The Manual of Communication Protocol Development

Communication Protocol Developing

Communication protocol means a communication agreement with which an host PC can communicate with a reader/writer via the typical communication interfaces (e.g. RS232, RS485, USB, etc).

1. The definition of commands frames:

Command frames are kind of data which is transferred between a reader/writer and a PC. As shown in the following table:

Packet Type	Station Num	Length	Command Code	Command Data	. . ..	Command Data	Command Data	Checksum
0xA5	0xFF	n+2	1 byte	Byte 1	.	Byte n-1	Byte n	cc

- Packet Type is the type of the packet domain, it is fixed one of “0xA5”.
- Station Num is the domain address, in the specific network (e.g. RS485 network), it is used to identify the unique address of the readers.
  - 0xFF represents any arbitrary address
  - 0x00 represents the broadcast address,
  - 0x01 ~ 0xFE represents any independent station.
- Length means the data length of the packet.
- Command Code is the command itself which is transferred between the host and the reader/writer.
- Command Data are the parameters which are used in a specific command.
- Checksum is for data verification.

2. The definition of response frames:

Response frames are the data format which are returned from reader/writer according to the specific commands which the hosts send. The definition is as shown in the table below:

Packet Type	Station Num	Length	Response Code	Response Data	…	Response Data	Response Data	Checksum
0xE5	0xFF	n+2	1 byte	Byte 1		Byte n-1	Byte n	cc

- Packet Type is the type of the packet domain, it is fixed one of “0xE5”.
- Station Num is the domain address, in the specific network (e.g. RS485 network), it is used to identify the unique address of the readers.
- Length means the data length of the packet.
- Response Code is the domain of the response code.
- Response Data represents the parameters in response frames.
- Checksum is for data verification.

3. ***The definition of the response frames completion from readers to confirm commands have been executed.***

Packet Type	Station Num	Length	Command Code	Status	Checksum
0xE9	0xFF	0x03	1 byte	1 Byte	cc

- Packet Type is the type of the packet domain, it is fixed one of “0xE9”.
- Station Num is the domain address, in the specific network (e.g. RS485 network), it is used to identify the unique address of the readers.
- Length means the data length of the packet. It is fixed of “0x03”.
- Command Code is the domain of the commands.
- Status is the domain of status.
- Checksum is for data verification.

4. Typical Command formats for UHF Gen2 RFID Reader/Writers

4.1 Set Baud Rate

Configure the RS232 Baud Rate of readers

Length	Command Code	Command Data	Checksum
3	0x74	New Baud Rate	cc

The New Baud Rate in the table refers to the Baud Rate users want to adopt, the available options are:

0x00 – 9600bps

0x01 – 19200bps

0x02 – 38400bps

0x03 – 57600bps

0x04 – 15200bps

After receiving the command, readers will return the response frame completion back to the host and the new Baud Rate will be used for the communication.

4.2 Reset Reader

Length	Command Code	Checksum
2	0x75	cc

After receiving the command, readers will return the response frame completion back to the host and the readers will be reset.

4.3 Get the Firmware Version

Length	Command Code	Checksum
2	0x7A	cc

After receiving the command, the format of response from the reader is as below:

Length	Response Code	Response Data	Response Data	Checksum
4	0x7A	Major Firmware	Minor Firmware	cc

Major firmware is the main firmware in the reader.

Minor firmware is the sub firmware in the reader.

4.4 Set Frequency – Hopping / Fixed Mode

Set readers to the frequency-hopping working mode

Length	Command Code	Command Data	Checksum
3	0x7D	Channel	cc

Channel is the hopping frequency which needs to be configured .

“0” means the hopping frequency mode, according to the pre-designed channels and the frequency-hopping sequence, the reader will be acting as the frequency- hopping method in the fixed interval;

1~50 (For the American Standard) means the fixed frequency mode, the reader will be working under the fixed Channel frequency. The definition lists below:

Value	Specified Frequency
1	902.5MHz
2	903.0MHz
3	903.5MHz
4	904.0MHz
5	904.5MHz
6	905.0MHz
7	905.5MHz
8	906.0MHz
9	906.5MHz
10	907.0MHz
11	907.5MHz
12	908.0MHz
13	908.5MHz
14	909.0MHz
15	909.5MHz

16	910.0MHz
17	910.5MHz
18	911.0MHz
19	911.5MHz
20	912.0MHz
21	912.5MHz
22	913.0MHz
23	913.5MHz
24	914.0MHz
25	914.5MHz
26	915.0MHz
27	915.5MHz
28	916.0MHz
29	916.5MHz
30	917.0MHz
31	917.5MHz
32	918.0MHz
33	918.5MHz
34	919.0MHz
35	919.5MHz
36	920.0MHz
37	920.5MHz
38	921.0MHz
39	921.5MHz
40	922.0MHz
41	922.5MHz
42	923.0MHz
43	923.5MHz
44	924.0MHz
45	924.5MHz
46	925.0MHz
47	925.5MHz
48	926.0MHz
49	926.5MHz
50	927.0MHz

1~11 (For the European Standard) means the fixed frequency mode, the reader will be working under the fixed Channel frequency. The definition lists below:

Value	Specified Frequency
1	865.6MHz
2	865.8MHz
3	866.0MHz
4	866.2MHz
5	866.4MHz
6	866.6MHz
7	866.8MHz
8	867.0MHz
9	867.2MHz
10	867.4MHz
11	867.6MHz

By the default, reader is designed as the frequency-hopping working mode.

