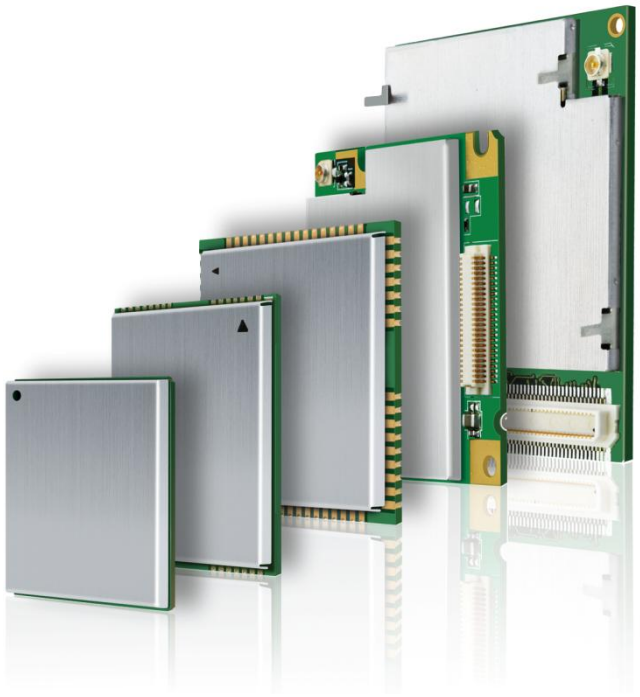
GSM

Quectel Cellular Engine

Firmware Update Protocol Application Notes

Fw_Update_Protocol_AN_V1.2



Document Title	Firmware Update Protocol Application Notes
Version	1.2
Date	2012-01-19
Status	Released
Document Control ID	Fw_Update_Protocol_AN_V1.2

General Notes

Quectel offers this information as a service to its customers, to support application and engineering efforts that use the products designed by Quectel. The information provided is based upon requirements specifically provided for customers of Quectel. Quectel has not undertaken any independent search for additional information, relevant to any information that may be in the customer's possession. Furthermore, system validation of this product designed by Quectel within a larger electronic system remains the responsibility of the customer or the customer's system integrator. All specifications supplied herein are subject to change.

Copyright

This document contains proprietary technical information of Quectel Co., Ltd. Copying this document, distribution to others, and communication of the contents thereof, are forbidden without permission. Offenders are liable to the payment of damages. All rights are reserved in the event of a patent grant or registration of a utility model or design. All specifications supplied herein are subject to change without notice at any time.

Copyright © Quectel Wireless Solutions Co., Ltd. 2012.

Quectel Confidential

Contents

Quectel Confidential

Table Index

Quectel Confidential

Figure Index

Quectel Confidential

0. Revision history

Revision	Date	Author	Description of change
1.0	2011-10-18	Jay XIN	Initial
2.0	2011-11-29	Ivan ZHANG	Added update mode

Quectel Confidential

1. Introduction

The module's Firmware can be downloaded and updated by MCU via UART with Quectel private protocol. This document defines the firmware update protocol between MCU and Quectel module.

