

RFID Command Format Description

目录

1. Command Format & RS232 setting	3
1.1 command format.....	5
1.1.1 Command to RFID module	5
1.1.2 Response from RFID module	6
2. UHF Command	6
2.1 UHF Module Connect& Disconnect.....	7
2.1.1 Open UHF Module.....	7
2.1.2 Close UHF Module.....	7
2.1.3 Reset the RFID module.....	8
2.2. UHF Get & Set Configuration.....	8
2.2.1 Get Module Product Information.....	8
2.2.2 Set Power	9
2.2.3 Set Frequency Region.....	10
2.2.4 Set Filtering Criteria.....	11
2.2.5 Clear Filtering Criteria	12
2.2.6 Set Speed Mode	12
2.2.7 Set Inventory Time	13
2.2.8 Set Inventory Tag Stop Count	14
2.2.9 Set GPIO Trigger	14
2.2.10 Set Working Mode.....	16
2.2.11 Set Tag Group	17
2.2.12 Set Rx Sensitivity	18
2.2.13 Set Fixed Frequency	18
2.2.14 Get Module Configuration	21
2.2.15 Get Firmware Version.....	22
2.2.16 Set Tag Return Mode.....	22
2.2.17 Get Tag Return Mode	23
2.2.18 Heartbeat Packet.....	23
2.2.19 Enable Heartbeat Packet	24
2.2.20 Test Channel Performance	24
2.2.21 Set Optimal Freq Channel	27
2.2.22 Get Optimal Freq Channel.....	27
2.2.23 Get UHF Module Version.....	28
2.2.24 Check Antenna status.....	29
2.2.25 set antenna dwell time.....	30
2.2.26 Set GPO	31
2.2.27 Set GPI	31
2.2.28 Set Profile	33
2.2.29 Get Profile	33

2.2.30 Get dwell time	34
2.3 UHF Inventory & Access	35
2.3.1 Start Inventory.....	35
2.3.2 Stop Inventory	35
2.3.3 set access password	36
2.3.4 Write Data to Tag.....	36
2.3.5 Read Data from Tag	37
2.3.6 Lock Tag	38
2.3.7 Unlock Tag	39
2.3.8 Kill Tag.....	40
2.3.9 Block Write Data to Tag	40
2.3.10 Group Read Data From Tag	41
2.3.11 Perm Lock Tag.....	42
2.3.12 Perm Unlock Tag.....	43
2.3.13 Single Read EPC and Data From Tag	44
2.3.14 Set QT Control	45
2.2.15 Read Data with password.....	46
2.2.16 Write Data with password.....	47
2.2.17 Block Write data with password.....	48
3. Storage Command.....	50
3.1 Read Block Data.....	50
3.2 Read Block Count	51
3.3 Write Block Data.....	51
3.4 Get Block Size	52
3.5 Initial Storage Data	52
4. IP Setting Command.....	53
4.1 Set IP Address.....	53
4.2 Set TCP Port.....	54
4.3 Set Subnet Mask.....	55
4.4 Set Gateway.....	55
4.5 Enable or Disable DHCP.....	56
4.6 Get IP Configuration	56
4.7 save UHF & IP CFG to Flash	57
5. LED Indicators.....	58
5.1 Power Indicator	58
5.2 UHF Ready Indicator.....	58
5.3 Antenna Indicators	58
5.4 Working Mode Indicator	58
5.5 Inventory& Access Operation Indicator	59

Version No.	Editor	Date	Demo
1.0	Software	2014/3/31	Initial version
1.1	Software	2014/4/17	
1.2	Software	2014/6/24	Add Japan region support
1.3	Software	2014/6/24	Add group read support
1.4	Software	2014/7/08	Add perm lock and perm unlock command
2.0	Software	2014/9/12	add group read command , single read EPC and data command
2.2	Software	2014/9/25	Ecube firmware work with UHF comand firmware
2.4	Software	2014/10/16	revise firmware upgrade method and add antenna connection detect command
2.7	Software	2014/11/07	add set antenna dwell time
2.12	Software	2015/01/12	split gpio setting to gpi and gpo

1. Command Format & RS232 setting

RFID UART default setting:

Bound rate: 115200

Data-bit: 8

Stop-bit: 1

Parity type: None

Flow Control: None

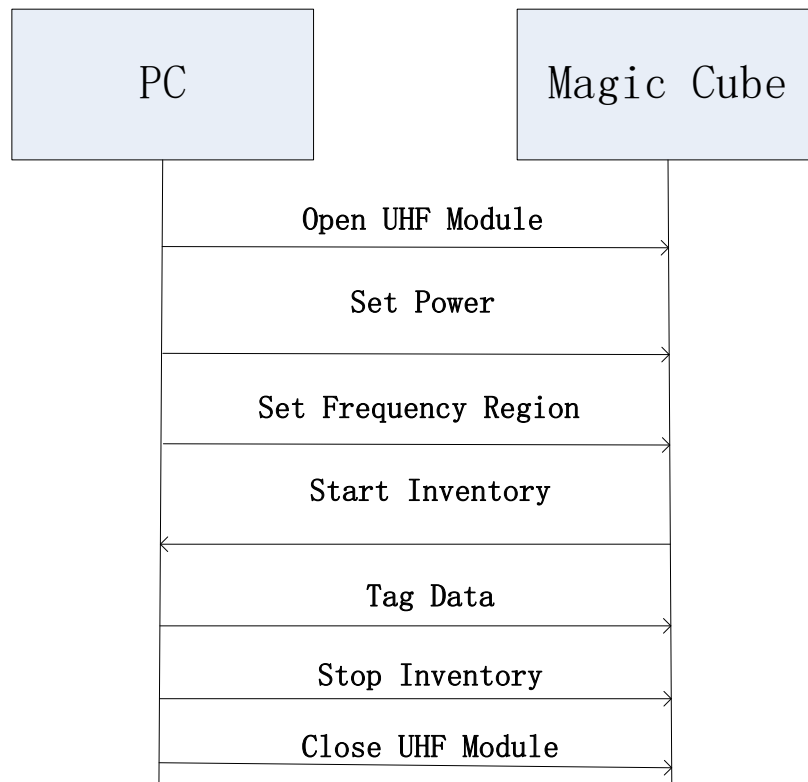
RFID Ethernet default setting:

HostName:JW_UHF

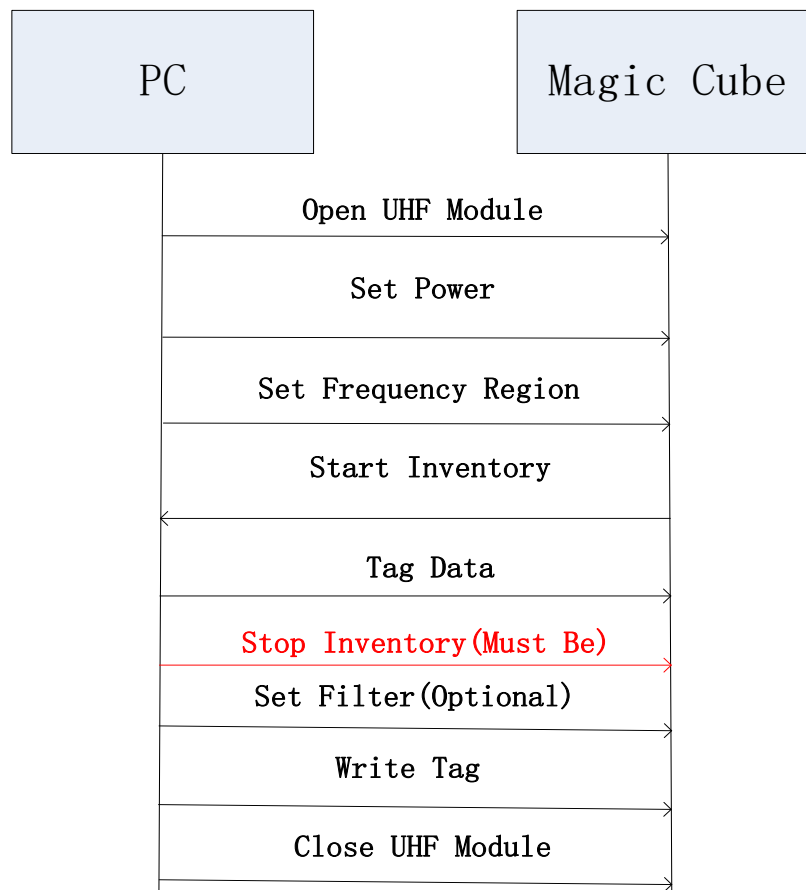
IP:192.168.100.168

Port:9761

Inventory procedure



Set filter & write tag procedure



1.1 command format

1.1.1 Command to RFID module

head	reserved	len	command data	crc
0xff 0xff	0	len	command data	crc
2 bytes	1 byte	1 byte	variable length	1 byte

the format of command data is as following:

CMD ID	P0	P1	P2	P3	...
Command ID	Parameter 0	Parameter 1	Parameter 3	Parameter 4	...
1 Byte	1 Byte	1 Byte	1 Byte	1 Byte	...

