	checksum
0A	FF	02	14	E1

sof : 0x0A

addr : 0xFF
len : 0x02
cmd : 0x14
data : none
checksum: 0xE1

4.4.2 Response frame definition

cmd : 0x14
data : Configuration parameters + firmware version + firmware release time
eg: 0B 14 CE 00 55 01 02 09 01 00 B4 00 34 33 35 35 31 30 33 30 30 33 45 30 30 33 39 00 00 00 01 C0 A8 01 C7 FF FF FF 00 C0 A8 01 01 64 00 32 31 38 2E 31 37 2E 31 35 37 2E 32 31 34 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 F8 11 32 31 38 2E 31 37 2E 31 35 37 2E 32 31 34 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 F8 11 00 51 7F 3E 00 39 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 06 01 06 01 06 FF FF 10 4D 52 37 39 30 31 2D 30 30 33 45 30 30 33 39 00 A8 A8 A8 A8 1F 1F 1F 1F 00 A1 00 05 00 00 02 09 41 70 72 20 31 30 20 32 30 31 37 2C 31 31 3A 32 34 3A 31 31 94

sof	cmd	len	opt	data[0] initial flag		checksum
0B	14	CE	00	55	...	94

sof : 0x0B
cmd : 0x14
len : 0xCE
opt : 0x00 (Successful operation)
data : （Please refer to Table 1 for specific format description）

55 : 1. The 5th byte in the frame, the parameter characteristic value, when reading the configuration parameter, it is fixed at 0x55

01 : 2. The 6th byte in the frame, the working mode is: GPRS transmission, and the tag records are transmitted to the platform. (Definition of the lower four digits: 0x01: GPRS 0x02: LAN)

02 09 : 3. Starting from the 7th byte in the frame, firmware version V2.9 (main version number 2, from version 9)

01 : 4. The 9th byte in the frame, buzzer identification, turn on the buzzer (0x00: off, 0x01: on)

01 : 5. The 10th byte in the frame, reserved 1

B4 00 : 6. Starting at the 11th byte in the frame, the tag filter time is 0x00B4, which is 180 seconds. (Low byte first, high byte second), Judgment time for leaving base station in V3.0 and above

34 33 35 35 31 30 33 30 30 33 45 30 30 33 39 00 : 7.Starting at the 13th byte in the frame, the device ID, "4355103003E0039"

00 00 : 8. Starting at the 29th byte in the frame, the 0x0000 base station stay timing reporting function is disabled (V3.3 version)

01 : 9. The 31st byte in the frame, DHCP is enabled (0x00: off, 0x01: on, for

LAN)

C0 A8 01 C7 : 10. Starting at the 32nd byte in the frame, LAN local IP, 192.168.1.199

FF FF FF 00 : 11. Starting at the 36th byte in the frame, LAN subnet mask 255.255.255.0

C0 A8 01 01 : 12. Starting at the 40th byte in the frame, the LAN gateway 192.168.1.1

64 00 : 13. Starting at the 44th byte in the frame, LAN local IP port 0x0064, which is 100 (low byte first, high byte second)

32 31 38 2E 31 37 2E 31 35 37 2E 32 31 34 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 : 14. Starting at the 46th byte in the frame, the IP of GPRS server 1, "218.17.157.214", platform IP (balanced server address)

F8 11 : 15.Starting at the 78th byte in the frame, the port of GPRS server 1, 0x11F8 is 4600 (low byte first, high byte second), platform port

32 31 38 2E 31 37 2E 31 35 37 2E 32 31 34 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 : 16. Starting at the 80th byte in the frame, the IP of LAN server 1, "218.17.157.214", platform IP (balanced server address)

F8 11 : 17. Starting at the 112th byte in the frame, the port of LAN server 1, 0x11F8, which is 4600 (low byte first, high byte second)

00 51 7F 3E 00 39 : 18. Starting at the 114th byte in the frame, LAN local MAC address 00-51-7F-3E-00-39

00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 : 19. Starting at the 120th byte in the frame, reserved 3

01 06 01 06 01 06 FF FF : 20. Starting from the 148th byte in the frame, the antenna firmware version corresponds to the firmware version of antennas 1 to 4 respectively. Each antenna version occupies 2 bytes. When it is FF FF, it means that reading the antenna version failed. That is, the firmware versions of antennas 1 to 4 are: V1.6, V1.6, V1.6, none (Failed to read antenna 4, the antenna may not be connected to channel 4)

10 : 21. The 156th byte in the frame, GPRS signal strength 0x10 (16)

4D 52 37 39 30 31 2D 30 30 33 45 30 30 33 39 00: 22. Starting at the 157th byte in the frame, the device number is "MR7901-003E0039"

A8 A8 A8 A8 : 23. Starting at the 173rd byte in the frame, the rssi filtering thresholds for antennas 1, 2, 3, and 4 are -88dBm, -88dBm, -88dBm, -88dBm

1F 1F 1F 1F : 24.Starting at the 177th byte in the frame, the gains of antennas 1, 2, 3, and 4 are 31 dBm, 31 dBm, 31 dBm, and 31 dBm, respectively

00 : 25. The 181st byte in the frame, the Bluetooth output tag flag, 0x00 does not output the tag, 0x01 outputs the tag

A1 : 26. The 182th byte in the frame, the communication connection status, 0xA1: the device has established a communication connection with the platform through GPRS (if it is 0xA2: the device and the platform have established a communication connection through the

LAN, 0xA3: the device and the platform communicate through GPRS and LAN connection)

00 : 27. The 183th byte in the frame, turn off tag direction judgment filtering

05 : 28. The 184th byte in the frame, the filter interval for tag direction judgment is 5 seconds

00 00 : 29. Starting at the 185th byte in the frame, reserve 4

02 09 : 30. Starting from the 187th byte in the frame, firmware version V2.9 (main version number 2, from version 9)

41 70 72 20 31 30 20 32 30 31 37 2C 31 31 3A 32 34 3A 31 31 : 31. The 189th byte in the frame starts, the firmware is released on Apr 10 2017, 11:24:11

checksum : 0x99

4.5 Get tag data 0x18

Get a tag record in the buffer.

Note:

1. When calling this function command, it will automatically set the "Bluetooth output tag identification" to the output tag status (value 1)
2. If the "Bluetooth output tag identification" is not 0, the tag will not be uploaded to the platform.

4.5.1 Command frame definition

cmd : 0x18

data : None or the tag ID you want to read

1. Read tags without filtering

eg1: 0A FF 02 18 DD (no filter)

sof	addr	len	cmd	checksum
0A	FF	02	18	DD

sof : 0x0A

addr : 0xFF

len : 0x02

cmd : 0x18

data : none

checksum: 0xDD

2. Read tags and output the specified tag ID only

eg2: 0A FF 06 18 12 34 56 78 C5 （Filter tags and only output tag records with tag number 12 34 56

78）

sof	addr	len	cmd	data[0]	data[1]	data[2]	data[3]	checksum
0A	FF	06	18	12	34	56	78	C5

sof : 0x0A
addr : 0xFF
Len : 0x06
cmd : 0x18
data : 12 34 56 78 : Output tag records with tags 12 34 56 78 only
checksum: 0xC5

4.5.2 Response frame definition

cmd : 0x18
data : When there is a tag, return one tag record

1. When there is a tag record:

eg1: 0B 18 15 00 01 20 12 34 56 78 CC 20 20 00 D4 10 0B 18 0B 2C 07 01 11 30 （When there is a tag, or when you need to search for a tag）

sof	cmd	len	opt	data[0]				
0B	18	15	00	01	20	12	34	56
78	CC	20	20	00	D4	10	0B	18
					checksum			
0B	2C	07	01	11	30			

sof : 0x0B
cmd : 0x18
len : 0x15
opt : 0x00 (Successful operation)
Data : 01 : Antenna channel number, tag read by antenna 1 (value range 1 to 4, corresponding to antenna east, south, north, and north)
20 12 34 56 78 CC 20 20 00 D4 : Tag data, please refer to the description of tag data format in Chapter 6
10 0B 18 0B 2C 07 : Tag recording time, corresponding to year, month, day, hour, minute, and second respectively, the year is based on 2000, that is, the time is November 24, 2016 11:44:07
01 11 : The number of records in the device buffer is 0x0111, high byte first.
checksum: 0x30

2. When there is no tag record:

eg2 : 0B 18 02 06 D5

sof	cmd	len	opt	checksum
0B	18	02	06	D5

sof : 0x0B
cmd : 0x18
len : 0x02
opt : 0x06 (no tag record)
data : none
checksum: 0xD5

4.6 Set Bluetooth output tag data identification 0x19

Turn on or off the Bluetooth output tag data enable identify.

Note：

1. If the "Bluetooth output tag identity" is not 0, the tag will not be uploaded to the platform;
2. After the device is reset, the default "Bluetooth output tag identity" is 0.