Quectel Confidential

2. Hardware architecture

2.1. Update Firmware via MCU directly

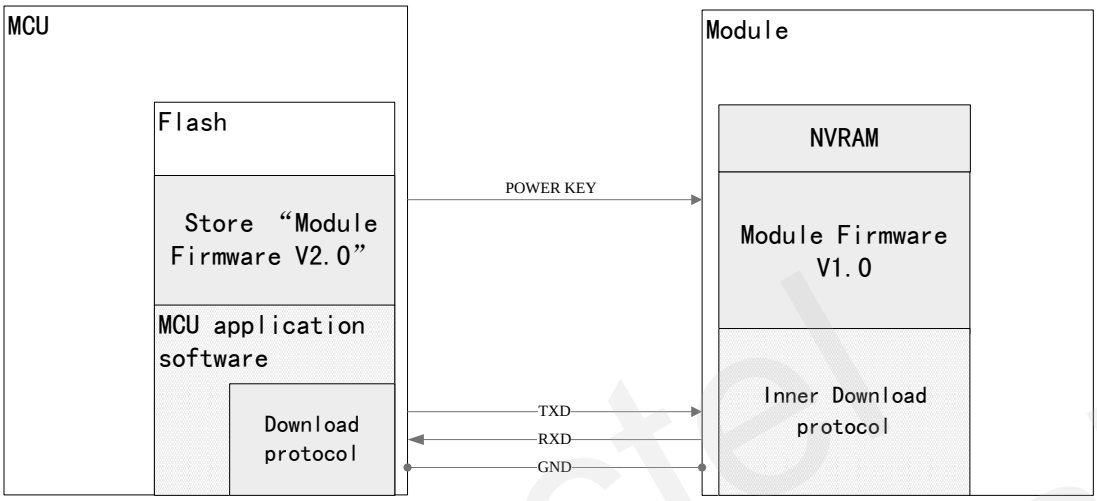


Figure 1: Direct download mode

The new firmware is stored in the flash of MCU. MCU updates the module's firmware based on the download protocol via the module's UART. The module's UART includes Main UART, Debug UART and AUX UART.

The data transmits between MCU and Module via the UART. The hardware parameter is illustrated as bellow:

Baud rate: 115200
Data bit: 8
Stop bit: 1
Parity bite: No
Flow control: No

The update process shall follow these sequences:

1. Power on MCU, open UART and send Sync Word.
2. Power on the module.
3. Module will be in the update procedure once the module receives Sync Word.
4. Once the firmware download has completed, data exchange ends.

Quectel Confidential

2.2. Update Firmware transparently

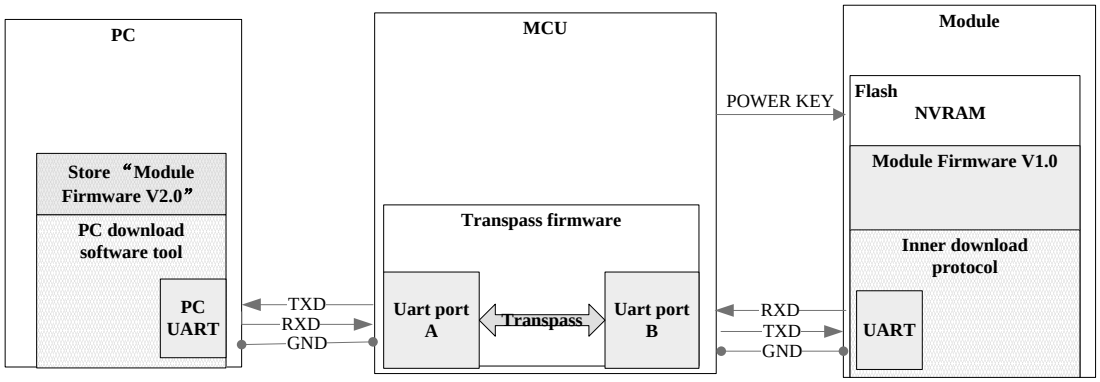


Figure 2: Transparent update mode

In this mode, MCU transmits data transparently, and the protocol download is implemented by PC. MCU receives the data sent by PC via UART Port A then transfers the data to the module via UART Port B. After the module receives the data, it will send the data through MCU. The module's UART includes Main UART, Debug UART and AUX UART.

Data transmission among PC, MCU and module is via UART. The hardware parameter is illustrated as bellow:

Baud rate: 115200
Data bit: 8
Stop bit: 1
Parity bite: No
Flow control: No

The update process shall follow these sequences:

1. After hardware connection, if UART port A and B have been ready for receiving and sending data, MCU can enter into transparent mode prior to PC.
2. Start update tool on the PC and send Sync Word.
3. MCU transfers the data to UART Port B once it receives the Sync Word via UART Port A.
4. Power on the module.
5. Module is in update process after receiving the Sync Word sent by MCU.
6. Once the firmware download has completed, data exchange ends.