If the length of command is k(include head, reserved, len, command data, except crc), then
 crc=0;

```
for(i=0;i<k;i++)
    crc^=command[i];
```

then total length of command is (k+1)

1.1.2 Response from RFID module

head	reserved	len	response data	crc
0xff 0xff	0	len	response data	crc
2 bytes	1 byte	1 byte	variable length	1 byte

If the length of response is k(include head, reserved, len, response data, except crc), then

```
crc=0;
for(i=0;i<k;i++)
    crc^=command[i];
```

then total length of response is (k+1)

the format of response data:

CMD ID	D0	Data
Command ID	Data of length	Data
1 Byte	1 byte	Length of data

This document is focus on command data & response data.

This document includes the following categories:

- 1) UHF Command
- 2) Storage Command
- 3) IP Setting Command

2. UHF Command

UHF command includes these categories:

- 1) UHF module connect & disconnect
- 2) UHF module get & set configuration
- 3) UHF inventory & access

2.1 UHF Module Connect& Disconnect

2.1.1 Open UHF Module

Support Interface Port: Ethernet, Uart

Command to RFID module:

CMD ID	P0	P1	P2	P3
0xA0	0x00	0x00	0x00	0x00
1 Byte	1 Byte	1 Byte	1 Byte	1 Byte

Before you can access this module, you must open it at first

Response from RFID module:

CMD ID	D0	Data
0xA0	0x02	result code
1 Byte	1 Byte	2 Byte

The meaning of result code (Data [0] is the high 8 bits and Data [1] is low 8 bits) as following:

0000: the operation is completed successfully.

FF00:the module can't be opened.

F000:the module was opened already.

Others: not defined.

2.1.2 Close UHF Module

Support Interface Port: Ethernet, Uart

Command to RFID module:

CMD ID	P0	P1	P2	P3
0xA1	0x00	0x00	0x00	0x00
1 Byte	1 Byte	1 Byte	1 Byte	1 Byte

After you access this module , you may close it.

Response from RFID module:

CMD ID	D0	Data

0xA1	0x02	result code
1 Byte	1 Byte	2 Byte

The meaning of result code (Data [0] is the high 8 bits and Data [1] is low 8 bits) as following:

0000: the operation is completed successfully.

FF00:the module is closed.

Others: the operation is stopped with some error.

2.1.3 Reset the RFID module

Support Interface Port: Ethernet, Uart

Command to RFID module:

CMD ID	P0	P1	P2	P3
0xF9	0x00	0x00	0x00	0x00
1 Byte	1 Byte	1 Byte	1 Byte	1 Byte

If the module can't work for some critical problems, you can use this command to reset the module to secure state.

This command reset ecube or uhf module to default state

Response from RFID module:

CMD ID	D0	Data
0xF9	0x02	result code
1 Byte	1 Byte	2 Byte

The meaning of result code (Data [0] is the high 8 bits and Data [1] is low 8 bits) as following:

0000: the operation is completed successfully.

FFFE: module is busy. You can make the module to be free by issuing Stop Inventory command.

FF00:the module is closed.

Others: not defined.

2.2. UHF Get & Set Configuration

2.2.1 Get Module Product Information

Command to RFID module:

CMD ID	P0	P1	P2	P3
0xF0	0x00	0x00	0x00	0x00
1 Byte	1 Byte	1 Byte	1 Byte	1 Byte

Normal Response from RFID module:

CMD ID	D0	Data	E-Module Indicator
0xF0	0x10	Response module information	0x12 0x12 0x12 0x12
1 Byte	1 Byte	12 Byte	4 byte

Error:

CMD ID	D0	Data
0xF0	0x02	Error code
1 Byte	1 Byte	2 Byte

The meaning of error code (Data [0] is the high 8 bits and Data [1] is low 8 bits) as following:

FFFF: no response from module.

FFFE: module is busy. You can make the module to be free by issuing Stop Inventory command.

FF00:the module is closed.

Others: not defined.

2.2.2 Set Power

Command to RFID module:

CMD ID	P0	P1	P2	P3
0xF3	Ant0 power	Ant1 power	Ant2 power	Ant3 power
1 Byte	1 Byte	1 Byte	1 Byte	1 Byte

P0~03: hex format. If greater than 0, the antenna is working and the value will be output power. If the value is zero, the mean antenna is not working.

For example:

ANT1 output power is 16 dB, ANT2 output power is 18 dB

Command:

F3 00 16 12 00

Response from RFID module:

CMD ID	D0	Data
0xF3	0x02	result code
1 Byte	1 Byte	2 Byte

The meaning of result code (Data [0] is the high 8 bits and Data [1] is low 8 bits) as following:

0000: the operation is completed successfully.

FFFF: no response from module.

FFFE: module is busy. You can make the module to be free by issuing Stop Inventory command.

FF00: the module is closed.

Others: not defined.

2.2.3 Set Frequency Region**Command to RFID module:**

CMD ID	P0	P1	P2	P3
0xF5	Region code	0x00	0x00	0x00
1 Byte	1 Byte	1 Byte	1 Byte	1 Byte

P0 = 0, FCC

P0 = 1, CCC

P0 = 2, NCC

P0 = 3, JPN

Response from RFID module:

CMD ID	D0	Data
0xF5	0x02	result code
1 Byte	1 Byte	2 Byte

The meaning of result code (Data [0] is the high 8 bits and Data [1] is low 8 bits) as following:

0000: the operation is completed successfully.

FFFF: no response from module.

FFFE: module is busy. You can make the module to be free by issuing Stop Inventory command.

FF00:the module is closed.

Others: not defined.

2.2.4 Set Filtering Criteria

Command to RFID module:

CMD ID	P0	P1	P2	P3	Data
0xF6	bank	offset	length	nomatch	Filter data
1 Byte	1 Byte	1 Byte	1 Byte	1 Byte	length Byte

P0=0, reserved bank

P0=1, EPC bank

P0=2, TID bank

P0=3, User bank

P1 is offset from the P0 bank

P2 is the filter data of length

P3 defines which tags will be report. if nomatch==0, then tags matching filter will be report;

if nomatch==1, then tags not matching filter will be report.

For example, you want to filter EPC begin with A0123456, then

P0=0x01, P1=0x00, P2=0x04, Data=0xA0123456

Response from RFID module:

CMD ID	D0	Data
0xF6	0x02	result code
1 Byte	1 Byte	2 Byte

The meaning of result code (Data [0] is the high 8 bits and Data [1] is low 8 bits) as following:

0000: the operation is completed successfully.

FFFF: no response from module.

FFFE: module is busy. You can make the module to be free by issuing Stop Inventory command.

FF00:the module is closed.

Others: not defined.

2.2.5 Clear Filtering Criteria

Command to RFID module:

CMD ID	P0	P1	P2	P3
0xF8	0x00	0x00	0x00	0x00
1 Byte	1 Byte	1 Byte	1 Byte	1 Byte

Response from RFID module:

CMD ID	D0	Data
0xF8	0x02	result code
1 Byte	1 Byte	2 Byte

The meaning of result code (Data [0] is the high 8 bits and Data [1] is low 8 bits) as following:

0000: the operation is completed successfully.

FFFF: no response from module.

FFFE: module is busy. You can make the module to be free by issuing Stop Inventory command.

FF00: the module is closed.

Others: not defined.

2.2.6 Set Speed Mode

Speed mode of RFID module default setting is normal speed.

Command to RFID module:

CMD ID	P0	P1	P2	P3
0xFA	Mode	0x00	0x00	0x00
1 Byte	1 Byte	1 Byte	1 Byte	1 Byte

Mode:

0x00 High Speed

0x01 Normal Speed

0x02 power save mode

Response from RFID module:

CMD ID	D0	Data
0xFA	0x02	result code
1 Byte	1 Byte	2 Byte

The meaning of result code (Data [0] is the high 8 bits and Data [1] is low 8 bits) as following:

0000: the operation is completed successfully.

FFFF: no response from module.

FFFE: module is busy. You can make the module to be free by issuing Stop Inventory command.

FF00: the module is closed.

Others: not defined.

2.2.7 Set Inventory Time**Command to RFID module:**

CMD ID	P0	P1	P2	P3
0xB0	Time0	Time1	Time2	Time3
1 Byte	1 Byte	1 Byte	1 Byte	1 Byte

when you want to set the inventory time, you may set this command.

if you want to set inventory time is 1000(decimal)(hex 0x03e8) milliseconds, then

Time0=0x00

Time1=0x00

Time2=0x03

Time3=0xE8

if you want to inventory for indefinite time, then

Time0=0x00

Time1=0x00

Time2=0x00

Time3=0x00

Response from RFID module:

CMD ID	D0	Data
0xB0	0x02	result code
1 Byte	1 Byte	2 Byte

The meaning of result code (Data [0] is the high 8 bits and Data [1] is low 8 bits) as following:

0000: the operation is completed successfully.

FFFF: no response from module.

FFFE: module is busy. You can make the module to be free by issuing Stop Inventory command.

FF00:the module is closed.

Others: not defined.

2.2.8 Set Inventory Tag Stop Count

Command to RFID module:

CMD ID	P0	P1	P2	P3
0xB1	Count	0x00	0x00	0x00
1 Byte	1 Byte	1 Byte	1 Byte	1 Byte

when you want to set the inventory tag stop count, you may set this command.

Count must be select between 0 and 1.

if Count is equal to 0, then inventory will not be stopped until you send a stop command

if count is not equal to 0, then inventory will be stopped after get count tags.

Response from RFID module:

CMD ID	D0	Data
0xB1	0x02	result code
1 Byte	1 Byte	2 Byte

The meaning of result code (Data [0] is the high 8 bits and Data [1] is low 8 bits) as following:

0000: the operation is completed successfully.

FFFF: no response from module.