4.5 Set_Power

Set reader's RF transmission power.

Length	Command Code	Command Data	Checksum
3	0x7F	Power Level	cc

The value of the power level ranges from 2 to 15. See the list below for details

Power Level	Specified Power
2	20dBm
3	21dBm
4	22dBm
5	23dBm
6	24dBm
7	25dBm
8	26dBm
9	27dBm
10	27.5dBm
11	28dBm
12	28.5dBm
13	29dBm
14	29.5dBm
15	30dBm

4.6 Relay Switch

Set relays status on the reader

Length	Response Code	Command Data	Command Data	Checksum
3	0x57	Mask	State	cc

Mask : “D0” is for the first relay

“D1” is for the second relay

State : the status of relays

“1” – close the relay

“0” – open the relay

4.7 Read Tag

Length	Command Code	Command Data	Command Data	Command Data	Checksum
5	0x90	Tag Type	Addr	Length	cc

Tag Type is defined as below:

- 0x01: ISO18000-B tag
- 0x02: EPC Class 0 tag
- 0x03: EPC Class 1 Tag
- 0x04: EPC Class 1 Gen 2 tag

Address is the address of byte in tag’s memory chip. Ranges from 0 to 255.

Length is the number of bytes users need to read from tags.

After receiving the command, reader will read the data content from the specific address in tags. If the content of data is CORRECTLY read, the response frame will be returned, otherwise, only the response frame completion will be returned.

The format of response frame is as below:

Length	Response Code	Response Data	Response Data	Response Data	Response Data	Response Data	Checksum
13+ Length	0x90	Tag Type	Address	Length	ID	Data	cc

The definition of Tag Type is as same as above.

Address is the address of byte in tag’s memory chip.

Length is the number of bytes of the data.

ID is the ID code of tags.

Data is the content inside tag's memory (the length of content is exactly as same as the length value defined in the "Read Tag" operation).

4.7 Read Tags With specific ID Codes

Length	Command Code	Command Data	Command Data	Command Data	Command Data	Checksum
13	0xA0	Tag Type	Address	Length	ID	cc

Tag Type is the type of tag needs to be read. Defined as below:

- 0x01: ISO18000-B
- 0x02: EPC Class 0
- 0x03: EPC Class 1
- 0x04: EPC Class 1 Gen 2

Address is the address of byte in tag's memory chip. Ranges from 0 to 255.

Length is the number of bytes of the data.

ID is the ID code of tags.

The format of response frame is as same as the form below:

Length	Response Code	Response Data	Response Data	Response Data	Response Data	Checksum
13+ Length	0x90	Tag Type	Address	Length	Data	cc

The definition of Tag Type is as same as above.

Address is the address of byte in tag's memory chip.

Length is the number of bytes of the data.

Data is the content inside tag's memory (the length of content is exactly as same as the length value defined in the "Read Tag" operation).

4.8 Write Tags

Length	Command Code	Command Data	Command Data	Command Data	Command Data	Checksum
5+n	0x91	Tag Type	Addr	Length	Data n	cc

Tag Type is the type of tag needs to be read. Defined as below:

- 0x01: ISO18000-B
- 0x02: EPC Class 0
- 0x03: EPC Class 1
- 0x04: EPC Class 1 Gen 2

Addr is the first address of byte needs to be written in.

Length is the number of bytes needs to be written in.

Data is the n-Byte data needs to be written in.

The reader will write the data in the appointed location in the tag and will return the response frame.

The format of response frame is as same as below:

Length	Response Code	Response Data	Response Data	Response Data	Response Data	Response Data	Checksum
13+ Length	0x91	Tag Type	Address	Length	ID	Result n	cc

4.9 Write Tag With ID Code

Length	Command Code	Command Data	Command Data	Command Data	Command Data	Command Data	Checksum
13+n	0xA1	Tag Type	Addr	Length	ID	Data n	cc

Tag Type is the type of tag needs to be read. Defined as below:

- 0x01: ISO18000-B
- 0x02: EPC Class 0
- 0x03: EPC Class 1

- 0x04: EPC Class 1 Gen 2

Addr is the first address of byte needs to be written in.