The Bluetooth output label identity is defined as follows：

SN	Bluetooth output identity value	Application scenario
1	0	Power-on default value, tag data is uploaded to the platform
2	1	When Bluetooth reads tag data (cmd = 0x18), it is automatically set to 1; when exiting Bluetooth to read the tag number, you need to set this value to 0.
3	2	When the Bluetooth search tag (cmd = 0x2A), it is automatically set to 2; when exiting, it is automatically set to 0

4.6.1 Command frame definition

cmd： 0x19
data： Enable flag 0: Off, 1: Bluetooth output tag data, 2: Bluetooth output tag data automatically.
eg： 0A FF 03 19 00 DB

sof	addr	len	cmd	data[0]	checksum
0A	FF	03	19	00	DB

sof : 0x0A
addr : 0xFF
len : 0x03
cmd : 0x19
data : 00 : Turn off the Bluetooth output tag data
checksum: 0xDB

4.6.2 Response frame definition

cmd : 0x19

data : none

eg： 0B 19 02 00 DA

sof	cmd	len	opt	checksum
0B	19	02	00	DA

sof : 0x0B

cmd : 0x19

len : 0x02

opt : 0x00 (no tag record)

data : none

checksum: 0xDA

4.7 Get Bluetooth output tag data identification 0x20

Get the Bluetooth output tag data enable identification.

4.7.1 Command frame definition

cmd： 0x20

data： none

eg： 0A FF 02 20 D5

sof	addr	len	cmd	checksum
0A	20	02	20	D5

sof : 0x0A

addr : 0xFF

len : 0x02

cmd : 0x20

data : none

checksum: 0xD5

4.7.2 Response frame definition

cmd : 0x20

data : Bluetooth output tag data enable identification. 0: Off, 1: Bluetooth output tag data, 2: Bluetooth output tag data automatically.

eg： 0B 20 03 00 00 D2

sof	cmd	len	opt	data[0]	checksum
0B	20	03	00	00	D2

sof : 0x0B
cmd : 0x20
len : 0x03
opt : 0x00 (Successful operation)
data : 00 Bluetooth output tag identification is off
checksum: 0xD2

4.8 Get the number of tag records 0x25

Get the number of tag records in the device buffer (the number of wireless transmission buffer tags, the number of wired transmission buffer tags, and the number of filtered buffer tags (or the number of tags used for pre-judgment)).

4.8.1 Command frame definition

cmd： 0x25
data： none
eg：0A FF 02 25 D0

sof	addr	len	cmd	checksum
0A	FF	02	25	D0

sof : 0x0A
addr : 0xFF
Len : 0x02
cmd : 0x25
data : none
checksum: 0xD0

4.8.2 Response frame definition

cmd : 0x25
data : Number of tag records
eg1： 0B 25 04 00 00 81 49 (V2.7 ， V2.6 version)

sof	cmd	len	opt	data[0]	data[1]	checksum
0B	25	04	00	00	81	4B

sof : 0x0B
cmd : 0x25
len : 0x04
opt : 0x00 (Successful operation)
data : 00 81 : Number of tag records in wireless transmission buffer 0x0081 (high byte first)
checksum: 0x4B

eg2: 0B 25 08 00 00 04 03 E8 04 68 6D （V2.8 version or above）

sof	cmd	len	opt	data[0]	data[1]	data[2]	data[3]	data[4]	data[5]	checksum
0B	25	08	00	00	04	03	E8	04	68	6D

sof : 0x0B
cmd : 0x25
len : 0x08
opt : 0x00 (Successful operation)
data : 00 04 03 E8 04 68
00 04 : Number of tag records in wireless transmission buffer 0x0004 (high byte first)
03 E8 : Number of tag records in wired transmission buffer 0x03E8 (high byte first)
04 68: Number of tag records in the filter cache (or pre-judge cache) 0x0468 (high byte first)
checksum: 0x6D

4.9 Set transmission tag record identification 0x26

Enable identification of set whether device transmits tag records to the platform

note：

1. After this identification is set, it will be saved in flash and will not be lost after reset
2. Transmit the tag record identification, the factory default is 0: upload the tag record to the platform;

4.9.1 Command frame definition

cmd： 0x26
data： Identification of device transfer data to platform 0: transmit, 1: do not transmit
eg： 0A FF 03 26 01 CD

sof	addr	len	cmd	data[0]	checksum
0A	FF	3	26	01	CD

sof : 0x0A
addr : 0xFF
len : 0x03
cmd : 0x26
data : 01 :)Whether to upload tag records to the platform (0x00: upload tags to the platform, 0x01 does not upload tags to the platform)
checksum: 0xCD

4.9.2 Response frame definition

cmd : 0x26

data： none

eg： 0B 26 02 00 CD

sof	cmd	len	opt	checksum
0B	26	02	00	CD

sof : 0x0B

cmd : 0x26

len : 0x02

opt : 0x00 (Successful operation)

data : none

checksum: 0xCD

4.10 Get transmission tag record identification 0x27

Get enable identification of whether transfer tag records to platform

4.10.1 Command frame definition

cmd： 0x27

data： none

eg： 0A FF 02 27 CE

sof	addr	len	cmd	checksum
0A	FF	02	27	CE

sof : 0x0A

addr : 0xFF

len : 0x02

cmd : 0x27

data : none

checksum: 0xCE

4.10.2 Response frame definition

cmd： 0x27

data： Identification of device transfer data to platform 0: transmit, 1: do not transmit

eg： 0B 27 03 00 01 CA

sof	cmd	len	opt	data[0]	checksum
0B	27	03	00	01	CA

sof : 0x0B

cmd : 0x27

len : 0x03

opt : 0x00 (Successful operation)

data : 01 : Not upload tag records to the platform (0x00: upload tags to the platform, 0x01 does

not upload tags to the platform)

checksum: 0xCA

4.11 Get GPRS signal strength 0x0C

Get GPRS signal strength

Note：

1. When the device contains a GPRS module, the signal strength of the GPRS module can be obtained;
2. 20 seconds after starting, when the signal strength is 99, it means there is no GPRS module;
3. The normal range of GPRS signal strength is 0 to 31.

4.11.1 Command frame definition

Reset device command.

cmd ： 0x0C

data ： none

eg：0A FF 02 0C E9

sof	addr	len	cmd	checksum
0A	FF	02	0C	E9

sof : 0x0A

addr : 0xFF

len : 0x02

cmd : 0x0C

data : none

checksum: 0xE9

4.11.2 Response frame definition

cmd : 0x0C

data : The signal strength of the gprs module

eg： 0B 0C 03 00 17 CF

sof	cmd	len	opt	data[0]	checksum
0B	0C	03	00	17	CF

sof : 0x0B

cmd : 0x0C

len : 0x03

opt : 0x00 (Successful operation)

data : 17 : GPRS signal strength is 0x17 (23)

checksum: 0xD2

4.12 Get antenna information 0x28

Get the current antenna information of the device (antenna gain, rssi threshold, antenna firmware version).

Note:

To obtain the antenna information, the antenna must be connected to the device before device is powered on; If the antenna is connected after the device works normally, the information of this antenna cannot be read.

4.12.1 Command frame definition

cmd： 0x28

data： none

eg：0A FF 02 28 CD

sof	addr	len	cmd	checksum
0A	FF	02	28	CD

sof : 0x0A

addr : 0xFF

len : 0x02

cmd : 0x28

data : none

checksum: 0xCD

4.12.2 Response frame definition

cmd : 0x28

data : Antenna version + gain + rssi threshold

eg： 0B 28 12 00 01 03 01 03 01 03 FF FF 1F 1F 1F FF A8 A8 A8 01 5C

sof	cmd	len	opt	data[0]				
0B	28	12	00	01	03	01	03	01
03	FF	FF	1F	1F	1F	FF	A8	A8
		checksum						
A8	01	5C						

sof : 0x0B

cmd : 0x0C

len : 0x12

opt : 0x00 (Successful operation)

data :

01 03 01 03 01 03 FF FF : 4 antenna firmware versions (each antenna version occupies 2 bytes)

Antenna 1: Version is V1.3

Antenna 2: Version is V1.3
Antenna 3: Version is V1.3
Antenna 4: No version information is obtained (the reason may be that the antenna is not connected)

1F 1F 1F FF : 4 antenna gain values (value range 0 to 31, FF is invalid)
Antenna 1：31dBm
Antenna 2：31dBm
Antenna 3：31dBm
Antenna4： Not obtained (it may be that the antenna is not connected)

A8 A8 A8 01 : 4 antenna signal strength rssi filtering threshold (Value range -1 ～ -128, 1 is invalid value)
Antenna 1：-88dBm
Antenna 2：-88dBm
Antenna 3：-88dBm
Antenna 4： Not obtained (it may be that the antenna is not connected)

checksum : 0x5C

4.13 Get device number 0x 24

This number is the device model number MR7901 + MCU, which has a certain uniqueness.