FFFE: module is busy. You can make the module to be free by issuing Stop Inventory command.

FFFD: invalid tag stop count

FF00:the module is closed.

Others: not defined.

2.2.9 Set GPIO Trigger

Command to RFID module:

CMD ID	P0	P1	P2	P3
0xB2	Gpo0	Gpo1	Gpi0	Gpi1
1 Byte	1 Byte	1 Byte	1 Byte	1 Byte

when you want to trig inventory tag by GPIO, you may set this command.

if Gpi0=0, then GPIO0 is not set;

if Gpi0=1, then inventory is trigged when Gpi0's falling edge and is stopped by Gpi0's rising edge.

If the value of Gpi0 changes from high to low, then B2 04 01 00 00 00 will be returned to host; if the value of Gpi0 changes from low to high, then B2 04 01 00 01 00 will be returned to host.

if Gpi0=2, then Gpi0 is set as input pin. If the value of Gpi0 changes from high to low, then B2 04 02 00 00 00 will be returned to host; if the value of Gpi0 changes from low to high, then B2 04 02 00 01 00 will be returned to host.

if Gpi0=3, then gpi0 is set as output high

if gpi0=4, then gpi0 is set as output low

if Gpi1=0, then Gpi1 is not set;

if Gpi1=1, then inventory is trigged when Gpi1's falling edge and is stopped by Gpi1's rising edge .

If the value of Gpi1 changes from high to low, then B2 04 00 01 00 00 will be returned to host; if the value of GPI1 changes from low to high, then B2 04 00 01 00 01 will be returned to host.

if Gpi1=2, then GPI1 is set as input pin. If the value of GPI1 changes from high to low, then B2 04 00 02 00 00 will be returned to host; if the value of GPI1 changes from low to high, then B2 04 00 02 00 01 will be returned to host.

if Gpi1=3, then gpi1 is set as output high

if gpi1=4, then gpi1 is set as output low

if Gpo0=1, then GPO0 is set as output high

if Gpo0=0, then GPO0 is set as output low

if Gpo1=1, then Gpo1is set as output high

if Gpo1=0, then Gpo1is set as output low

Response from RFID module:

CMD ID	D0	Data
0xB2	0x02	result code
1 Byte	1 Byte	2 Byte

The meaning of result code (Data [0] is the high 8 bits and Data [1] is low 8 bits) as following:

0000: the operation is completed successfully.

FFFF: no response from module.

FFFE: module is busy. You can make the module to be free by issuing Stop Inventory command.

FF00:the module is closed.

Others: not defined.

if GPIO or GPI1 is set to 1 or 2,when the value of GPI changes from high to low of visa, response is:

CMD ID	D0	GPIO setting	data
0xB2	0x04	setting	data
1 Byte	1 Byte	2 Byte	2 Byte

2.2.10 Set Working Mode

Command to RFID module:

CMD ID	P0	P1	P2	P3
0xB5	mode	0x00	0x00	0x00
1 Byte	1 Byte	1 Byte	1 Byte	1 Byte

If mode==0, then UHF device is at slave mode. After reboot the device can be driven by command or GPIO trigger

If mode ==1, then UHF device is at master mode. After reboot the device, it executes inventory operation immediately.

Response from RFID module:

CMD ID	D0	Data
0xB5	0x02	result code
1 Byte	1 Byte	2 Byte

The meaning of result code (Data [0] is the high 8 bits and Data [1] is low 8 bits) as following:

0000: the operation is completed successfully.

FFFF: no response from module.

FFFE: module is busy. You can make the module to be free by issuing Stop Inventory command.

FF00:the module is closed.

Others: not defined.

2.2.11 Set Tag Group

Command to RFID module:

CMD ID	P0	P1	P2	P3
0xB6	session	target	Search_mode	0x00
1 Byte	1 Byte	1 Byte	1 Byte	1 Byte

session:0~3 (Please reference the 18000-6C protocol)

target:0~1(0 is target A, 1 is target B, reference 18000-6C protocol)

search_mode:0~2(0 is dual target, 1 is single target,2 is single target with suppression)

if target==0 && search_mode==1, then selects whether tags whose inventoried flag is A participate in the inventory round

if search_mode==0, then selects whether tags whose inventoried flag is A and B participate in the inventory round

if search_mode==2, then session and target is disabled, one tag can only be inventoried one time.

Response from RFID module:

CMD ID	D0	Data
0xB6	0x02	result code
1 Byte	1 Byte	2 Byte

The meaning of result code (Data [0] is the high 8 bits and Data [1] is low 8 bits) as following:

0000: the operation is completed successfully.

FFFF: no response from module.

FFFE: module is busy. You can make the module to be free by issuing Stop Inventory command.

FF00:the module is closed.

Others: not defined.

2.2.12 Set Rx Sensitivity

Command to RFID module:

CMD ID	P0	P1	P2	P3
0xB7	Rssi_fileter_on	Rssi_threshold1	Rssi_threshold0	0x00
1 Byte	1 Byte	1 Byte	1 Byte	1 Byte

if Rssi_fileter_on ==1, then rssi_threshold is valid; otherwise rssi fileter is off.

For example, if Rssi_fileter_on ==1, Rssi_threshold1=0xFE, Rssi_threshold0=0xED, then RSSI=-275, the real rssi is -27.5dB. All tags's RSSI great or equal to -27.5dB can be report to host.

Response from RFID module:

CMD ID	D0	Data
0xB7	0x02	result code
1 Byte	1 Byte	2 Byte

The meaning of result code (Data [0] is the high 8 bits and Data [1] is low 8 bits) as following:

0000: the operation is completed successfully.

FFFF: no response from module.

FFFE: module is busy. You can make the module to be free by issuing Stop Inventory command.

FF00: the module is closed.

Others: not defined.

2.2.13 Set Fixed Frequency

Command to RFID module:

CMD ID	P0	P1	P2	P3
0xBF	channel_num	ant_port	ant_power	freq_index
1 Byte	1 Byte	1 Byte	1 Byte	1 Byte

if ant_port==0 && ant_power==0 && freq_index==0,
 then channel_num is used to set fixed frequency.
 antenna port & antenna power setting follows set power command
 the mapping between channel_num with frequency will be described below.
 else
 ant_port , ant_power and freq_index will be used to set fixed frequency.
 if use the three paramters, you must antenna port and antenna power by ant_port&
 ant_power
 $\text{real frequency} = 840250 + \text{freq_index} * 500 \text{ KHz}$
 Ex, if freq_index=10, then real frequency=840250+10*500=845250KHz=845.250MHz

channel_num and fixed frequency is mapped as following:

channel_num	freq(MHz)
0	915.75
1	915.25
2	903.25
3	926.75
4	926.25
5	904.25
6	927.25
7	920.25
8	919.25
9	909.25
10	918.75
11	917.75
12	905.25
13	904.75
14	925.25
15	921.75
16	914.75
17	906.75
18	913.75
19	922.25
20	911.25
21	911.75
22	903.75
23	908.75
24	905.75
25	912.25
26	906.25
27	917.25
28	914.25

29	907.25
30	918.25
31	916.25
32	910.25
33	910.75
34	907.75
35	924.75
36	909.75
37	919.75
38	916.75
39	913.25
40	923.75
41	908.25
42	925.75
43	912.75
44	924.25
45	921.25
46	920.75
47	922.75
48	902.75
49	923.25

Response from RFID module:

CMD ID	D0	Data
0xB7	0x02	result code
1 Byte	1 Byte	2 Byte

The meaning of result code (Data [0] is the high 8 bits and Data [1] is low 8 bits) as following:

0000: the operation is completed successfully.

FFFF: no response from module.

FFFE: module is busy. You can make the module to be free by issuing Stop Inventory command.

FF00:the module is closed.

Others: not defined.

2.2.14 Get Module Configuration

Command to RFID module:

CMD ID	P0	P1	P2	P3
0xB3	0x00	0x00	0x00	0x00
1 Byte	1 Byte	1 Byte	1 Byte	1 Byte

Normal Response from RFID module:

CMD ID	Info length	Power	Region	Speed mode	Inv time	Inv count	GPIO Trigger	Working Mode
0xB3	0x16	Ant0~Ant3	Region	Mode	Time0~Time3	Count0	Gpio0~Gpio3	mode
1 Byte	1 Byte	4 Byte	1 Byte	1 Byte	4 Byte	1 Byte	4 Byte	1 Byte

Session	target	Search mode	Rssi_filter_on	Rssi_threshold
session	target	Search mode	Region	Rssi_threshold
1 Byte	1 Byte	1 Byte	1 Byte	2Byte

Ant0~Ant3 definition is same to Set Power command

Region definition is same to set Frequency command

Mode definition is same to set Speed Mode Setting command

Time0 definition is same to Set Inventory Time command

Count0 definition is same to Set Inventory Tag Stop Count command

Gpio0~Gpio3 definition is same to GPIO Trigger Setting

Error Response from RFID module:

CMD ID	D0	Data
0xB3	0x02	result code
1 Byte	1 Byte	2 Byte

The meaning of result code (Data [0] is the high 8 bits and Data [1] is low 8 bits) as following:

0000: the operation is completed successfully.

FFFF: no response from module.

FFFE: module is busy. You can make the module to be free by issuing Stop Inventory command.

FF00:the module is closed.

Others: not defined.