Length is the number of bytes needs to be written in.

Data is the n-Byte data needs to be written in.

ID is the ID code of tags.

4.10 Single Tag Identification

Length	Command Code	Command Data	Checksum
3	0x92	Tag Type	cc

Tag Type is the type of tag needs to be identified. The definition of Tag Type is as same as above.

After receiving the command, the reader will read the ID of tag. Normally, the response frame will be returned. Otherwise, command-complete frame will be returned.

The format of response frame is the same as the form below:

Length	Response Code	Response Data	Response Data	Checksum
11	0x92	Tag Type	ID	cc

The definition of Tag Type is as same as above.

For the ISO18000-B tag, ID is an 8-Byte ID code; for EPC tag, ID is the an 16-byte EPC code.

4.11 Multiple Tag Identification

Length	Command Code	Comman d Data	Checksum
3	0x93	Tag Type	cc

The format of the returned response frame is as below:

Length	Response Code	Response Data	Checksum
3	0x93	ID count	cc

The ID count is the number of tags that were identified.

4.12 GET ID BUF

Length	Command Code	Command Data	Command Data	Checksum
4	0x61	Operation Type	ID Counts	cc

Operation Type is the type of operation, “01” means reading the data of tag.

Id Counts is the expected number of the tags .

After receiving the command, the reader will return a command-responding frame. The format of the command-responding frame is as follow.

Length	Response Code	Response Data	Response Data	Response Data	Response Data	Checksum
10*n+5	0x61	Operation Type	N IDs	More IDs	ID Data 10 Bytes	cc

Operation Type - 01 means returning the data of tag.

N IDs means the number of the IDs in the response frame.

More IDs means whether tag data is available or not, if the value is “1”, that means ID data is available. “0” means no tag data.

ID Data is the data of tag, it’s ten bytes altogether. The first byte is the type of tag. e.g. “1” means an ISO18000-6B tag, the second byte means the sequence number of antenna, (1~4 respectively). 3~10 bytes contain the UID of the tag.

4.13 Master Acknowledge

Length	Command Code	Checksum
2	0x80	cc

After receiving the command, the reader will delete the ID data that is sent by the reader last time.

No response frame returns for this command.

4.14 Query ID

Length	Command Code	Command Data	Checksum
3	0x95	Mode	cc

Mode is the inquiry mode. The values of Mode are:

- 0x00 means a normal mode.
- 0x01 to 0x04 mean the antenna ports, the reader will return the ID data corresponding the assigned antenna port.

After receiving the command, the reader will return the ID data to the Host according to the port No. which is assigned in the inquiry mode .The format of response frame is as follow:

Packet Type	Length	Response Code	Response Data	Response Data	Checksum
0xF0	4	0xFA	Tag Type	N ID	cc

4.15 Kill EPC Tag

Length	Command Code	Command Data	Command Data	Checksum
4	0x96	Tag Type		cc

After receiving the command, the reader will kill the tag permanently and return the command-completed frame.

****

4.16 Lock Tag

Length	Command Code	Command Data	Command Data	Checksum
4	0x97	Tag Type	Address	cc

The definition of the tag's type is as same as above.

Address is the address of bytes that need to be locked.

After receiving the command and locking the corresponding bytes in the tag,

the reader will return the command-completed frame

4.17 Lock Tag With ID Code

Length	Command Code	Command Data	Command Data	Command Data	Checksum
12	0xA7	Tag Type	ID	Address	cc

The definition of the tag's type is as same as above.

ID is the specified ID code.

Address is the address of the bytes that need to be locked

After receiving the command and locking the corresponding bytes in the tag, the reader will return the command-completed frame.

4.18 Query Lock

Length	Command Code	Command Data	Command Data	Command Data	Checksum
5	0x98	Tag Type	Address	Length	cc

The definition of the tag's type is as same as above.

Address is the address of bytes that need to be locked.

Length is the number of bytes that need to be queried.

After receiving the command and inquiring the specified bytes' Lock Status, the reader will return the response frame after the right operation. Or else, it will return the command complete frame.

The format of the response frame is defined as the following

Length	Response Code	Response Data	Response Data	Response Data	Checksum
11+ Length	0x98	Tag Type	8 ID	Lock Status	cc

4.19 Query Lock With ID Code

Length	Command Code	Command Data	Command Data	Command Data	Command Data	Checksum
13	0xA8	Tag Type	Address	Length	8 ID	cc

The definition of the tag's type is the same as above.

ID is ID code of the tag.

Address is the address of the locked bytes that need to be queried.

Length is the number of bytes that need to be queried.

After receiving the command and inquiring the corresponding bytes' Lock Status, the reader will return the response frame after the right operation. Or else, it will return the command completing frame.

Length	Response Code	Response Data	Response Data	Checksum
3+ Length	0xA8	Tag Type	Lock Status	cc