4.13.1 Command frame definition

cmd： 0x24
data： none
eg： 0A FF 02 24 D1

sof	addr	len	cmd	checksum
0A	FF	02	24	D1

sof : 0x0A
addr : 0xFF
Len : 0x02
cmd : 0x24
data : none
checksum: 0xD1

4.13.2 Response frame definition

cmd : 0x24
data : device number

eg： 0B 24 12 00 4D 52 37 39 30 31 2D 30 30 33 43 30 30 32 35 00 85

sof	cmd	len	opt	data[0]				
0B	24	12	00	4D	52	37	39	30
31	2D	30	30	33	43	30	30	32
		checksum						
35	00	85						

sof : 0x0B

cmd : 0x24

len : 0x12

opt : 0x00 (Successful operation)

data :

4D 52 37 39 30 31 2D 30 30 33 43 30 30 32 35 00 : Device number (string) "MR7901-003C0025"

checksum : 0x85

4.14 Get GPRS module IMEI 0x15

Get the IEMI number of the GPRS module (this command is only valid when there is a GPRS module and a SIM card is installed).

4.14.1 Command frame definition

cmd： 0x15

data： none

eg： 0A FF 02 15 E0

sof	addr	len	cmd	checksum
0A	FF	02	15	E0

sof : 0x0A

addr : 0xFF

len : 0x02

cmd : 0x15

data : none

checksum: 0xE0

4.14.2 Response frame definition

cmd : 0x15

data : IMEI number of the gprs module

eg： 0B 15 12 00 38 36 31 36 39 34 30 33 34 32 30 35 38 39 36 00 B7

sof	cmd	len	opt	data[0]				
0B	15	12	00	38	36	31	36	39

34	30	33	34	32	30	35	38	39

		checksum
36	00	B7

sof : 0x0B
cmd : 0x15
Len : 0x12
opt : 0x00 (Successful operation)
data :

38 36 31 36 39 34 30 33 34 32 30 35 38 39 36 00 : IMEI number (string)
"861694034205896"

checksum: 0xB7

4.15 Set device RTC time 0x16

Set device RTC time

4.15.1 Command frame definition

cmd： 0x16
data： none
eg： 0A FF 08 16 10 0B 01 09 00 00 B4

sof	addr	len	cmd	data[0]	data[1]	data[2]	data[3]	data[4]	data[5]	checksum
0A	FF	8	16	10	0B	01	09	00	00	B4

sof : 0x0A
addr : 0xFF
Len : 0x08
cmd : 0x16
data : 10 0B 01 09 00 00 : The set time corresponds to the year, month, day, hour, minute, and second, and the start time of the year is 2000（2016.11.01,9:00:00）
checksum: 0xB4

4.15.2 Response frame definition

cmd : 0x16
data : none
eg： 0B 16 02 00 DD

sof	cmd	len	opt	checksum
0B	16	02	00	DD

sof : 0x0B
cmd : 0x16
len : 0x02

opt : 0x00 (Successful operation)
data : none
checksum: 0xDD

4.16 Get device RTC time 0x17

Get device RTC time

4.16.1 Command frame definition

cmd： 0x17
data： none
eg： 0A FF 02 17 DE

sof	addr	len	cmd	checksum
0A	FF	02	17	DE

sof : 0x0A
addr : 0xFF
len : 0x02
cmd : 0x17
data : none
checksum: 0xDE

4.16.2 Response frame definition

cmd : 0x17
data : device RTC time
eg：0B 17 08 00 11 01 0B 17 01 04 9D

sof	cmd	len	opt	data[0]	data[1]	data[2]	data[3]	data[4]	data[5]	checksum
0B	17	8	00	11	01	0B	17	01	04	9D

sof : 0x0B
cmd : 0x17
Len : 0x08
opt : 0x00 (Successful operation)
data : 11 01 0B 17 01 04 : RTC time, corresponding to the year, month, day, hour, minute and second, the starting time of the year is 2000（2017.01.11, 23:01:04）
checksum: 0x9D

4.17 Get the IP and port of the current GPRS connection 0x29

Get the IP , port and status of the current GPRS connection

4.17.1 Command frame definition

cmd： 0x29

data： none

eg： 0A FF 02 29 CC

sof	addr	len	cmd	checksum
0A	FF	02	29	CC

sof : 0x0A

addr : 0xFF

len : 0x02

cmd : 0x29

data : none

checksum: 0xCC

4.17.2 Response frame definition

cmd : 0x29

data : GPRS connection server IP, port, connection status

eg：0B 2A 25 00 32 31 38 2E 31 37 2E 31 35 37 2E 32 31 34 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 94 11 01 3F

sof	cmd	len	opt	data[0] IP(MSB)	data[1]	data[2]	data[3]	data[4]
0B	29	25	00	32	31	38	2E	31
37	2E	31	35	37	2E	32	31	34
	...	data[31] IP (LSB)	data[32] port(L)	data[33] port(H)	data[34] link status	checksum		
00	...	00	94	11	01	3F		

sof : 0x0B

cmd : 0x29

len : 0x25

opt : 0x00 (Successful operation)

data : 32 31 38 2E 31 37 2E 31 35 37 2E 32 31 34 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

00 00 : Server IP of current GPRS connection “218.17.157.214”

94 11 : Connect port 0x1194, which is 4500, low byte first.

01 : Connection status (0x01: has established a link connection, 0x00: no connection)

checksum: 0x3F

4.18 Get the IP and port of the current LAN connection 0x2B

Get the IP , port and status of the current LAN connection

4.18.1 Command frame definition

cmd： 0x2B

data： none

eg： 0A FF 02 2B CB

sof	addr	len	cmd	checksum
0A	FF	02	2B	CB

sof : 0x0A

addr : 0xFF

Len : 0x02

cmd : 0x2B

data : none

checksum: 0xCB

4.18.2 Response frame definition

cmd : 0x2B

data : LAN connection IP, port, connection status

eg1：0B 2B 25 00 32 31 38 2E 31 37 2E 31 35 37 2E 32 31 34 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 24 13 01 AC

sof	cmd	len	opt	data[0] IP(MSB)	data[1]	data[2]	data[3]	data[4]
0B	2B	25	00	32	31	38	2E	31
37	2E	31	35	37	2E	32	31	34
	...	data[31] IP (LSB)	data[32] port(L)	data[33] port(H)	data[34] link status	checksum		
00	...	00	24	13	01	AC		

sof : 0x0B

cmd : 0x2B

len : 0x25

opt : 0x00 (Successful operation)

data : 32 31 38 2E 31 37 2E 31 35 37 2E 32 31 34 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 : IP of current GPRS connection “218.17.157.214”

24 13 : The server port is 0x1324, which is 4900, with the low byte first.

01 : Connection status (0x01: has established a link connection, 0x00: no connection)

checksum: 0xAC

eg2：0B 2B 02 80 48

sof	cmd	len	opt	checksum
0B	2B	02	80	48

sof : 0x0B

cmd : 0x2B

len : 0x02

opt : 0x80 (The operation failed, the device does not support the lan function)

data : none

checksum: 0x48

4.19 Host firmware upgrade 0x31/0x32/0x33

4.19.1 Upgrade process

1. Upgrade starts, send upgrade file size

The Bluetooth app sends the command code 0x31 to the device, The data field is the size of the upgrade file; The device receives the 0x31 command and the format is correct, responding to the 0x00 status to the Bluetooth app; After receiving 0x00, the Bluetooth app enters the next step;

eg:

app send : 0A FF 06 31 00 00 60 A0 C0

app receive : 0B 31 02 00 C2

2. Send upgrade file content

The Bluetooth app sends the command code 0x32 to the device. The data field is the content of the upgrade file and the effective length is 64Bytes (the last packet is not less than 64Bytes, filled with 0) The device receives the 0x32 command and the format is correct, responding to the 0x00 status to the Bluetooth app; After receiving 0x00, the Bluetooth app enters the next step;

eg:

app send : 0A FF 42 32 58 3D 00 20 A1 4E 00 08 9D 31 00 08 9F 31 00 08 A3 31 00 08 A7 31 00 08 AB 31 00 08 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 AF 31 00 08 B1 31 00 08 00 00 00 00 B3 31 00 08 89 7E 00 08 BC

app receive : 0B 32 02 00 C1

3. End of upgrade

Bluetooth app sends command code 0x33 to the device;

After the device receives the 0x33 command and responds to the Bluetooth app with a status of 0x00, the device resets and runs on the new firmware

After the Bluetooth app receives 0x00, the upgrade process ends.

eg:

app send : 0A FF 02 33 C2

app receive : 0B 33 02 00 C0

4.19.2 Upgrade starts 0x31

1. Command frame definition：

cmd ： 0x31

data： length of upgrade file

eg： 0A FF 06 31 00 00 60 A0 C0

sof	addr	len	cmd	data[0]	data[1]	data[2]	data[3]	checksum
0A	FF	06	31	00	00	60	A0	C0

sof : 0x0A

addr : 0xFF

len : 0x06

cmd : 0x31

data : 00 00 60 A0 size of upgrade file： 0x000060A0(24736) Bytes (High byte first)

checksum: 0xC0

2. Response frame definition：

cmd : 0x31

data : none

eg： 0B 31 02 00 C2

sof	cmd	len	opt	checksum
0B	31	02	00	C2

sof : 0x0B

cmd : 0x31

len : 0x02

opt : 0x00 (Successful operation)

data : none

checksum: 0xC2

4.19.3 Send upgrade file content 0x32

The fixed length of the data field is 64Bytes, the last packet is less than 64Btyes filled with 0.