2.2.15 Get Firmware Version

Command to RFID module:

CMD ID	P0	P1	P2	P3
0xB4	0x00	0x00	0x00	0x00
1 Byte	1 Byte	1 Byte	1 Byte	1 Byte

Response from RFID module:

CMD ID	D0	Result	Data	
0xB4	0x04	Result code	Major Version	Minor Version
1 Byte	1 Byte	2 Byte	1 Byte	1 Byte

The meaning of result code (Data [0] is the high 8 bits and Data [1] is low 8 bits) as following:

0000: the operation is completed successfully.

FFFF: no response from module.

FFFE: module is busy. You can make the module to be free by issuing Stop Inventory command.

FF00:the module is closed.

Others: not defined.

2.2.16 Set Tag Return Mode

Command to RFID module:

CMD ID	P0	P1	P2	P3
0xBE	mode	0x00	0x00	0x00
1 Byte	1 Byte	1 Byte	1 Byte	1 Byte

If P0=0x00, then all tags in scope will be return many times(repeated tags also be returned)

if P0=0x01, then all tags in scope will be return only one time

Response from RFID module:

CMD ID	D0	result
0xBE	0x02	result
1 Byte	1 Byte	2 Byte

The meaning of result code (Data [0] is the high 8 bits and Data [1] is low 8 bits) as following:

0000: the operation is completed successfully.

FFFF: no response from module.

FFFE: module is busy. You can make the module to be free by issuing Stop Inventory command.

FF00:the module is closed.

Others: not defined.

2.2.17 Get Tag Return Mode

Command to RFID module:

CMD ID	P0	P1	P2	P3
0xBD	0x00	0x00	0x00	0x00
1 Byte	1 Byte	1 Byte	1 Byte	1 Byte

Response from RFID module:

CMD ID	D0	result
0xBE	0x02	result
1 Byte	1 Byte	2 Byte

The meaning of result code (Data [0] is the high 8 bits and Data [1] is low 8 bits) as following:

0000: the operation is completed successfully.

FFFF: no response from module.

FFFE: module is busy. You can make the module to be free by issuing Stop Inventory command.

FF00:the module is closed.

Others: not defined.

2.2.18 Heartbeat Packet

Support Port: Ethernet

Pre-condition:

1) Ecube is connected with host through TCP

- 2) UHF module is opened
- 3) device is in idle state at least 3000 ms

if conditions above is reached,then uhf device will send Heartbeat packet to host.

response from RFID module:

CMD ID	D0	Data
0xaf	0x02	00 00
1 Byte	1 Byte	2 Byte

2.2.19 Enable Heartbeat Packet

Support Port: Ethernet

Command to RFID module:

CMD ID	P0	P1	P2	P3
0xae	Enable	0x00	0x00	0x00
1 Byte	1 Byte	1 Byte	1 Byte	1 Byte

if Enable =1, then heartbeat packet will be used.

if Enable =0, then heartbeat packet will not be used.

Response from RFID module:

CMD ID	D0	Data
0xae	0x02	Result code
1 Byte	1 Byte	2Byte

The meaning of result code (Data [0] is the high 8 bits and Data [1] is low 8 bits) as following:

0000: the operation is completed successfully.

FFFF: no response from module.

FFFE: module is busy. You can make the module to be free by issuing Stop Inventory command.

FF00:the module is closed.

Others: not defined.

2.2.20 Test Channel Performance

This command is used to test channel performance.

Command to RFID module:

CMD ID	P0	P1	P2	P3
0xC1	ant_port	ant_power	reverse_power_threshold	0x00
1 Byte	1 Byte	1 Byte	1 Byte	1 Byte

ant_port is the antenna port should be test;

ant_power is power of selected antenna port;

reverse_power_threshold is the threshold of reverse power.

For example, if we want to find the reverse power should be less than 10dB while ant_port is 0 and ant_power is 30dB, then

ant_port=0,

ant_power=0x1E,

reverse_power_threshold=0x0a;

channel_num and fixed frequency is mapped as following:

channel_num	freq(MHz)
0	915.75
1	915.25
2	903.25
3	926.75
4	926.25
5	904.25
6	927.25
7	920.25
8	919.25
9	909.25
10	918.75
11	917.75
12	905.25
13	904.75
14	925.25
15	921.75
16	914.75
17	906.75
18	913.75
19	922.25
20	911.25
21	911.75
22	903.75
23	908.75
24	905.75
25	912.25
26	906.25

27	917.25
28	914.25
29	907.25
30	918.25
31	916.25
32	910.25
33	910.75
34	907.75
35	924.75
36	909.75
37	919.75
38	916.75
39	913.25
40	923.75
41	908.25
42	925.75
43	912.75
44	924.25
45	921.25
46	920.75
47	922.75
48	902.75
49	923.25

Response from RFID module:

CMD ID	D0	channel_num	Forward_power	Reverse_power
0xCC	0x09	channel_num	Forward_power	Reverse_power
1 Byte	1 Byte	1 Byte	4 Byte	4 Byte

**test will return 50 responses (forward_power+reverse_power)+last_response
last reponse:**

CMD ID	D0	Data	Freq_mask0	Freq_mask1
0xC1	0x0a	result code	Freq_mask0	Freq_mask0
1 Byte	1 Byte	2 Byte	4 Byte	4 Byte

if channel 0 is good , then bit0 of freq_mask0 is 1;otherwise it is 0;
and so forth;

if channel 32 is good, then bit0 of freq_mask1 is 1; otherwise it is 0;

and so forth;

The meaning of result code (Data [0] is the high 8 bits and Data [1] is low 8 bits) as following:

0000: the operation is completed successfully.

FFFF: no response from module.

FFFE: module is busy. You can make the module to be free by issuing Stop Inventory command.

FF00:the module is closed.

Others: not defined.

2.2.21 Set Optimal Freq Channel

This command is used to set optimal freq.

Command to RFID module:

CMD ID	P0	P1	P2	P3
0xC2	0x00	0x00	0x00	0x00
1 Byte	1 Byte	1 Byte	1 Byte	1 Byte

Response from RFID module:

CMD ID	D0	Data
0xC2	0x02	result code
1 Byte	1 Byte	2 Byte

The meaning of result code (Data [0] is the high 8 bits and Data [1] is low 8 bits) as following:

0000: the operation is completed successfully.

FFFF: no response from module.

FFFE: module is busy. You can make the module to be free by issuing Stop Inventory command.

FF00:the module is closed.

FFF0: no good channel

Others: not defined.

2.2.22 Get Optimal Freq Channel

This command is used to get the optimal freq

Command to RFID module:

CMD ID	P0	P1	P2	P3
0xC3	0x00	0x00	0x00	0x00
1 Byte	1 Byte	1 Byte	1 Byte	1 Byte

Response from RFID module:

CMD ID	D0	Data	Freq_mask0	Freq_mask1
0xC3	0x0a	result code	Freq_mask0	Freq_mask0
1 Byte	1 Byte	2 Byte	4 Byte	4 Byte

if channel 0 is good , then bit0 of freq_mask0 is 1;otherwise it is 0;
and so forth;
channel definition is as channel_num in 2.2.13

if channel 32 is good, then bit0 of freq_mask1 is 1; otherwise it is 0;
and so forth;

The meaning of result code (Data [0] is the high 8 bits and Data [1] is low 8 bits) as following:

0000: the operation is completed successfully.

FFFF: no response from module.

FFFE: module is busy. You can make the module to be free by issuing Stop Inventory command.

FF00:the module is closed.

FFF0: no good channel

Others: not defined.

2.2.23 Get UHF Module Version

This command is used to set optimal freq.

Command to RFID module:

CMD ID	P0	P1	P2	P3
0xC7	0x00	0x00	0x00	0x00
1 Byte	1 Byte	1 Byte	1 Byte	1 Byte

Response from RFID module:

CMD ID	D0	Result	Data	
0xC7	0x04	Result code	Major Version	Minor Version
1 Byte	1 Byte	2 Byte	1 Byte	1 Byte

The meaning of result code (Data [0] is the high 8 bits and Data [1] is low 8 bits) as following:

0000: the operation is completed successfully.

FFFF: no response from module.

FFFE: module is busy. You can make the module to be free by issuing Stop Inventory command.

FF00:the module is closed.

Others: not defined.

2.2.24 Check Antenna status

Command to RFID module:

CMD ID	P0	P1	P2	P3
0xC9	Ant0_Check	Ant1_Check	Ant2_Check	Ant3_Check
1 Byte	1 Byte	1 Byte	1 Byte	1 Byte

if Ant0_check==1, then Antenna port 0 will be checked;

if Ant1_check==1, then Antenna port 1will be checked;

if Ant2_check==1, then Antenna port 2 will be checked;

if Ant3_check==1, then Antenna port 3 will be checked;

Response from RFID module:

CMD ID	D0	Data	Check Result
0xC9	0x06	result code	check_result
1 Byte	1 Byte	2 Byte	4 Byte

if Ant0_check ==0, then check_result[0]=0

else if(ant0_check==1) and antenna0 is connected, then check_result[0]=1

if Ant1_check ==0, then check_result[1]=0

else if(ant1_check==1) and antenna1 is connected, then check_result[1]=1

else if (ant1_check==1) and antenna1 is disconnected, then check_result[1]=2

if Ant2_check ==0, then check_result[2]=0

else if(ant2_check==1) and antenna2 is connected, then check_result[2]=1

else if (ant2_check==1) and antenna2 is disconnected, then check_result[2]=2

if Ant3_check ==0, then check_result[3]=0

else if(ant3_check==1) and antenna3 is connected, then check_result[3]=1

else if (ant3_check==1) and antenna3 is disconnected, then check_result[3]=2

The meaning of result code (Data [0] is the high 8 bits and Data [1] is low 8 bits) as following:

0000: the operation is completed successfully.