Quectel Confidential

2.3. Update Firmware via Debug UART or AXU UART

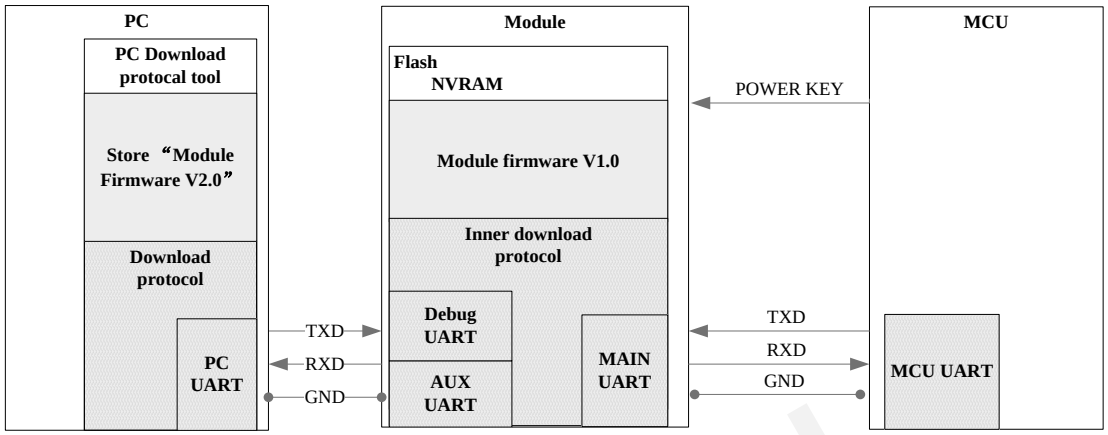


Figure 3: Update firmware via Debug UART or AXU UART

In this mode, PC updates the firmware through Debug UART or AUX UART of the module.

The data transmission between firmware update tool and module is via the DEBUG UART or AUX UART. The hardware parameter is illustrated as bellow:

Baud rate: 115200
Data bit: 8
Stop bit: 1
Parity bite: No
Flow control: No

The update process shall follow these sequences:

1. Connect the Debug UART or AUX UART of the module to UART Port on the PC.
2. Start update tool on the PC and send Sync Word.
3. Power on the module.
4. Module is in update process after receiving the Sync Word sent by MCU.
5. Data exchange ends once the firmware download has completed.

2.4. Firmware updating failure handling

Possible causes for firmware update failure can be:

- Downloading firmware fails during updating process.
- Power supply interrupts

In these cases, the firmware update process is interrupted and the module's firmware is invalid.

Quectel Confidential

Meanwhile, the module cannot work. Users must restart to update the module's firmware then the module's firmware is fully operational.