1. Command frame definition：

cmd ： 0x32

data： content of update file

eg： 0A FF 42 32 58 3D 00 20 A1 4E 00 08 9D 31 00 08 9F 31 00 08 A3 31 00 08 A7 31 00 08 AB 31 00 08 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 AF 31 00 08 B1 31 00 08 00 00 00 00 B3 31 00 08 89 7E 00 08 BC

sof	addr	len	cmd	data[0]	…	data[63]	checksum
0A	FF	42	32	58	…	08	BC

sof : 0x0A

addr : 0xFF

len : 0x06

cmd : 0x32

data : 58 3D 00 20 A1 4E 00 08 9D 31 00 08 9F 31 00 08 A3 31 00 08 A7 31 00 08 AB 31 00 08 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 AF 31 00 08 B1 31 00 08 00 00 00 00 B3 31 00 08 89 7E 00 08 content of update file

checksum: 0xBC

2. Response frame definition：

cmd： 0x32

data： none

eg： 0B 32 02 00 C1

sof	cmd	len	opt	checksum
0B	32	02	00	C1

sof : 0x0B

cmd : 0x32

Len : 0x02

opt : 0x00 (Successful operation)

data : none

checksum: 0xC1

4.19.4 End of upgrade 0x33

1. Command frame definition：

cmd： 0x33

data： none

eg： 0A FF 02 33 C2

sof	addr	len	cmd	checksum
0A	FF	02	33	C2

sof : 0x0A

addr : 0xFF

len : 0x02

cmd : 0x33

data : none

checksum: 0xC2

2. Response frame definition：

cmd : 0x33

data : none

eg： 0B 33 02 00 C0

sof	cmd	len	opt	checksum
0B	33	02	00	C0

sof : 0x0B

cmd : 0x33

len : 0x02

opt : 0x00 (Successful operation)

data : none

checksum: 0xC0

4.20 Tag search 0x2A

Bluetooth automatically outputs the tag data read by the device（MR7901）.

4.20.1 Bluetooth app operation process

1. When you click "Tag Search"
   a. Send the "Enable tag output without filtering" command to the device: 0A FF 04 2A 01 00 C8
   b. Device response：0B 2A 03 00 01 C7
   c. After the device responds to the Bluetooth app, it will automatically output the tag information
      eg: one tag data 02 30 34 30 41 32 30 31 36 31 30 46 35 32 37 39 45 30 30 30 30 30 30 44 35 31 44 0D 0A ， in string "_040A201610F53095000000E111"
   eg:
      app send : 0A FF 04 2A 01 00 C8
      app receive : 0B 2A 03 00 01 C7
      app receive : 02 30 34 30 41 32 30 31 36 31 30 46 35 32 37 39 45 30 30 30 30 30 30 44 35 31 44 0D 0A
   ....

2. When leaving (exiting) "Tag Search ",
   a. Send the command "Close tag output, clear filter tag" to the device: 0A FF 04 2A 00 01 C8
   b. Device response：0B 2A 03 00 00 C8
   c. After the device responds to the app, it stops outputting the tag information.
   eg:
      app send : 0A FF 04 2A 00 01 C8
      app receive : 0B 2A 03 00 00 C8

3. ”When you click the confirmation button of "Deployment Data", send "Add Filter Tag" After adding the filter tag, the device only outputs the tag data of the control.
   eg1 : add filter 16 10 01 79
   0A FF 08 2A 02 00 16 10 01 79 23
   device response：0B 2A 03 00 02 C6
   eg2 ： add filter 16 10 01 79 and 16 10 9C 3B
   0A FF 0C 2A 02 00 16 10 01 79 16 10 9C 3B 22
   device response：0B 2A 03 00 02 C6

4. When you click "Mode Search-Patrol",
   Note：
   You can switch between "Search" and "Patrol" modes only after adding filter tags
   1>. Patrol (no filtering), then send the command: 0A FF 04 2A 01 00 C8
   device response： 0B 2A 03 00 01 C7
   2>. Search (filter), then send the command: 0A FF 04 2A 01 01 C7
   device response：0B 2A 03 00 01 C7

4.20.2 Command frame definition

The search tag command determines different functions by carrying parameters. The parameters are "Stop search", "Start search, but not filter output", "Start search, filter output".

cmd ： 0x2A

data ： The first byte of the data field indicates:

0x00 ： Stop search
0x01 ： Start search, but not filter output
0x02 ： Start search, filter output

1. Stop searching tags, clear filter tags

After receiving this command, the device will stop outputting tags to Bluetooth and clear the tag id used for filtering.

eg1：0A FF 04 2A 00 01 C8

sof	addr	len	cmd	data[0]	data[1]	checksum
0A	FF	04	2A	00	01	C8

sof : 0x0A
addr : 0xFF
len : 0x04
cmd : 0x2A
data : 00 01
0x00: Stop searching tags (Bluetooth will stop outputting tag data)
0x01: Clear filter tag
checksum: 0xC8

2. Stop searching tags without clearing filter tags

After receiving this command, the device will stop outputting tags to Bluetooth, and the tag id used for filtering will not be cleared.

eg2：0A FF 04 2A 00 00 C9

sof	addr	len	cmd	data[0]	data[1]	checksum
0A	FF	04	2A	00	00	C9

sof : 0x0A

addr : 0xFF

len : 0x04

cmd : 0x2A

data : 00 01

0x00: Stop searching tags (Bluetooth will stop outputting tag data)

0x00: Do not clear filter tag

checksum: 0xC9

3. Search tags without filtering output

After receiving this command, the device will output all tag data to Bluetooth.

eg3：0A FF 04 2A 01 00 C8

sof	addr	len	cmd	data[0]	data[1]	checksum
0A	FF	04	2A	01	00	C8

sof : 0x0A

addr : 0xFF

len : 0x04

cmd : 0x2A

data : 01 00

0x01 : start tag search

0x00 : Without filtering, directly output all read tag data

checksum: 0xC8

4. Search tags, filter output

After receiving this command, the device will output the read filter tag data to Bluetooth.

Note：

he premise of this command must be that the filter tag has been added;

eg4：0A FF 04 2A 01 01 C7

sof	addr	len	cmd	data[0]	data[1]	checksum
0A	FF	04	2A	01	01	C7

sof : 0x0A

addr : 0xFF

len : 0x04
cmd : 0x2A
data : 01 00
0x01 : start tag search
0x01 : Use filtering, Output filter tag data
checksum: 0xC7

5. Add filter tags

The total number of filtered tags does not exceed 512, and a maximum of 62 tags are set for each frame of data. If the filtered tags are greater than 62, sub-packaging is required.

Note:

1. The total number of filter tags is not more than 512;
2. After receiving this command, the device will output only the tag data in the filter tag;
3. The tag ID is 4Btyes.

eg5: 0A FF 0C 2A 02 00 16 10 01 79 16 10 9C 3B 22 （deploy 6 10 01 79 and 16 10 9C 3B two tags）

sof	addr	len	cmd	data[0]	data[1]	data[2]	data[3]	data[4]
0A	FF	0C	2A	02	00	16	10	01
data[5]	**data[6]**	**data[7]**	**data[8]**	**data[9]**	checksum			
79	16	10	9C	3B	22			

sof : 0x0A
addr : 0xFF
len : 0x0C
cmd : 0x2A
data : 02 00 16 10 01 79 16 10 9C 3B
data[0] : 02 : Add filter tags;
data[1] : 00 : The serial number of the tag search package, Since a maximum of 62 tags are transmitted in a single data frame, more than 62 tags need to be transmitted in multiple frames;
data[1] <= 9, Filter tag can be set up to 62 *8 + 16*1 = 512

16 10 01 79 16 10 9C 3B : Tag id to search， That is, only tags with tag IDs of 16 10 01 79 and 16 10 9C 3B are output.

checksum: 0x22

4.20.3 Response frame definition

cmd : 0x2A
data : ccording to different parameters, different

1. Stop searching tags, clear filter tags response

eg1：0B 2A 03 00 00 C8

sof	cmd	len	opt	data[0]	checksum
0B	2A	03	00	00	C8

sof : 0x0B
cmd : 0x2A
len : 0x03
opt : 0x00 (Successful operation)
data : 0x00 : stop tag search
checksum: 0xC8

2. Stop searching for tags without clearing the filter tag response

eg2：0B 2A 03 00 00 C8

sof	cmd	len	opt	data[0]	checksum
0B	2A	03	00	00	C8

sof : 0x0B
cmd : 0x2A
len : 0x03
opt : 0x00 (Successful operation)
data : 0x00 : stop tag search
checksum: 0xC8