FFFF: no response from module.

FFFE: module is busy. You can make the module to be free by issuing Stop Inventory command.

FF00:the module is closed.

FFF0: no good channel

Others: not defined.

2.2.25 set antenna dwell time

Command to RFID module:

CMD ID	P0	P1	P2	P3
0xca	time3	time2	time1	time0
1 Byte	1 Byte	1 Byte	1 Byte	1 Byte

dwelltime =(time3<<24)|(time2<<16)|(time1<<8)|time0

Response from RFID module:

CMD ID	D0	result
0xca	0x02	result
1 Byte	1 Byte	2 Byte

The meaning of result code (Data [0] is the high 8 bits and Data [1] is low 8 bits) as following:

0000: the operation is completed successfully.

FFFF: no response from module.

FFFE: module is busy. You can make the module to be free by issuing Stop Inventory command.

FF00:the module is closed.

Others: not defined.

2.2.26 Set GPO

Command to RFID module:

CMD ID	P0	P1	P2	P3
0xCE	Gpo0	Gpo1	0x00	0x00
1 Byte	1 Byte	1 Byte	1 Byte	1 Byte

if Gpo0=1, then GPO0 is set as output high

if Gpo0=0, then GPO0 is set as output low

if Gpo1=1, then Gpo1 is set as output high

if Gpo1=0, then Gpo1 is set as output low

Response from RFID module:

CMD ID	D0	Data
0xCE	0x02	result code
1 Byte	1 Byte	2 Byte

The meaning of result code (Data [0] is the high 8 bits and Data [1] is low 8 bits) as following:

0000: the operation is completed successfully.

FFFF: no response from module.

FFFE: module is busy. You can make the module to be free by issuing Stop Inventory command.

FF00: the module is closed.

Others: not defined.

Response:

No response

2.2.27 Set GPI

Command to RFID module:

CMD ID	P0	P1	P2	P3
0xCD	Gpi0	Gpi1	0x00	0x00
1 Byte	1 Byte	1 Byte	1 Byte	1 Byte

when you want to trig inventory tag by GPIO, you may set this command.

if Gpi0=0, then GPIO0 is not set;

if Gpi0=1, then inventory is triggered when Gpi0's falling edge and is stopped by Gpi0's rising edge.
 If the value of Gpi0 changes from high to low, then B2 04 01 00 00 00 will be returned to host; if
 the value of Gpi0 changes from low to high, then B2 04 01 00 01 00 will be returned to host.

if Gpi0=2, then Gpi0 is set as input pin. If the value of Gpi0 changes from high to low, then B2 04
 02 00 00 00 will be returned to host; if the value of Gpi0 changes from low to high, then B2 04 02
 00 01 00 will be returned to host.

if Gpi1=0, then Gpi1 is not set;

if Gpi1=1, then inventory is triggered when Gpi1's falling edge and is stopped by Gpi1's rising edge .
 If the value of Gpi1 changes from high to low, then B2 04 00 01 00 00 will be returned to host; if
 the value of GPI1 changes from low to high, then B2 04 00 01 00 01 will be returned to host.

if Gpi1=2, then GPI1 is set as input pin. If the value of GPI1 changes from high to low, then B2 04
 00 02 00 00 will be returned to host; if the value of GPI1 changes from low to high, then B2 04 00
 02 00 01 will be returned to host.

Response from RFID module:

CMD ID	D0	Data
0xCD	0x02	result code
1 Byte	1 Byte	2 Byte

The meaning of result code (Data [0] is the high 8 bits and Data [1] is low 8 bits) as following:

0000: the operation is completed successfully.

FFFF: no response from module.

FFFE: module is busy. You can make the module to be free by issuing Stop Inventory command.

FF00:the module is closed.

Others: not defined.

if GPIO or GPI1 is set to 1 or 2,when the value of GPI changes from high to low of visa, response
 is:

CMD ID	D0	GPIO setting	data
0xB2	0x04	setting	data
1 Byte	1 Byte	2 Byte	2 Byte

2.2.28 Set Profile

Command to RFID module:

CMD ID	P0	P1	P2	P3
0x86	profile	0x00	0x00	0x00
1 Byte	1 Byte	1 Byte	1 Byte	1 Byte

we can set profile between 0~3

Response from RFID module:

CMD ID	D0	Data
0x86	0x02	result code
1 Byte	1 Byte	2 Byte

The meaning of result code (Data [0] is the high 8 bits and Data [1] is low 8 bits) as following:

0000: the operation is stopped successfully.

FFFF: no response from module.

FF00:the module is closed.

Others: not defined.

Ex:

Send: 86 00 00 00 00 (set profile)

Response:86 02 00 00 (set profile successfully)

2.2.29 Get Profile

Command to RFID module:

CMD ID	P0	P1	P2	P3
0x87	0x00	0x00	0x00	0x00
1 Byte	1 Byte	1 Byte	1 Byte	1 Byte

Response from RFID module:

CMD ID	D0	Data	profile
0x87	0x03	result code	profile
1 Byte	1 Byte	2 Byte	1 byte

The meaning of result code (Data [0] is the high 8 bits and Data [1] is low 8 bits) as following:

0000: the operation is stopped successfully.

FFFF: no response from module.

FF00:the module is closed.

Others: not defined.

Ex:

Send: 87 00 00 00 00 (get profile)

Response:87 03 00 00 01 (get profile successfully, the current profile is 1)

2.2.30 Get dwell time

Command to RFID module:

CMD ID	P0	P1	P2	P3
0x60	0x00	0x00	0x00	0x00
1 Byte	1 Byte	1 Byte	1 Byte	1 Byte

Response from RFID module:

CMD ID	D0	Data	dwell time
0x60	0x06	result code	time3,time2,time1,time0
1 Byte	1 Byte	2 Byte	4 byte

if time3=0x00,time2=0x00,time1=0x00,time0=0xc8, then the dwell time is equal to 0x000000c8

The meaning of result code (Data [0] is the high 8 bits and Data [1] is low 8 bits) as following:

0000: the operation is stopped successfully.

FFFF: no response from module.

FF00:the module is closed.

Others: not defined.

Ex:

Send: 60 00 00 00 00 (get dwell time)

Response:60 06 00 00 00 00 c8 (get dwell time successfully, the current dwell time is 0x000000c8 ms, equal to 200 ms)

2.3 UHF Inventory & Access

2.3.1 Start Inventory

Command to RFID module:

CMD ID	P0	P1	P2	P3
0xF1	P0	0x00	0x00	0x00
1 Byte	1 Byte	1 Byte	1 Byte	1 Byte

If P0=0x00, then all tags in scope will be return many times(repeated tags also be returned)

if P0=0x01, then all tags in scope will be return only one time

Notice: if P0=0x01, the length of EPC must <=12 Bytes, and the total tags count is less 1000. otherwise there will be error occurred.

Normal Response from RFID module:

CMD ID	D0	Data
0xF1	Data of length	Ant No[0] + RSSI[1~2] + EPC Data[3~]
1 Byte	1 Byte	

Notice: RSSI value, its data type is a signed int16

For example, RSSI is 0xFEED, then RSSI=-275

Because the unit of RSSI is 0.1 dB, so the real RSSI is -27.5 dB

Error Response from RFID module:

CMD ID	D0	Data
0xF1	0x02	Error code
1 Byte	1 Byte	2 Byte

FFFF: no response from module.

FFFE: module is busy. You can make the module to be free by issuing Stop Inventory command.

FF00:the module is closed.

0000: Inventory is stopped without error.

Others: Inventory is stopped with some error.

2.3.2 Stop Inventory

Command to RFID module:

CMD ID	P0	P1	P2	P3
0xF2	0x00	0x00	0x00	0x00
1 Byte	1 Byte	1 Byte	1 Byte	1 Byte

Response from RFID module:

CMD ID	D0	Data
0xF2	0x02	result code
1 Byte	1 Byte	2 Byte

The meaning of result code (Data [0] is the high 8 bits and Data [1] is low 8 bits) as following:

0000: the operation is stopped successfully.

FFFF: no response from module.

FFFE: module is busy. You can make the module to be free by issuing Stop Inventory command.

FF00:the module is closed.

Others: not defined.

2.3.3 set access password

Command to RFID module:

CMD ID	P0	P1	P2	P3
0xBA	Pwd0	Pwd1	Pwd2	Pwd3
1 Byte	1 Byte	1 Byte	1 Byte	1 Byte

This command is used with access operations, such as read, write, lock, unlock, or kill.

before you send access operation, you may issue this command firstly. if you send access operation without sending this command, then the default access password is 0x00.

For example, if you want to set access password to 0x12345678,then

Pwd0=0x12, Pwd1=0x34, Pwd2=0x56, Pwd3=0x78

Response from RFID module:

This command have no response. After you issue it ,you can send access command immediately.

2.3.4 Write Data to Tag

Command to RFID module:

CMD ID	P0	P1	P2	P3	Data
--------	----	----	----	----	------

0xF7	bank	offset	length	0x00	New EPC Data
1 Byte	1 Byte	1 Byte	1 Byte	1 Byte	Length Byte

P0=0x00, reserved bank

P0=0x01, EPC bank

P0=0x02, TID bank

P0=0x03, User bank

if P0!=0x01, then offset must be multiples of 2

if P0==0x01, then offset must be 0

P3 P1 is offset from the P0 bank; if P3=0x01, P1=0x00, then offset=0x0100

(offset must be multiples of 2)

P2 is the data of length

Notice: data length must be Multiples of 4 and must not be greater than 240.