Quectel Confidential

3. Procedure for downloading firmware

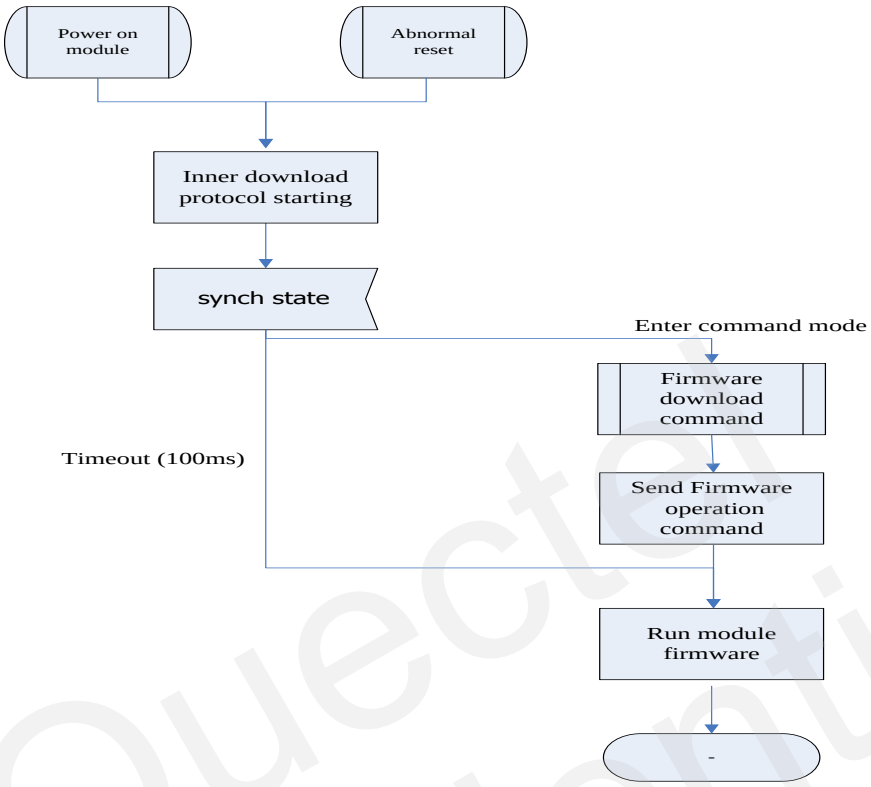


Figure 4: Produce for downloading firmware

Send "synchronous sequence" if updating firmware is necessary, which can synchronize the module and MCU. After that, the module will enter into the "Command Mode". MCU can download firmware via the download command.

On the other hand, need not to seed the "synchronous sequence". When it is timeout, the module will operate the firmware that has been stored in the module.

3.1. Boot synchronous sequence

If MCU needs to update the firmware, please follow these steps listed as below:

1. Power off the module.

2. Send SYNC_WORD1 to the module via UART at interval of 20ms, and then power on the module, which aims to synchronize the MCU and the module. When the module returns SYNC_WORD_RSP1, MCU sends SYNC_WORD2 and the module responds with SYNC_WORD_RSP2. The cycle must be finished within 300ms. The baud rate of the

interface should be set as 115200. After that, the module will enter into "Command Mode". In this mode, the MCU can send the command to download the firmware. If the module cannot receive the "synchronous sequence" or finish synchronous negotiation within 100ms, the module will run the firmware that has been stored in the module.