3. Search tags without output response filtering

eg3：0B 2A 03 00 01 C7

sof	cmd	len	opt	data[0]	checksum
0B	2A	03	00	01	C7

sof : 0x0B
cmd : 0x2A
len : 0x03
opt : 0x00 (Successful operation)
data : 0x01 : start tag search
checksum: 0xC7

4. Search tags, filter output response

Note：

1>. The premise of this command must be that the filter tag has been added;

2>. After the device sends this message, it will only output the tag data in the filter tag.

eg4：0B 2A 03 00 01 C7

sof	cmd	len	opt	data[0]	checksum
0B	2A	03	00	01	C7

sof : 0x0B

cmd : 0x2A
len : 0x03
opt : 0x00 (Successful operation)
data : 0x01 : start tag search
checksum: 0xC7

5. Add filter tag response

After the device sends this message, it will only output the tag data in the filter tag.

eg5：0B 2A 03 00 02 C6

sof	cmd	len	opt	data[0]	checksum
0B	2A	03	00	02	C6

sof : 0x0B
cmd : 0x2A
len : 0x03
opt : 0x00 (Successful operation)
data : 0x02 : Add filter tags
checksum: 0xC6

6. Tag output

If "tag search " is enabled and the device has tag data that needs to be sent, this tag data packet is output to Bluetooth

	SOF	Addr	Len	Data	Check	EOF
Len（Byte）	1	2	2	n	2	2
content	02					0D 0A

Explanation：

1. The SOF and EOF fields are fixed at 0x02 and 0x0D 0x0A, and the other fields are expressed in ASCII code;
2. SOF ： Length is 1Byte, fixed at 0x02 (Hex)
3. Addr : length is 2Bytes, which is expressed in ASCII (The address here is the antenna number,
4. East South West North, corresponding to numbers 1, 2, 3, 4);
5. Len ： The length is 2Btyes, which is expressed in ASCII, indicating the length of the Data field;
6. Data : The length is determined by Len, which is expressed in ASCII and is the tag data;
7. Check: The length is 2Byes, which is the hexadecimal checksum of the Addr, len field, and Data field (accumulated by bytes, inverted, plus 1);
8. EOF : The length is 2Byte, fixed at 0x0D 0x0A.

Note: Hexadecimal numbers, when expressed in ASCII, high nibble first, low nibble second.
（eg： 0x31, in ASCII is 0x33 0x31）

eg6.

02 30 31 30 41 32 30 39 39 38 38 37 37 36 36 45 32 30 30 30 30 30 31 41 38 34 43 0D 0A

Explanation1：

02 : SOF

30 31 : Addr, 0x01 in hex;

30 41 : Len, 0x0A in hex，That is, the length of the Data field is 10Btyes；

32 30 39 39 38 38 37 37 36 36 45 32 30 30 30 30 30 31 41 38 : Data， 20 99 88 in hex 77 66 E2 00 00 01 a8， tag data, For format description, please see Chapter 6 "6. Tag Format Description"

34 43 : Check, 0x4C in hex，is the checksum (hex) of len and data that is the checksum of 01 0A 20 99 88 77 66 E2 00 00 01 a8 (Accumulate by byte, invert, add 1)；

0D 0A : EOF

Explanation2：

Addr + Len + Data + Check , transfer to hex as follow:

01 0A 20 99 88 77 66 E2 00 00 01 A8 4C

4.21 Get device hardware information 0x07

Device hardware information include Device ID, device number (factory number), lower 15 digits of MCU UUID, IMEI number of GPRS module, CCID behind the sim card, battery power, device power supply status, etc.

4.21.1 Command frame definition

cmd： 0x05

data： none

eg：0A FF 02 07 EE

sof	addr	len	cmd	checksum
0A	FF	02	07	EE

sof : 0x0A

addr : 0xFF

len : 0x02

cmd : 0x07

data : none

checksum: 0xEE

4.21.2 Response frame definition

After receiving this message, the device will report the device's current hardware information (total 127Bytes)

SN	Data segment	Bytes	Description

1	Current device ID cur_device_id	16	String, the ID used in the current communication packet header, the last byte is 0
2	Hardware ID mcu_device_id	16	String, the last byte is 0
3	Produce SN product_sn	16	String, the last byte is 0
4	GPRS module IMEI gprs_imei	16	String, the last byte is 0
5	Sim CCID sim_ccid	21	String, the last byte is 0
6	Battery power battery_level	1	Value, value range: 0 ~ 10, 10 means that the power is 100%
7	external power identification power_link_status	1	Value, 0: external power supply is normal, 1: external power supply is disconnected
8	Reserved reserved	40	reserved

cmd： 0x07

data： device hardware info

eg：0B 07 81 00 31 33 36 35 31 31 35 30 30 32 34 30 30 33 32 00 31 33 36 35 31 31 35 30 30 32 34 30 30 33 32 00 4D 52 37 39 30 31 4B 2D 30 32 34 30 30 33 32 00 38 36 32 36 33 31 30 33 36 34 39 30 38 31 30 00 38 39 38 36 30 32 62 31 31 39 31 36 39 30 30 30 32 33 32 39 00 0A 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 F7

sof	cmd	len	opt	data[0]	…	data[126]	checksum
0B	07	81	00	31	…	00	F7

sof : 0x0B

cmd : 0x07

len : 0x81

opt : 0x00 (Successful operation)

data :

cur_device_id : 31 33 36 35 31 31 35 30 30 32 34 30 30 33 32 00 1. “136511500240032” （Start at the 5th byte in the frame）

mcu_device_id : 31 33 36 35 31 31 35 30 30 32 34 30 30 33 32 00 2. “136511500240032” （Start at the 21st byte in the frame）

product_sn : 4D 52 37 39 30 31 4B 2D 30 32 34 30 30 33 32 00 3. “MR7901K-0240032” （Start at the 37th byte in the frame）

gprs_imei: 38 36 32 36 33 31 30 33 36 34 39 30 38 31 30 00 4. “862631036490810” （Start at the 53rd byte in the frame）

sim_ccid : 38 39 38 36 30 32 62 31 31 39 31 36 39 30 30 30 32 33 32 39 00 5. “898602b1191690002329” （Start at the 69th byte in the frame）

battery_level : 0A 6. battery power 100%（Start at the 90th byte in the frame）

power_link_status : 00 7. external power connected（Start at the 91st byte in the frame）

reserved : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 8. reserved（Start at the 92nd byte in the frame）

checksum: 0xF7

4.22 Set working mode 0x51

When you need to test the device or exit the test mode, use this command to configure the device.

After the device is turned on, the default is: normal working mode.

This command is used in conjunction with 0x52 (query current mode) and 0x53 (query test result).

4.22.1 Command frame definition

cmd： 0x51

data： Setting mode of device

Data field description：

Field	Bytes	Explanation
mode	1	**0x00** —— Normal mode **0x01** —— Testing mode
tag_id	4	Tag ID to be tested (high byte first), only testing mode is valid
m_rssi	1	Value range (-1 ~ -128), only testing mode is valid
s_rssi	1	Value range (-1 ~ -128), only testing mode is valid
timeout	2	Unit: second (≥ 10) (high byte first), only testing mode is valid

eg1：0A FF 0B 51 01 16 10 F4 BD D8 D3 00 78 A0

sof	addr	len	cmd	data[0] mode	data[1] tag_id(MSB)	data[2]	data[3]	data[4] tag_id(LSB)
0A	FF	0B	51	01	16	10	F4	BD

data[5] m_rssi	data[6] s_rssi	data[7] timeout(MSB)	data[8] timeout(LSB)	checksum
D8	D3	00	78	A0

sof : 0x0A

addr : 0xFF

len : 0x0B

cmd : 0x51

data : 01 16 10 F4 BD D8 D3 00 78

mode : 01 Set the device into "testing mode"

tag_id	: 16 10 F4 BD Tag ID for testing (high byte first)
m_rssi	: D8 The threshold rssi of the master antenna is -40
s_rssi	: D3 The threshold rssi of the slave antenna is -45
timeout	: 00 78 he timeout period is 0x0078, 120 seconds (High byte first)

checksum: 0xA0

eg2：0A FF 03 51 00 A3

sof	addr	len	cmd	data[0] mode	checksum
0A	FF	03	51	00	A3

sof : 0x0A
addr : 0xFF
len : 0x03
cmd : 0x51
data : 00 ： mode = 0x00, Set the device to enter "normal mode"
checksum: 0xA3

4.22.2 Response frame definition

After receiving this message, the device directly responds to the received command, and then sets the mode to the antenna.

cmd : 0x51
data : none
eg： 0B 51 02 00 A2

sof	cmd	len	opt	checksum
0B	51	02	00	A2

sof : 0x0B
cmd : 0x51
len : 0x02
opt : 0x00 (Successful operation)
data : none
checksum: 0xA2

4.23 Query the current working mode 0x52

Query the current device mode and antenna working mode.