For example, if you want to revise the value of EPC to 12345678,

The setting is P0=1, P1=0, P2=4, Data=0x12345678

Response from RFID module:

CMD ID	D0	Data
0xF7	0x02	result code
1 Byte	1 Byte	2 Byte

The meaning of result code (Data [0] is the high 8 bits and Data [1] is low 8 bits) as following:

0000: the operation is completed successfully.

FFFF: no response from module.

FFFE: module is busy. You can make the module to be free by issuing Stop Inventory command.

FF00: the module is closed.

Others: not defined.

2.3.5 Read Data from Tag

Command to RFID module:

CMD ID	P0	P1	P2	P3
0xFB	bank	offset	length0	0
1 Byte	1 Byte	1 Byte	1 Byte	1 Byte

P0=0x00, reserved bank

P0=0x01, EPC bank

P0=0x02, TID bank

P0=0x03, User bank

P3 P1 is offset from the P0 bank; if P3=0x01,P1=0x00, then offset=0x0100

(offset must be multiples of 2)

P2 is the data of length

Notice: data length must be Multiples of 2 and must not be greater than 240.

Response from RFID module:

CMD ID	D0	Data	
0xFB	2+ Len	result code	Read data
1 Byte	1 Byte	2 Byte	Len Byte

The meaning of result code (Data [0] is the high 8 bits and Data [1] is low 8 bits) as following:

0000: the operation is completed successfully.

FFFF: no response from module.

FFFE: module is busy. You can make the module to be free by issuing Stop Inventory command.

FF00:the module is closed.

Others: not defined.

if result Code !=0000, then

Len=0

2.3.6 Lock Tag

Command to RFID module:

CMD ID	P0	P1	P2	P3
0xFC	Password0	Password1	Password2	Password3
1 Byte	1 Byte	1 Byte	1 Byte	1 Byte

when you want to lock a tag, you must provide a 32bit password(it can't be all zero)

for example, if you want to use 0x12345678 as password, then

Password0=0x12

Password1=0x34

Password2=0x56

Password3=0x78

when you lock a tag, Password0~Password3 can't all be zero

Response from RFID module:

CMD	D0	Data
-----	----	------

ID		
0xFC	0x02	result code
1 Byte	1 Byte	2 Byte

The meaning of result code (Data [0] is the high 8 bits and Data [1] is low 8 bits) as following:

0000: the operation is completed successfully.

FFFF: no response from module.

FFFE: module is busy. You can make the module to be free by issuing Stop Inventory command.

FFFD: invalid password

FF00:the module is closed.

Others: not defined.

2.3.7 Unlock Tag

Command to RFID module:

CMD ID	P0	P1	P2	P3
0xFD	Password0	Password1	Password2	Password3
1 Byte	1 Byte	1 Byte	1 Byte	1 Byte

when you want to unlock a tag, you must provide a 32bit password(it can't be all zero)

for example, if you want to use 0x12345678 as password, then

Password0=0x12

Password1=0x34

Password2=0x56

Password3=0x78

when you lock a tag, Password0~Password3 can't all be zero

Response from RFID module:

CMD ID	D0	Data
0xFD	0x02	result code
1 Byte	1 Byte	2 Byte

The meaning of result code (Data [0] is the high 8 bits and Data [1] is low 8 bits) as following:

0000: the operation is completed successfully.

FFFF: no response from module.

FFFE: module is busy. You can make the module to be free by issuing Stop Inventory command.

FFFD: invalid password

FF00:the module is closed.

Others: not defined.

2.3.8 Kill Tag

Command to RFID module:

CMD ID	P0	P1	P2	P3
0xFE	Password0	Password1	Password2	Password3
1 Byte	1 Byte	1 Byte	1 Byte	1 Byte

when you want to kill a tag, you must provide a 32bit password(it can't be all zero)

for example, if you want to use 0x12345678 as password, then

Password0=0x12

Password1=0x34

Password2=0x56

Password3=0x78

kill password must not be zero

Response from RFID module:

CMD ID	D0	Data
0xFE	0x02	result code
1 Byte	1 Byte	2 Byte

The meaning of result code (Data [0] is the high 8 bits and Data [1] is low 8 bits) as following:

0000: the operation is completed successfully.

FFFF: no response from module.

FFFE: module is busy. You can make the module to be free by issuing Stop Inventory command.

FFFD: invalid kill password

FF00:the module is closed.

Others: not defined.

2.3.9 Block Write Data to Tag

Command to RFID module:

CMD ID	P0	P1	P2	P3	Data
0xC0	bank	offset	Length	0x00	Data
1 Byte	1 Byte	1 Byte	1 Byte	1 Byte	Length Byte

P0=0x00, reserved bank

P0=0x01, EPC bank

P0=0x02, TID bank

P0=0x03, User bank

if P0!=0x01, then offset must be multiples of 4

if P0==0x01, then offset must be 0

P3 P1 is offset from the P0 bank; if P3=0x01, P1=0x00, then offset=0x0100
(offset must be multiples of 2)

P2 is the data of length

Notice: data length must be Multiples of 2 and must not be greater than 240.

For example, if you want to revise the value of EPC to 12345678,
The setting is P0=1, P1=0, P2=4, Data=0x12345678

Response from RFID module:

CMD ID	D0	Data
0xC0	0x02	result code
1 Byte	1 Byte	2 Byte

The meaning of result code (Data [0] is the high 8 bits and Data [1] is low 8 bits) as following:

0000: the operation is completed successfully.

FFFF: no response from module.

FFFE: module is busy. You can make the module to be free by issuing Stop Inventory command.

FF00: the module is closed.

Others: not defined.

2.3.10 Group Read Data From Tag

Command to RFID module:

CMD ID	P0	P1	P2	P3
0xC4	bank	offset	length0	0
1 Byte	1 Byte	1 Byte	1 Byte	1 Byte

P0=0x00, reserved bank

P0=0x01, EPC bank

P0=0x02, TID bank

P0=0x03, User bank

P3 P1 is offset from the P0 bank; if P3=0x01, P1=0x00, then offset=0x0100
(offset must be multiples of 2)

P2 is the data of length

Notice: data length must be Multiples of 2 and must not be greater than 240.

Response from RFID module:

CMD ID	D0	Data
0xC4	Epc_len+data_len+2	result code
1 Byte	1 Byte	2 Byte

epc

CMD ID	D0	Data
0xF1	Data_len	Ant_No[0] + RSSI[1~2] + EPC_Data[3~]
1 Byte	1 Byte	

data

CMD ID	D0	Data	
0xFB	2+ Len	result code	Read data
1 Byte	1 Byte	2 Byte	Len Byte

The meaning of result code (Data [0] is the high 8 bits and Data [1] is low 8 bits) as following:

0000: the operation is completed successfully.

FFFF: no response from module.

FFFE: module is busy. You can make the module to be free by issuing Stop Inventory command.

FF00: the module is closed.

Others: not defined.

if result Code !=0000, then Len=0

2.3.11 Perm Lock Tag**Command to RFID module:**

CMD ID	P0	P1	P2	P3
--------	----	----	----	----

0xC5	EPC_Perm	USER_Perm	0x00	0x00
1 Byte	1 Byte	1 Byte	1 Byte	1 Byte

if EPC_Perm==0, then EPC perm lock operation will not be executed ,
else if EPC_Perm==1, then EPC perm lock operation will be executed

if USER_Perm ==0, then USER perm lock operation will not be executed
else if USER_Perm ==1, then USER perm lock operation will be executed

Once you perm lock a tag on the selected banks, then the selected banks can't be written forever.

Response from RFID module:

CMD ID	D0	Data
0xC5	0x02	result code
1 Byte	1 Byte	2 Byte

The meaning of result code (Data [0] is the high 8 bits and Data [1] is low 8 bits) as following:

0000: the operation is completed successfully.

FFFF: no response from module.

FFFE: module is busy. You can make the module to be free by issuing Stop Inventory command.

FF00:the module is closed.

Others: not defined.

2.3.12 Perm Unlock Tag

Command to RFID module:

CMD ID	P0	P1	P2	P3
0xC6	EPC_Perm	USER_Perm	0x00	0x00
1 Byte	1 Byte	1 Byte	1 Byte	1 Byte

if EPC_Perm==0, then EPC perm lock operation will not be executed ,
else if EPC_Perm==1, then EPC perm lock operation will be executed

if USER_Perm ==0, then USER perm lock operation will not be executed
else if USER_Perm ==1, then USER perm lock operation will be executed

Once you perm lock a tag on the selected banks, then the selected banks can't be written forever.

Response from RFID module:

CMD ID	D0	Data
0xC6	0x02	result code
1 Byte	1 Byte	2 Byte

The meaning of result code (Data [0] is the high 8 bits and Data [1] is low 8 bits) as following:

0000: the operation is completed successfully.

FFFF: no response from module.

FFFE: module is busy. You can make the module to be free by issuing Stop Inventory command.

FF00: the module is closed.

Others: not defined.