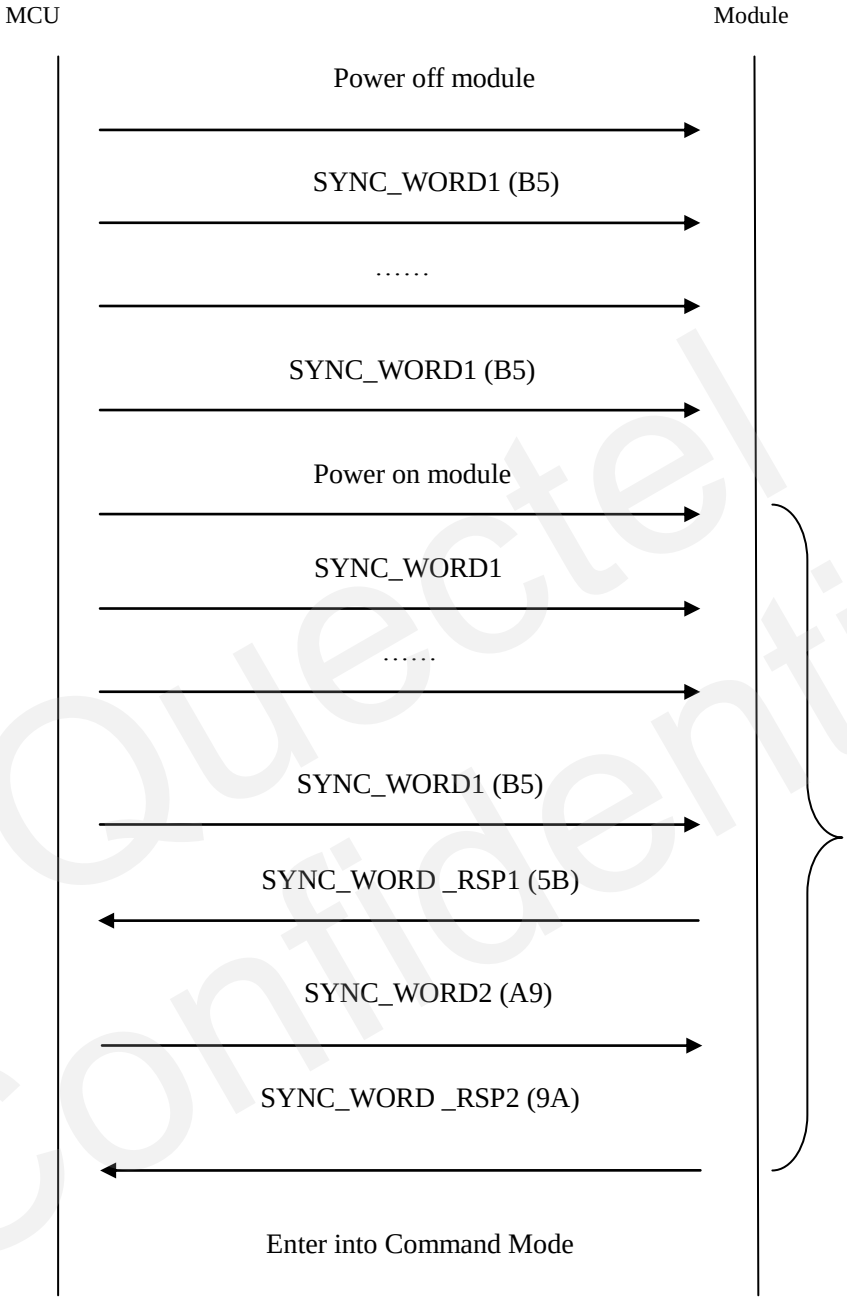


Figure 5: Boot synchronous sequence

Note: In the "Command mode", if MCU did not send any commands, the module will be in the "Command mode" all the time.

3.2. Firmware download procedure

After the module enters into the "Command mode", MCU can send download command to the module. The detailed procedure is shown as below:

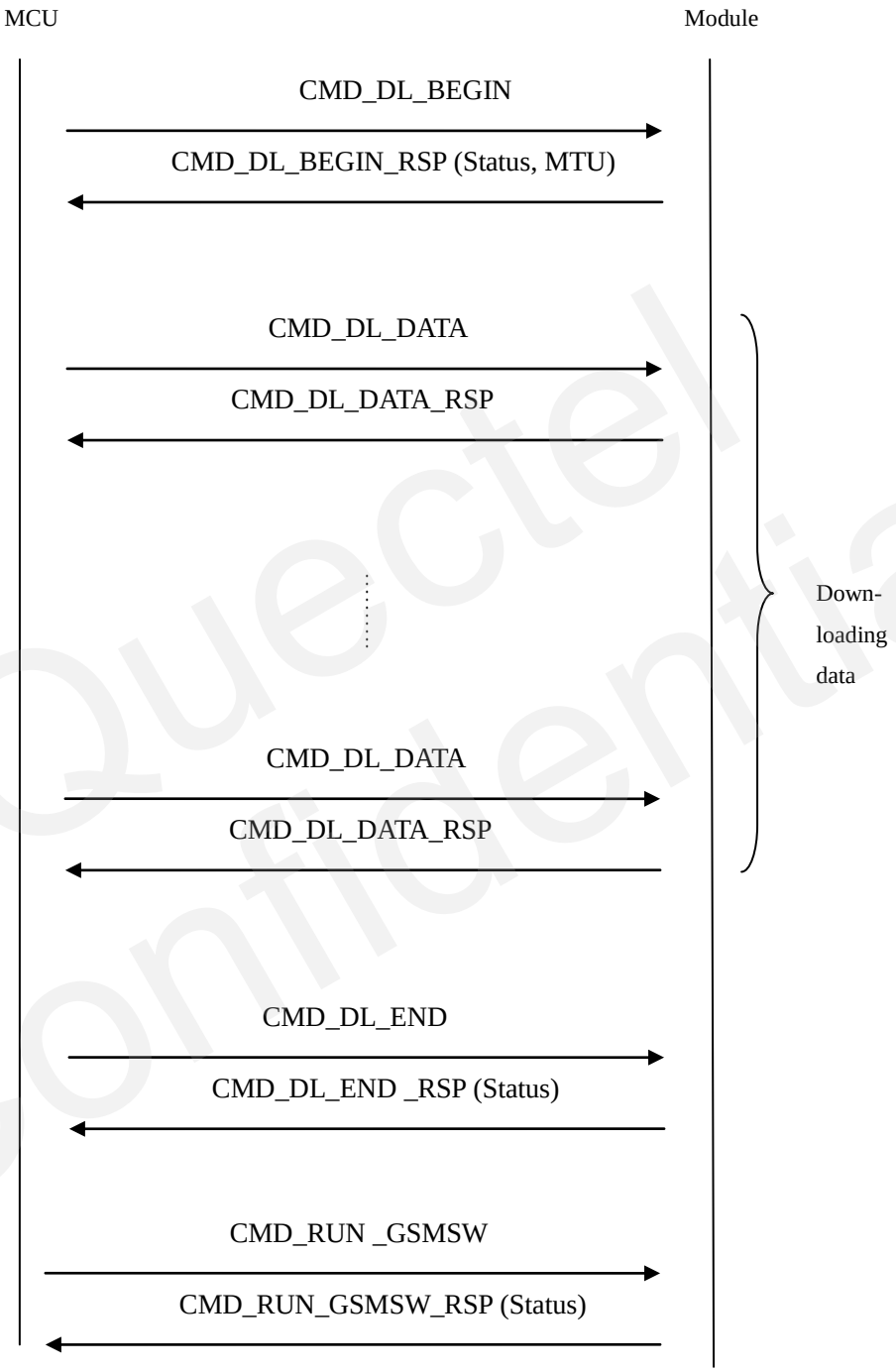


Figure 6: Download procedure

First, MCU sends CMD_DL_BEGIN to the module and then module returns the CMD_DL_BEGIN_RSP. After that, MCU packs the firmware data (including sequence number and data block) into the command CMD_DL_DATA then sends the data package to the module.

Quectel Confidential

Please take the following points into account.

1. The value of "Data Length" field in the command CMD_DL_DATA includes the sequence number and data block length. E.g. if the data block length in the data package is 1024, the value of "Data length" field is 1028.

2. The total length of command package sent by MCU cannot exceed the MTU value responded by the module.

3. The value of the sequence number starts from 0.

4. When the module received the data package and verified the data has been written successfully, it will return CMD_DL_DATA_RSP (Status=0). Then MCU can send the next data packet.

5. If the module returns CMD_DL_DATA_RSP (Status=1 or Status=4), MCU will retransmit the specified data packet.

6. If the module returns CMD_DL_DATA_RSP (Status=2), it means the Flash is error. The MCU will restart the module and download the firmware again.

7. MCU will read and send the data block of the application software in turn. The length of the other data block must be aligned in even-type, except the last data block.

After MCU downloaded the whole application software data block, it will send CMD_DL_END to the module, which means the firmware download is finished. The module will return CMD_DL_END_RSP and exit from download mode.

When MCU finished the download procedure above, it can inform the module of starting the application software by sending CMD_RUN_GSMSW to the module. The module will return CMD_RUN_GSMSW_RSP.

Note:

When MCU sent command package to the module, if the module didn't receive the response package within 3 seconds, the Module will send the command again. If MCU sent the command for more than three times, the MCU will restart the module and download the procedure again.

Quectel Confidential

4. Definition of the Command package

4.1. Format of command package

Table 1: The format of command package:

Head	Type	Length	Data	CRC16
1 byte (0xAA)	2 byte	2 byte	N byte	2 byte

The value of "length" means the length of the data field, which does not include the length of CRC16's two bytes. The checksum range consists of "Type" field, "Data Length" field and "Data" field.

Note:
CRC16 Polynomial: CRC-16-CCITT x16 + x12 + x5 + 1.

4.2. Command list

Table 2: Command list

Type	Cmdid	Description	Direction
CMD_DL_BEGIN	0x0001	Begin to download	MCU to Module
CMD_DL_BEGIN_RSP	0x0002	Response to beginning downloading	Module to MCU
CMD_DL_DATA	0x0003	Download data	MCU to Module
CMD_DL_DATA_RSP	0x0004	Response to data downloading	Module to MCU
CMD_DL_END	0x0005	End Downloading	MCU to Module
CMD_DL_END _RSP	0x0006	Response to data downloading end	Module to MCU
CMD_RUN _GSMSW	0x0007	Require to run application software	MCU to Module
CMD_RUN_GSMSW_RSP	0x0008	Response to running application software	Module to MCU

4.3. Description of Command field

4.3.1. CMD_DL_BEGIN

The length of the data field is defined by the data length field. The content of the data field is

Quectel Confidential

defined as below:

Content	Bytes	Description
Application software version data	4	Reserve

Example:
Application software version is 1, and the data package of the command CMD_DL_BEGIN is shown as below:
0xAA 0x0001 0x0004 0x00 0x00 0x00 0x01 0x?? 0x??