Note：

After receiving this command, the device first responds antenna working mode that read previously, and then sends a command to read the current working mode of the antenna. Therefore, after sending this command, wait for 5 seconds and read it again to get the latest antenna working mode.

4.23.1 Command frame definition

cmd： 0x52
data： none

eg：0A FF 02 52 A3

sof	addr	len	cmd	checksum
0A	FF	02	52	A3

sof : 0x0A
addr : 0xFF
len : 0x02
cmd : 0x52
data : none
checksum: 0xA3

4.23.2 Response frame definition

After receiving this message, the device first responds to the current device mode and the previously antenna mode, and then asks the device to query the antenna working mode again.

cmd : 0x52
data : Working mode of main unit + working mode of 4 antennas

Data field description：

Field	Bytes	Explanation
Device current mode	1	**0x00** —— Normal mode **0x01** —— Testing mode
Antenna working mode	4	Corresponding to 1,2,3,4 (East, South, West, North) The working modes of the four antennas are described as follows: **0x00** —— Normal mode

		0x01 —— Testing mode **0xFF** —— Failed

eg： 0B 52 07 00 01 01 01 01 FF 9F

sof	cmd	len	opt	data[0]	data[1]	data[2]	data[3]	data[4]	checksum
0B	52	07	00	01	01	01	01	FF	9F

sof : 0x0B

cmd : 0x52

len : 0x07

opt : 0x00 (Successful operation)

data : 01 01 01 01 FF

01 : The current working mode of the device is testing mode

01 01 01 FF : The current working modes of the four antennas are

01: Antenna 1: Testing mode

01: Antenna 2: Testing mode

01: Antenna 3: Testing mode

FF: Antenna 4, Get failed

checksum: 0x9F

4.24 Query test results 0x53

Used with command codes 0x51 (setting working mode) and 0x18 (getting tag data), it can realize the function test of the device.

4.24.1 Command frame definition

cmd： 0x53

data： none

eg： 0A FF 02 53 A2

sof	addr	len	cmd	checksum
0A	FF	02	53	A2

sof : 0x0A

addr : 0xFF

len : 0x02

cmd : 0x53

data : none

checksum: 0xA2

4.24.2 Response frame definition

Upload the current device gprs / wired network status.

cmd : 0x53

data : Current device gprs / wired network status (total 46 bytes)

Data field description：(total 46 bytes）

SN	Field	Bytes	Explanation
1	Test Results	1	**0x00** —— Test failed **0x01** —— Test ok **0x02** —— On testing **0x03** —— Non testing mode
2	Connection status with platform	1	The high 4 digits are fixed at A, and the lower digits indicate the network connection status,among them Bit 0: GPRS connection, 1 valid Bit 1: Wired network connection, 1 valid eg: **0xA0** —— no connect **0xA1** —— GPRS connected **0xA3** —— GPRS/wired connected
3	Connection status of GPRS TCP	1	**1 :** connected， **0 :** disconnected
4	Connection status of wired TCP	1	**1 :** connected， **0 :** disconnected
5	GPRS rssi	1	Value range: 0 ～ 31, 99 (If it is 99, the GPRS module does not work normally)
6	Antenna firmware version	8	Corresponding to the firmware version of antennas 1 to 4 respectively If it is "FF FF", it means that the version of the antenna is not read
7	Antenna gain	4	Corresponding to the gains of antennas 1 to 4 (value range 0 to 31) If it is FF, it means that the gain of the antenna is not read
8	Antenna rssi	4	Corresponding to the rssi of antennas 1 to 4 (value range -1 to -128) If it is 1, it means that the rssi of the antenna is not read
9	Device current mode	1	**0x00** —— Normal mode **0x01** —— Testing mode
10	Antenna work mode	4	Corresponding to the working modes of four antennas (1,2,3,4 (east, south, west, north) respectively, the values are explained as follows:

			0x00 —— Normal mode **0x01** —— Testing mode **0xFF** ——The current mode of the antenna is not read
11	The master antenna rssi threshold during testing	1	For Single byte, range （-10 ～ -128）, Only testing mode is valid
12	The slave antenna rssi threshold during testing	1	For Single byte, range （-10 ～ -128）, Only testing mode is valid
13	Test results of Antenna 1 (East) master antenna	1	Only testing mode is valid **0x00** —— Test failed **0x01** —— Test ok **0xFF** —— Test tag not read
14	RSSI of of Antenna 1 (East) master antenna	1	For Single byte, range （-10 ～ -128）, Only testing mode is valid
15	Test results of Antenna 1 (East) slave antenna	1	Only testing mode is valid **0x00** —— Test failed **0x01** —— Test ok **0xFF** —— Test tag not read
16	RSSI of of Antenna 1 (East) slave antenna	1	For Single byte, range （-10 ～ -128）, Only testing mode is valid
17	Test results of Antenna 2 (South) master antenna	1	Only testing mode is valid **0x00** —— Test failed **0x01** —— Test ok **0xFF** —— Test tag not read
18	RSSI of Antenna 2 (South) master antenna	1	For Single byte, range （-10 ～ -128）, Only testing mode is valid
19	Test results of Antenna 2 (South) slave antenna	1	Only testing mode is valid **0x00** —— Test failed **0x01** —— Test ok **0xFF** —— Test tag not read
20	RSSI of Antenna 2 (South) slave antenna	1	For Single byte, range （-10 ～ -128）, Only testing mode is valid
21	Test results of Antenna 3 (West) master antenna	1	Only testing mode is valid **0x00** —— Test failed **0x01** —— est ok **0xFF** —— Test tag not read
22	RSSI of Antenna 3 (West) master antenna	1	For Single byte, range （-10 ～ -128）, Only testing mode is valid
23	Test results of Antenna 3 (West) slave antenna	1	Only testing mode is valid **0x00** —— Test failed **0x01** —— Test ok **0xFF** —— Test tag not read
24	RSSI of Antenna 3 (West) slave antenna	1	For Single byte, range （-10 ～ -128）, Only testing mode is valid
25	Test results of Antenna 4	1	Only testing mode is valid

	(North) master antenna		**0x00** —— Test failed **0x01** —— Test ok **0xFF** —— Test tag not read
26	RSSI of Antenna 4 (North) master antenna	1	For Single byte, range （-10 ～ -128）, Only testing mode is valid
27	Test results of Antenna 4 (North) slave antenna	1	Only testing mode is valid **0x00** —— Test failed **0x01** —— Test ok **0xFF** —— Test tag not read
28	RSSI of Antenna 4 (North) slave antenna	1	For Single byte, range （-10 ～ -128）, Only testing mode is valid

eg：0B 53 2E 00 01 A1 01 00 15 01 07 01 07 01 07 01 07 1F 1F 1F 1F 80 80 80 80 01 01 01 01 01 DD D8 01 E8 01 DE 01 E6 01 EC 01 E0 01 E5 01 E8 01 DD 3C

sof	cmd	len	opt	data[0]		data[43]	checksum
0B	53	2C	00	01	...	DD	3C

sof : 0x0B

cmd : 0x53

Len : 0x2E

opt : 0x00 (Successful operation)

data : 01 A1 01 00 15 01 07 01 07 01 07 01 07 1F 1F 1F 1F 80 80 80 80 01 01 01 01 DD D8 01 E8 01 DE 01 E6 01 EC 01 E0 01 E5 01 E8 01 DD

: 01 1.The 5th byte in the frame, the test result: “Test ok”

: A1 2. The 6th byte in the frame, the connection status with the platform: “GPRS connected”

: 01 3. The 7th byte in the frame, GPRS TCP connection status: “connected”

: 00 4. The 8th byte in the frame, wired TCP connection status: “connected”

: 15 5. The 9th byte in the frame, GPRS signal rssi: 0x15， 21

: 01 07 01 07 01 07 01 07 6. The 10th byte in the frame, the firmware version of the antenna: the firmware version of the 4 antennas are:

Antenna 1 (East): V1.7

Antenna 2 (South): V1.7

Antenna 3 (West): V1.7

Antenna 4 (Noeth): V1.7

: 1F 1F 1F 1F 7. The 18th byte in the frame, antenna gain: The gains of the four antennas are:

Antenna 1 (East): 31

Antenna 2 (South): 31

Antenna 3 (West): 31

Antenna 4 (Noeth): 31

: 80 80 80 80 8. The 22nd byte in the frame, the rssi filtering threshold of the antenna: the rssi of the 4 antennas is

Antenna 1 (East): -128

Antenna 2 (South): -128

Antenna 3 (West): -128
Antenna 4 (Noeth): -128

: 01 9. The 26th byte in the frame, the current mode of the device: “Testing mode”

: 01 01 01 01 10. The 27th byte in the frame, the working mode of the antenna: respectively 4 antennas The current working mode is:

Antenna 1 (East): Testing mode
Antenna 2 (South): Testing mode
Antenna 3 (West): esting mode
Antenna 4 (Noeth): Testing mode

: DD 11. The 31st byte in the frame, the master antenna rssi threshold during the test:D0xDD 即“-35”