2.3.13 Single Read EPC and Data From Tag

Command to RFID module:

CMD ID	P0	P1	P2	P3
0xC8	bank	offset	length0	0
1 Byte	1 Byte	1 Byte	1 Byte	1 Byte

P0=0x00, reserved bank

P0=0x01, EPC bank

P0=0x02, TID bank

P0=0x03, User bank

P3 P1 is offset from the P0 bank; if P3=0x01, P1=0x00, then offset=0x0100

(offset must be multiples of 2)

P2 is the data of length

Notice: data length must be Multiples of 2 and must not be greater than 240.

Normal Response from RFID module:

CMD ID	D0	Data
0xC8	Epc_len+data_len+2	result code
1 Byte	1 Byte	2 Byte

epc

CMD ID	D0	Data
--------	----	------

0xF1	Data_len	Ant_No[0] + RSSI[1~2] + EPC_Data[3~]
1 Byte	1 Byte	

data

CMD ID	D0	Data	
0xFB	2+ Len	result code	Read data
1 Byte	1 Byte	2 Byte	Len Byte

Error Response from RFID module:

CMD ID	D0	Data
0xC8	0x02	Error code
1 Byte	1 Byte	2 Byte

The meaning of result code (Data [0] is the high 8 bits and Data [1] is low 8 bits) as following:

0000: the operation is completed successfully.

FFFF: no response from module.

FFFE: module is busy. You can make the module to be free by issuing Stop Inventory command.

FF00: the module is closed.

Others: not defined.

if result Code !=0000, then Len=0

2.3.14 Set QT Control

Command to RFID module:

CMD ID	P0	P1	P2	P3
0xB9	public_private	0	0	0
1 Byte	1 Byte	1 Byte	1 Byte	1 Byte

if public_private==0, then set the QT tag to public region

else if public_private==1, then set the QT tag to private region

Normal Response from RFID module:

CMD ID	D0	Data
0xB9	0x02	result code
1 Byte	1 Byte	2 Byte

The meaning of result code (Data [0] is the high 8 bits and Data [1] is low 8 bits) as following:

0000: the operation is completed successfully.

FFFF: no response from module.

FFFE: module is busy. You can make the module to be free by issuing Stop Inventory command.

FF00: the module is closed.

Others: not defined.

2.2.15 Read Data with password

Command to RFID module:

CMD ID	P0	P1	P2	P3	P4	P5	P6	P7
0x80	bank	offset	length0	0	Pwd0	Pwd1	Pwd2	Pwd3
1 Byte	1 Byte	1 Byte	1 Byte	1 Byte	1 Byte	1 Byte	1 Byte	1 Byte

P0=0x00, reserved bank

P0=0x01, EPC bank

P0=0x02, TID bank

P0=0x03, User bank

P3 P1 is offset from the P0 bank; if P3=0x01, P1=0x00, then offset=0x0100

(offset must be multiples of 2)

P2 and the read data of length(must be multiples of 2), the max value of length is 240 bytes

Pwd0~Pwd3 is password for read operation.

For example, if you want to set access password to 0x12345678, then

Pwd0=0x12, Pwd1=0x34, Pwd2=0x56, Pwd3=0x78

Response from RFID module:

CMD ID	D0	Data	
0x80	2+ Len	result code	Read data
1 Byte	1 Byte	2 Byte	Len Byte

The meaning of result code (Data [0] is the high 8 bits and Data [1] is low 8 bits) as following:

0000: the operation is completed successfully.

FFFF: no response from module.

FFFE: module is busy. You can make the module to be free by issuing Stop Inventory command.

FF00:the module is closed.

Others: not defined.

if result Code !=0000, then Len=0

Ex:

Send:80 02 00 04 00 00 00 00 00 (read Tid , offset=0, len=0x04 bytes, password is 0x00000000)

Response: 80 06 00 00 E2 80 B0 40

(read Tid successfully)

2.2.16 Write Data with password

Command to RFID module:

CMD ID	P0	P1	P2	P3	P4	P5	P6	P7	Data
0x81	bank	offset	Length	0x00	Pwd0	Pwd1	Pwd2	Pwd3	Data
1 Byte	1 Byte	1 Byte	1 Byte	1 Byte	1 Byte	1 Byte	1 Byte	1 Byte	Length Byte

P0=0x00, reserved bank

P0=0x01, EPC bank

P0=0x02, TID bank

P0=0x03, User bank

if P0!=0x01, then offset must be multiples of 2

if P0==0x01,then offset must be 0

P3 P1 is offset from the P0 bank; if P3=0x01,P1=0x00, then offset=0x0100

(offset must be multiples of 2)

P2 is the data of length

Notice: data length must be Multiples of 2 and must not be greater than 128.

Pwd0~Pwd3 is password for read operation.

For example, if you want to set access password to 0x12345678,then

Pwd0=0x12, Pwd1=0x34, Pwd2=0x56, Pwd3=0x78

For example, if you want to revise the value of EPC to 12345678,
The setting is P0=1, P1=0, P2=4, Data=0x12345678

Response from RFID module:

CMD ID	D0	Data
0x81	0x02	result code
1 Byte	1 Byte	2 Byte

The meaning of result code (Data [0] is the high 8 bits and Data [1] is low 8 bits) as following:

0000: the operation is completed successfully.

FFFF: no response from module.

FFFE: module is busy. You can make the module to be free by issuing Stop Inventory command.

FF00: the module is closed.

Others: not defined.

Ex:

Send: 81 01 00 04 00 12 34 56 78 12 34 56 78 (revise epc to 12 34 56 78, password is 0x12345678)

Response: 81 02 00 00 (revise epc successfully)

Ex:

Send: 81 03 00 04 00 12 34 56 78 12 34 56 78 (write user, offset=0x00 byte, length=0x04 byte, write data= 12 34 56 78, password is 0x12345678)

Response: 81 02 00 00 (write data to user successfully)

2.2.17 Block Write data with password

Command to RFID module:

CMD ID	P0	P1	P2	P3	P4	P5	P6	P7	Data
0x82	bank	offset	Length	0x00	Pwd0	Pwd1	Pwd2	Pwd3	Data
1 Byte	1 Byte	1 Byte	1 Byte	1 Byte	1 Byte	1 Byte	1 Byte	1 Byte	Length Byte

P0=0x00, reserved bank

P0=0x01, EPC bank

P0=0x02, TID bank

P0=0x03, User bank

if P0!=0x01, then offset must be multiples of 2

if P0==0x01, then offset must be 0

P3 P1 is offset from the P0 bank; if P3=0x01, P1=0x00, then offset=0x0100
(offset must be multiples of 2)

P2 is the data of length

Notice: data length must be Multiples of 2 and must not be greater than 128.

Pwd0~Pwd3 is password for read operation.

For example, if you want to set access password to 0x12345678, then

Pwd0=0x12, Pwd1=0x34, Pwd2=0x56, Pwd3=0x78

For example, if you want to revise the value of EPC to 12345678,

The setting is P0=1, P1=0, P2=4, Data=0x12345678

Response from RFID module:

CMD ID	D0	Data
0x82	0x02	result code
1 Byte	1 Byte	2 Byte

The meaning of result code (Data [0] is the high 8 bits and Data [1] is low 8 bits) as following:

0000: the operation is completed successfully.

FFFF: no response from module.

FFFE: module is busy. You can make the module to be free by issuing Stop Inventory command.

FF00: the module is closed.

Others: not defined.

Ex:

Send: 82 01 00 04 00 12 34 56 78 12 34 56 78 (revise epc to 12 34 56 78, password is 0x12345678)

Response: 82 02 00 00 (revise epc successfully)

Ex:

Send: 82 03 00 04 00 12 34 56 78 12 34 56 78 (write user, offset=0x00 byte, length=0x04 byte, write data= 12 34 56 78, password is 0x12345678)

Response: 82 02 00 00 (write data to user successfully)

3. Storage Command

Storage Command include the following commands:

- 1) Read Block Data
- 2) Read Block Count
- 3) Write Block Data
- 4) Get Block Size
- 5) Initial Storage Data

3.1 Read Block Data

Command to RFID module:

CMD ID	P0	P1	P2	P3
0xD0	Count0	Count1	0x00	0x00
1 Byte	1 Byte	1 Byte	1 Byte	1 Byte

when you want to read a block from flash, you may set this command.

if you want to read block 10(decimal), then

Count0=0x00

Count1=0x0A

Response from RFID module:

CMD ID	D0	result	Data
0xD0	2+block_size	result code	Block data
1 Byte	1 Byte	2 Byte	block_size Byte

The meaning of result code (Data [0] is the high 8 bits and Data [1] is low 8 bits) as following:

0000: the operation is completed successfully.

FFFE: module is busy. You can make the module to be free by issuing Stop Inventory command.

FFFD: the access block count exceeds the current max counts.

FF00:the module is closed.

Others: not defined.

3.2 Read Block Count

Command to RFID module:

CMD ID	P0	P1	P2	P3
0xD1	0x00	0x00	0x00	0x00
1 Byte	1 Byte	1 Byte	1 Byte	1 Byte

This command tries to acquire the current block count

Response from RFID module:

CMD ID	D0	Data	Block Count
0xD1	0x04	result code	Count0~Count1
1 Byte	1 Byte	2 Byte	2 Byte

The meaning of result code (Data [0] is the high 8 bits and Data [1] is low 8 bits) as following:

0000: the operation is completed successfully.

FFFE: module is busy. You can make the module to be free by issuing Stop Inventory command.

FF00: the module is closed.

Others: not defined.