Note: Different color in data package means different data field.

4.3.2. CMD_DL_BEGIN_RSP

The length of the data field is defined by the data length field. The content of the data field is defined as below:

Content	Bytes	Description
Status	2	Refer to the definition list
MTU	2	The maximum length of command package which module can received

Note:

1. ***Status means whether the module receives the download request.***
2. ***MTU means the maximum length of command package the module received at a time (the length value consists of Head field, Command Type field , Data field and CRC Parity field).***

Example：
The following is the data package of CMD_DL_BEGIN_RS. Its status is 0 and MTU is 1024.
0xAA 0x0002 0x0004 0x00 0x00 0x04 0x00 0x?? 0x??

4.3.3. CMD_DL_DATA

The length of the data field is defined by the data length field. The content of the data field is defined as below:

Content	Bytes	Description
Sequence number	4	The sequence number of Module's data package and begins from 0.
Module data	N-4 bytes	Module data; N is the data length of the command packet.

Quectel Confidential

Example:
The following is the data package of the command CMD_DL_DATA which means Sequence number is 4 and the length of module data is N-4 bytes.

Header	CMD	Len=N	Sequence number 4 BYTE	Module data N-4 byte
0xAA	0x0003	0x????	0x00 0x00 0x94 0x00	0x?? 0x?? 0x?? 0x?? 0x??... 0x?? 0x??

Note: Sequence number: ***0x00 0x00 0x94 0x00***
Module Data: 0x?? 0x?? 0x?.....
Module data Length = (Len)N - (Sequence number Length) 4

4.3.4. CMD_DL_DATA_RSP

The length of the data field is defined by the data length field. The content of the data field is defined as below:

Content	Bytes	Description
Status	2	Refer to definition list
Next sequence number	4	

Example:
The data package of CMD_DL_DATA_RSP is shown as below. Its status is 0 and the next sequence number is 245.

0xAA	0x0004	0x0006	0x00	0x00	0x00	0x00	0x00	0xF5	0x?? 0x??

4.3.5. CMD_DL_END

The command does not have data field. The length of data field is 0.

Example:
The data package of the command CMD_DL_END is shown as below:

0xAA	0x0005	0x0000	0x?? 0x??

4.3.6. CMD_DL_END_RSP

The length of the data field is defined by the data length field. The content of the data field is defined as below:

Content	Bytes	Description
Status	2	Refer to the definition list

Quectel Confidential

Example：
The following is the data package of CMD_DL_END_RSP whose status is 0.
0xAA 0x0006 0x0002 0x00 0x00 0x?? 0x??

4.3.7. CMD_RUN_GSMSW

The command does not have data field. The length of data field is 0.

Example:
The data package of CMD_RUN_GSMSW is shown as below:
0xAA 0x0007 0x0000 0x?? 0x??

4.3.8. CMD_RUN_GSMSW_RSP

Content	Bytes	Description
Status	2	Refer to the definition list

Example:
The data package of CMD_RUN_GSMSW_RSP whose status is 3 is shown as below:
0xAA 0x0008 0x0002 0x00 0x03 0x?? 0x??

4.4. Definition list

The following table describes the status values of the commands mentioned above.

Status value	Description	Response
0	Success	
1	CRC16 error	MCU retransmits the response sequence number.
2	Flash error	MCU restarts module, and downloads the application software again.
3	Module is in download mode.	
4	Data package error	MCU retransmits the response sequence number.

Quectel Confidential

Shanghai Queel Wireless Solutions Co., Ltd.

Room 501, Building 13, Tianzhou Road, Shanghai, China 200233

Tel: +86 21 5108 6236

Mail: info@quectel.com