: D8 12 The 32nd byte in the frame, the slave antenna rssi threshold during the test:0xD8 “-40”

: 01 E8 01 DE 13～16. The 33rd byte in the frame, Antenna 1 (East) test results:

Antenna 1 (East) master antenna: 01 test ok, rssi: 0xE8， -24
Antenna 1 (East) slave antenna: 01 test ok, rssi: 0xDE，-34

: 01 E6 01 EC 17～20. The 37th byte in the frame, Antenna 2 (South) test results:

Antenna 2 (South) master antenna: 01 test ok, rssi: 0xE6，-26
Antenna 2 (South) slave antenna: 01 test ok, rssi: 0xEC，-20

: 01 E0 01 E5 21～24. The 41st byte in the frame, Antenna 3 (West) test results:

Antenna 3 (West) master antenna: 01 test ok, rssi: 0xE0，-32
Antenna 3 (West) slave antenna: 01 test ok, rssi: 0xE5，-27

: 01 E8 01 DD 25～28. The 45th byte in the frame, Antenna 4 (North) test results:

Antenna 4 (North) master antenna: 01 test ok, rssi: 0xE8，-24
Antenna 4 (North) slave antenna: 01 test ok, rssi: 0xDD，-35

checksum: 0x3C

4.25 Bluetooth password verification 0x0A

In MR7901P V1.5 firmware, before modify the system parameters, the Bluetooth password must be verified. After the password is verified, the system parameters can be modified, otherwise the system parameters can only be read.

MR7901P V1.5： The default password for Bluetooth authentication is: "passwdss" (8 bytes)

4.25.1 Command frame definition

cmd ： 0x0A

data ： Type (verify password / change password) + password to be verified / password to be verified +

new password

Data field description：

Field	Bytes	Explanation
type	1	**0x01** —— verify password **0x02** —— change password
password to be verified passwd	8	Character type, no end character, default is "passwdss"
new password new_passwod	8	Character type, no end character (type = 0x02 is valid when changing the password)

1. verify password

eg：0A FF 0B 0A 01 70 61 73 73 77 64 73 73 69

sof	addr	len	cmd	data[0] type	data[1] passwd(MSB)	data[2]	data[3]	data[4]
0A	FF	0B	0A	01	70	61	73	73
data[5]	**data[6]**	**data[7]**	**data[8] passwd(LSB)**		**checksum**			
77	64	73	73		69			

sof : 0x0A

addr : 0xFF

len : 0x0B

cmd : 0x0A

data : 01 70 61 73 73 77 64 73 73

type :01 verify password

password to be verified passwd : 70 61 73 73 77 64 73 73 : password to be verified "passwd"

checksum: 0x69

2. change password

eg1：0A FF 13 0A 02 70 61 73 73 77 64 73 73 70 61 73 73 77 64 73 75 E6

sof	addr	len	cmd	data[0] type	data[1] passwd(MSB)	data[2]	data[3]
0A	FF	13	0A	01	70	61	73
data[4]	**data[5]**	**data[6]**	**data[7]**	**data[8] passwd(LSB)**	**data[9] new_passwd(MSB)**	**data[10]**	**data[11]**
73	77	64	73	73	70	61	73
data[12]	**data[13]**	**data[14]**	**data[15]**	**data[16] new_passwd(LSB)**	**checksum**		
73	77	64	73	75	E6		

sof : 0x0A

addr : 0xFF

len : 0x13

cmd : 0x0A

data : 02 70 61 73 73 77 64 73 73 70 61 73 73 77 64 73 75

type : 02 change password
password to be verified : 70 61 73 73 77 64 73 73 : password to be passwd verified “passwdss”
new password 70 61 73 73 77 64 73 75 : new password new_passwd “passwdsu”

checksum: 0xE6

4.25.2 Response frame definition

The device responds after receiving the command.

cmd : 0x0A
data : Type verify password/change password）

1. verify password response

eg: 0B 0A 03 00 01 E7

sof	cmd	len	opt	data[0] type	checksum
0B	0A	03	00	01	E7

sof : 0x0B
cmd : 0x0A
len : 0x03
opt : 0x00 (Successful operation)
data : 01 -- type verify password
checksum: 0xE7

2. change password response

eg: 0B 0A 03 00 02 E6

sof	cmd	len	opt	data[0] type	checksum
0B	0A	03	00	02	E6

sof : 0x0B
cmd : 0x0A
len : 0x03
opt : 0x00 (Successful operation)
data : 02 -- type change password
checksum: 0xE7

4.26 Set APN related parameters 0x62

In the firmware of MR7901P V1.3 and above (including this version), the APN related parameters (APN, authentication type, user name, password, etc.) of the GPRS module (or wireless communication module) can be configured through Bluetooth commands.

Note:

After the APN related parameters are successfully reconfigured, the system can be restarted (by sending the reset command 0x21, or power off and restart). After restarting, the system will configure the wireless communication module according to the newly configured apn related parameters.

4.26.1 Command frame definition

Command code : 0x62

Data : apn related parameters, the specific data field format is as follows

Data field description:

file	Number of bytes	Description
Access point name APN	32	Character type, "\0" is the terminator, the default is "3gnet"
Configuration flag cfg_flag	1	Numerical type, APN configuration is enabled 1: Configure 0: Not configured
Authentication protocol auth_type	1	Apn Authentication protocol 0: NONE 1: PAP 2: CHAP 3: PAP/CHAP
Username name	32	Character type, '\0' is the terminator
password	32	Character type, '\0' is the terminator

eg: 0A FF 64 62 63 74 6E 65 74 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 03 63 74 6E 65 74 40 6D 79 63 64 6D 61 2E 63 6E 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 76 6E 65 74 2E 6D 6F 62 69 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 A5

sof	addr	len	cmd	data[0] apn	....	checksum
0A	FF	64	62	63	...	A5

sof : 0x0A

addr : 0xFF
len : 0x64
cmd : 0x62
data : 63 74 6E 65 74 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 03 63 74 6E 65 74 40 6D 79 63 64 6D 61 2E 63 6E 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 76 6E 65 74 2E 6D 6F 62 69 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Access point nameAPN : 63 74 6E 65 74 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 apn is “ctnet”

Configuration flag : 01 : config apn cfg_flag

Authentication protocol : 03 : Authentication protocol is “PAP/CHAP” auth_type

Username name : 63 74 6E 65 74 40 6D 79 63 64 6D 61 2E 63 6E 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 username is “ctnet@mycdma.cn”

password : 76 6E 65 74 2E 6D 6F 62 69 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 password is “vnet.mobi”

checksum : 0xA5

4.26.2 Response frame definition

After receiving this message, the device responds with the following message.
Command code : 0x62
data : none
eg： 0B 62 02 00 91

sof	cmd	len	opt	checksum
0B	62	02	00	91

sof : 0x0B
cmd : 0x62
len : 0x02
opt : 0x00 (Operation is successful, failure is 0x80)
data : none
checksum : 0x91

4.27 Query APN related parameters 0x63

Used to query the APN related parameters used by the current system

4.27.1 Command frame definition

Get apn related parameters.

Command code ： 0x63

data： none

eg：0A FF 02 63 92

sof	addr	len	cmd	checksum
0A	FF	02	63	92

sof : 0x0A

addr : 0xFF

len : 0x02

cmd : 0x63

data : none

checksum: 0x92

4.27.2 Response frame definition

After receiving this message, the device responds with the following message.

Command code : 0x63

data : apn related parameters, the specific data field format is as follows

Data field description：

file	Number of bytes	description
Access point name APN	32	Character type, "\0" is the terminator, the default is "3gnet"
Configuration flag cfg_flag	1	Numerical type, APN configuration is enabled 1: Configure 0: Not configured
Authentication protocol auth_type	1	Apn Authentication protoco 0: NONE 1: PAP 2: CHAP 3: PAP/CHAP
Username name	32	Character type, ‘\0’ is the terminator
password	32	Character type, ‘\0’ is the terminator

eg：0B 63 64 00 63 74 6E 65 74 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 03 63 74 6E 65 74 40 6D 79 63 64 6D 61 2E 63 6E 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 76 6E 65 74 2E 6D 6F 62 69 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 A2

sof	cmd	len	opt	data[0]	....	checksum

				apn		
0B	63	64	00	63	...	A2

sof : 0x0B

cmd : 0x63

len : 0x64

opt : 0x00 (Operation is successful)

data : 63 74 6E 65 74 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 03 63 74 6E 65 74 40 6D 79 63 64 6D 61 2E 63 6E 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 76 6E 65 74 2E 6D 6F 62 69 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Access point name APN : 63 74 6E 65 74 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

5. System configuration parameter format description

When using command codes 0x13 and 0x14, it involves configuring and reading system configuration parameters. The specific description of these configuration parameters is as follows:

Table 1 System configuration parameters

SN	Data segment	Bytes	Read/write	Type	Description
1	Parameter characteristic value	1	R/W	number	When writing, keep 0x55 unchanged, the parameters can be configured normally, When writing, if it is not 0x55, the factory default parameters will be restored; When reading, fixed at 0x55
2	communication mode	1	R/W	number	Low 4 digits, read only, transmission method: 1bit: read only, GPRS connection, 1 valid 2 bit: read only, LAN connection, 1 valid 3bit: reserved 4bit: reserved 5bit: readable and writable, tag transmission identification, 0: transmit tag record to platform; 1: do not transmit tag record to platform 6 ~ 8bit: reserved eg：0x11, means GPRS connection, no tag record is transmitted to the platform. eg: 0x01, means GPRS connection, transfer tag record to the platform
3	firmware version	2	R	number	Firmware version, major version number first eg: 02 07， V2.7
4	Buzzer identification	1	R/W	number	1: Turn on the buzzer, 0: Turn off the buzzer
5	Revise 1	1	-	-	
6	Deduplication	2	R/W	number	Tag deduplication filter window, unit:

	window (time to know tag leave device)				second; no filter at 0x0000, low byte first, high byte second Value range: 20 ～ 65535
7	device ID	16	R/W	String	The 15-digit product serial number is ASCII, and the last 1 byte is filled with 0x00 eg: “861694034205896”
8	timeout of staying	2	R/W	number	The tag stays at the base station and is reported to the platform at this time interval (this function is only available in V3.3). The low byte is first and the high byte is second. Unit: second Value range: 0, 60 ～ 65535 0: Do not use this function 60 ～ 65535: timeout time
9	DHCP encable	1	R/W	number	1: On, 0: Off, suitable for LAN
10	LAN IP	4	R/W	number	Used for LAN network parameter configuration
11	LAN Subnet mask	4	R/W	number	Used for LAN network parameter configuration
12	LAN gateway	4	R/W	number	Used for LAN network parameter configuration
13	LAN port	2	R/W	number	Local IP port, suitable for LAN, low byte first, high byte second (value range 0 ～ 65536) eg: *24 13 , 即 0x1324(HEX) = 4900 (DEC)*
14	GPRS Server1 IP	32	R/W	String	IP or domain name, string
15	GPRS Server 1 Port	2	R/W	number	Low byte first, high byte second (Value range 0 ～ 65536)
16	LAN Server1 IP	32	R/W	String	IP or domain name, string
17	LAN Server 1 Port	2	R/W	number	Low byte first, high byte second (Value range 0 ～ 65536)
18	LAN local mac address	6	R/W	number	Used for LAN network parameter configuration
19	Reserved 3	28	-	-	-
20	Antenna version	8	R	number	Corresponding to the firmware version of 4 antennas Each antenna version occupies 2 bytes eg：01 06 is V1.6, if it is FF FF means reading antenna version failed (may be no antenna connected)

21	GPRS signal strengthI	1	R	number	00 or 99 means GPRS has no signal 99 means failed to read gprs signal Normal value range 0 ～ 31
22	factory number	16	R	String	eg: “MR7901-003C0025”
23	Antenna RSSI threshold	4	R/W	number with symbol	Value range: -1 ～ -128 The RSSI value of antenna 1, 2, 3 and 4. eg: -88
24	Antenna gain	4	R/W	number	Value range 0~31, The gain value of antenna 1, 2, 3 and 4.
25	Bluetooth output tag identification	1	R/W	number	0: Cannot output tags via Bluetooth 1: Can output tags via Bluetooth. At this time, the tag read by the antenna will only be output through Bluetooth, and the output of the label is prohibited by gprs and lan.
26	communication status	1	R	number	Direct connection status with the platform Lower 4 bytes, connection method 1bit: read only, GPRS connection, 1 valid 2 bit: read only, LAN connection, 1 valid 3bit: reserved 4bit: reserved High 4 bytes, fixed at A eg： 0xA0 No connection 0xA1 GPRS connection 0xA2 LAN connection 0xA3 GPRS &LAN connection
27	identification of tag directional filter	1	R/W	number	1: use filtering, 0: do not use
28	time interval of directional filter	1	R/W	number	Unit time: seconds (3 ~ 255)
29	reserved 4	2	-	-	
The following two items are only included when reading parameters; they are not included when writing to the device.					
30	Firmware version	2	R		Firmware version, major version number first eg: 02 07， V2.7

31	Firmware compilation time	20	R	String	Firmware compilation time, string type eg: “Jan 11 2017, 14:41:06”

6.Tag format description

6.1 4bytes Tag format description

Here we introduce the tag data format for reading the 4-byte tag ID base station, total of 10 bytes.

The tag data stored in the external flash and the tag data uploaded to the server have the same data format. The specific instructions are as follows:

eg : 20 E3 AF 22 32 FA 00 00 00 B2

Tag Type （1byte）	ID （4byte）	Checksum （1byte）	Activation address （2byte）	Alarm （1byte）	RSSI （1byte）
20	E3 AF 22 32	FA	00 00	00	B2

20 : Tag type,

E3 AF 22 32 : Tag ID,

FA : 20 E3 AF 22 32 Checksum (check algorithm in Chapter 9 Check Algorithm)

00 00 : Activation address, non-activation

00 : Alarm status (normally 00)

B2 : Signal strength, -78dBm (single byte with symbol)

Description of alarm status:

Description of alarm status bytes								
type	**7bit**	**6bit**	**5bit**	**4bit**	**3bit**	**2bit**	**anti-tamper indicate 1bit**	**0bit**
							1: remove alarm 0: normal	1: low battery alarm 0: normal

7.Command summary

SN	cmd	description
1	0x0C	Get GPRS signal strength
2	0x13	Set system configuration parameters
3	0x14	Get system configuration parameters and firmware info
4	0x15	Get GPRS module IMEI
5	0x16	Set device RTC time
6	0x17	Get device RTC time
7	0x18	Get tag data
8	0x19	Set Bluetooth output tag data identification
9	0x20	Get Bluetooth output tagl data identification
10	0X21	Reset the device
11	0x22	Get version informatio
12	0x24	Get device number
13	0x25	Get the number of tag records
14	0x26	Set transmission tag record identification
15	0x27	Get transmission tag record identification
16	0x28	Get antenna information
17	0x29	Get the IP , status and port of the current GPRS connection
18	0x2A	Tag search
19	0x2B	Get the IP , status and port of the current LAN connection
20	0x31	host PC firmware update start
21	0x32	send update field
22	0x33	end of update
23	0x07	Get device hardware information
24	0x51	Set work mode
25	0x52	Query work mode
26	0x53	Query test result
27	0x0A	Bluetooth password verification
28	0x62	Set APN related parameters
29	0x63	Query APN related parameters

8.Opcode summary

The operation code feedbacks the operation result of the device to the instruction. The highest bit reflects the operation result. When the highest bit is 1, it means that the operation failed, and the lower 4 bits indicate the error type. For example: 0x81 means that the operation failed, and the reason for the

failure is an instruction code error.

SN	status	Description
1	0x00	Successful operation
2	0x80	operation failed
3	0x40	no need to response
4	0x01	Incorrect command code, this command is not supported
5	0x02	check error
6	0x03	Data content error
7	~~0x04~~	
8	0x06	no tag data
9	~~0x08~~	
10	~~0x09~~	
11	0xFF	Undefined error

9.Checksum algorithm

9. 1 Checksum algorithm

Sum check is used in tag data.

9.1.1 C language calculation function

```
/*****************************************************************************
** Function name       :   CheckSum
** Descriptions        :   Checksum
** input parameters    :   uBuff data to be check
**                         uBuffLen length of check data
** output parameters :   none
** Returned value     :    check value
*****************************************************************************/
 uint8   CheckSum(uint8 *uBuff, uint16 uBuffLen)
 {
     uint16 i;
     uint8 uSum=0;

    for(i=0;i<uBuffLen;i++)
    {
        uSum = uSum + uBuff[i];
    }
    uSum = (~uSum) + 1;

    return uSum;
 }
```

9.1.2 JAVA Calculation method

```
/*************************************************************
 * JAVA algorithm of Checksum in tag data
 *
 * @param sendbyte  The range of checksum  needs to be calculated: 1 byte tag TYPE + 4 byte tag ID
 *
 * @return       Calculated checksum
 *                20 E3 AF 22 32 checksum：FA( -6 in dec)
```

```
**********************************************************/
protected static byte sendRcvByteNum(byte[] sendbyte) {
        byte sum = 0;
        for (int i = 0; i < sendbyte.length; i++) {
            sum += sendbyte[i];
        }
        byte rebyte = (byte) (~sum + 1);
        System.out.println("校验位 Check Digit: " + rebyte);
        return rebyte;
    }

//Calculated checksum 20 E3 AF 22 32 checksum : FA( -6 in dec)
public static void main(String[] args) {
        byte[] b = new byte[5];
        b[0] = 0x20;
        b[1] = (byte) 0xE3;
        b[2] = (byte) 0xAF;
        b[3] = 0x22;
        b[4] = 0x32;
        sendRcvByteNum(b);
    }
```