Only when result code is 0000, Count0~Count1 is meaningful

if Count0=0x00, Count1=0x0A

Then the current block count is 10(Decimal)

3.3 Write Block Data

Command to RFID module:

CMD ID	P0	P1	P2	P3	Data
0xD2	Count0	Count1	0x00	0x00	Block data
1 Byte	1 Byte	1 Byte	1 Byte	1 Byte	Block_size Byte

when you want to write a block to flash, you may set this command.

if you want to write block 10(decimal), then

Count0=0x00

Count1=0x0A

Response from RFID module:

CMD ID	D0	Data
0xD2	0x02	result code
1 Byte	1 Byte	2 Byte

The meaning of result code (Data [0] is the high 8 bits and Data [1] is low 8 bits) as following:

0000: the operation is completed successfully.

FFFE: module is busy. You can make the module to be free by issuing Stop Inventory command.

FFFD: the access block count exceeds the current max counts+1. This can make the storage non-continuous.

FF00:the module is closed.

Others: not defined.

3.4 Get Block Size

Command to RFID module:

CMD ID	P0	P1	P2	P3
0xD3	0x00	0x00	0x00	0x00
1 Byte	1 Byte	1 Byte	1 Byte	1 Byte

when you want to read block size from flash, you may set this command.

Response from RFID module:

CMD ID	D0	Data	Size
0xD3	0x03	result code	Block size
1 Byte	1 Byte	2 Byte	1 Byte

The meaning of result code (Data [0] is the high 8 bits and Data [1] is low 8 bits) as following:

0000: the operation is completed successfully.

FFFE: module is busy. You can make the module to be free by issuing Stop Inventory command.

FF00:the module is closed.

Others: not defined.

Only when the result code is 0000, block size is meaningful.

3.5 Initial Storage Data

Command to RFID module:

CMD ID	P0	P1	P2	P3
--------	----	----	----	----

0xD4	size	0x00	0x00	0x00
1 Byte	1 Byte	1 Byte	1 Byte	1 Byte

when you want to Initial flash Data Region, you may set this command.
size is the block size.

Notice: block size must less than 0x10

Response from RFID module:

CMD ID	D0	Data
0xD4	0x02	result code
1 Byte	1 Byte	2 Byte

The meaning of result code (Data [0] is the high 8 bits and Data [1] is low 8 bits) as following:

0000: the operation is completed successfully.

FFFE: module is busy. You can make the module to be free by issuing Stop Inventory command.

FF00:the module is closed.

Others: not defined.

4. IP Setting Command

IP command includes the following commands:

- 1) Set IP Address
- 2) Set TCP Port
- 3) Set Subnet Mask
- 4) Set Gateway
- 5) Enable or Disable DHCP
- 6) Get IP configuration

4.1 Set IP Address

Command to RFID module:

CMD ID	P0	P1	P2	P3
0xE4	IP0	IP1	IP2	IP3
1 Byte	1 Byte	1 Byte	1 Byte	1 Byte

when you want to set IP address, you may set this command.

For example, if you want to set IP to 192.168.100.123

then

IP0=0xC0(192 decimal)

IP1=0xA8(168 decimal)

IP2=0x64(100 decimal)

IP3=0x7B(123 decimal)

Response from RFID module:

CMD ID	D0	Data
0xE4	0x02	result code
1 Byte	1 Byte	2 Byte

The meaning of result code (Data [0] is the high 8 bits and Data [1] is low 8 bits) as following:

0000: the operation is completed successfully.

FFFE: module is busy. You can make the module to be free by issuing Stop Inventory command.

FF00:the module is closed.

Others: not defined.

4.2 Set TCP Port

Command to RFID module:

CMD ID	P0	P1	P2	P3
0xE5	Port0	Port1	Port2	Port3
1 Byte	1 Byte	1 Byte	1 Byte	1 Byte

when you want to set TCP Port, you may set this command.

for example, if you want set TCP port to 9671(0x000025C7)

then

Port0=0x00

Port1=0x00

Port2=0x25

Port3=0xC7

Response from RFID module:

CMD ID	D0	Data
0xE5	0x02	result code
1 Byte	1 Byte	2 Byte

The meaning of result code (Data [0] is the high 8 bits and Data [1] is low 8 bits) as following:

0000: the operation is completed successfully.

FFFE: module is busy. You can make the module to be free by issuing Stop Inventory command.

FF00:the module is closed.

Others: not defined.

4.3 Set Subnet Mask

Command to RFID module:

CMD ID	P0	P1	P2	P3
0xE6	Mask0	Mask1	Mask2	Mask3
1 Byte	1 Byte	1 Byte	1 Byte	1 Byte

when you want to set subnet mask, you may set this command.

For example, if you want to set subnet mask to 255.255.255.0,

then

Mask0=0xff

Mask1=0xff

Mask2=0xff

Mask3=0x0

Response from RFID module:

CMD ID	D0	Data
0xE6	0x02	result code
1 Byte	1 Byte	2 Byte

The meaning of result code (Data [0] is the high 8 bits and Data [1] is low 8 bits) as following:

0000: the operation is completed successfully.

FFFE: module is busy. You can make the module to be free by issuing Stop Inventory command.

FF00: the module is closed.

Others: not defined.

4.4 Set Gateway

Command to RFID module:

CMD ID	P0	P1	P2	P3
0xE7	Gateway0	Gateway1	Gateway2	Gateway3
1 Byte	1 Byte	1 Byte	1 Byte	1 Byte

when you want to set gateway, you may set this command.

For example, if you want set gateway to 192.168.100.1

then

Gateway0=0xC0(192 decimal)

Gateway1=0xA8(168 decimal)

Gateway2=0x64(100 decimal)

Gateway3=0x1(1 decimal)

Response from RFID module:

CMD ID	D0	Data
0xE7	0x02	result code
1 Byte	1 Byte	2 Byte

The meaning of result code (Data [0] is the high 8 bits and Data [1] is low 8 bits) as following:

0000: the operation is completed successfully.

FFFE: module is busy. You can make the module to be free by issuing Stop Inventory command.

FF00:the module is closed.

Others: not defined.

4.5 Enable or Disable DHCP

Command to RFID module:

CMD ID	P0	P1	P2	P3
0xE8	DHCP_on	0x00	0x00	0x00
1 Byte	1 Byte	1 Byte	1 Byte	1 Byte

when you want to change DHCP setting, you may set this command.

If DHCP_on=1, then DHCP is on, the module use dynamic IP address

if DHCP_on=0, then DHCP is off, the module use static IP address

Response from RFID module:

CMD ID	D0	Data
0xE8	0x02	result code
1 Byte	1 Byte	2 Byte

The meaning of result code (Data [0] is the high 8 bits and Data [1] is low 8 bits) as following:

0000: the operation is completed successfully.

FFFE: module is busy. You can make the module to be free by issuing Stop Inventory command.

FF00:the module is closed.

Others: not defined.

4.6 Get IP Configuration

Command to RFID module:

CMD ID	P0	P1	P2	P3
0xE9	0x00	0x00	0x00	0x00
1 Byte	1 Byte	1 Byte	1 Byte	1 Byte

when you want to Get IP configuration, you may set this command.

Normal Response from RFID module:

CMD ID	D0	Data				
0xE9	0x11	IP address	TCP Port	Mask	Gateway	DHCP
1 Byte	1 Byte	4 Byte	4 Byte	4 Byte	4 Byte	1 Byte

Error Response from RFID module:

CMD ID	D0	Data
0xB3	0x02	result code
1 Byte	1 Byte	2 Byte

The meaning of result code (Data [0] is the high 8 bits and Data [1] is low 8 bits) as following:

0000: the operation is completed successfully.

FFFE: module is busy. You can make the module to be free by issuing Stop Inventory command.

FF00:the module is closed.

Others: not defined.

4.7 save UHF & IP CFG to Flash

Command to RFID module:

CMD ID	P0	P1	P2	P3
0xEF	0x00	0x00	0x00	0x00
1 Byte	1 Byte	1 Byte	1 Byte	1 Byte

when you want to save configuration to flash, you may set this command.

Response from RFID module:

CMD ID	D0	Data
0xEF	0x02	result code

1 Byte	1 Byte	2 Byte
--------	--------	--------

The meaning of result code (Data [0] is the high 8 bits and Data [1] is low 8 bits) as following:

0000: the operation is completed successfully.

FFFE: module is busy. You can make the module to be free by issuing Stop Inventory command.

FF00:the module is closed.

Others: not defined.

Notice: IP configuration will take effect after reset.

5. LED Indicators

5.1 Power Indicator

When the device is power on, all LEDs are off except LED Power Indicator(LED7).

5.2 UHF Ready Indicator

When UHF device is opened successfully, UHF read indicator(LED5) is on.

5.3 Antenna Indicators

Antenna port0-->LED1

Antenna port1-->LED2

Antenna port2-->LED3

Antenna port3-->LED4

If antenna power0==0, then LED1 is off, otherwise LED1 is on;

If antenna power1==0, then LED1 is off, otherwise LED2 is on;

If antenna power2==0, then LED1 is off, otherwise LED3 is on;

If antenna power3==0, then LED1 is off, otherwise LED4 is on;

5.4 Working Mode Indicator

5.5 Inventory& Access Operation Indicator

Inventory & access operation indicator is LED6

If there is any command to UHF device, LED6 is off.

When Inventory is executed, if tags are found, LED6 is blinking.

When Inventory is stopped, LED6 is off.

When Access operation is successful, LED6 is on.