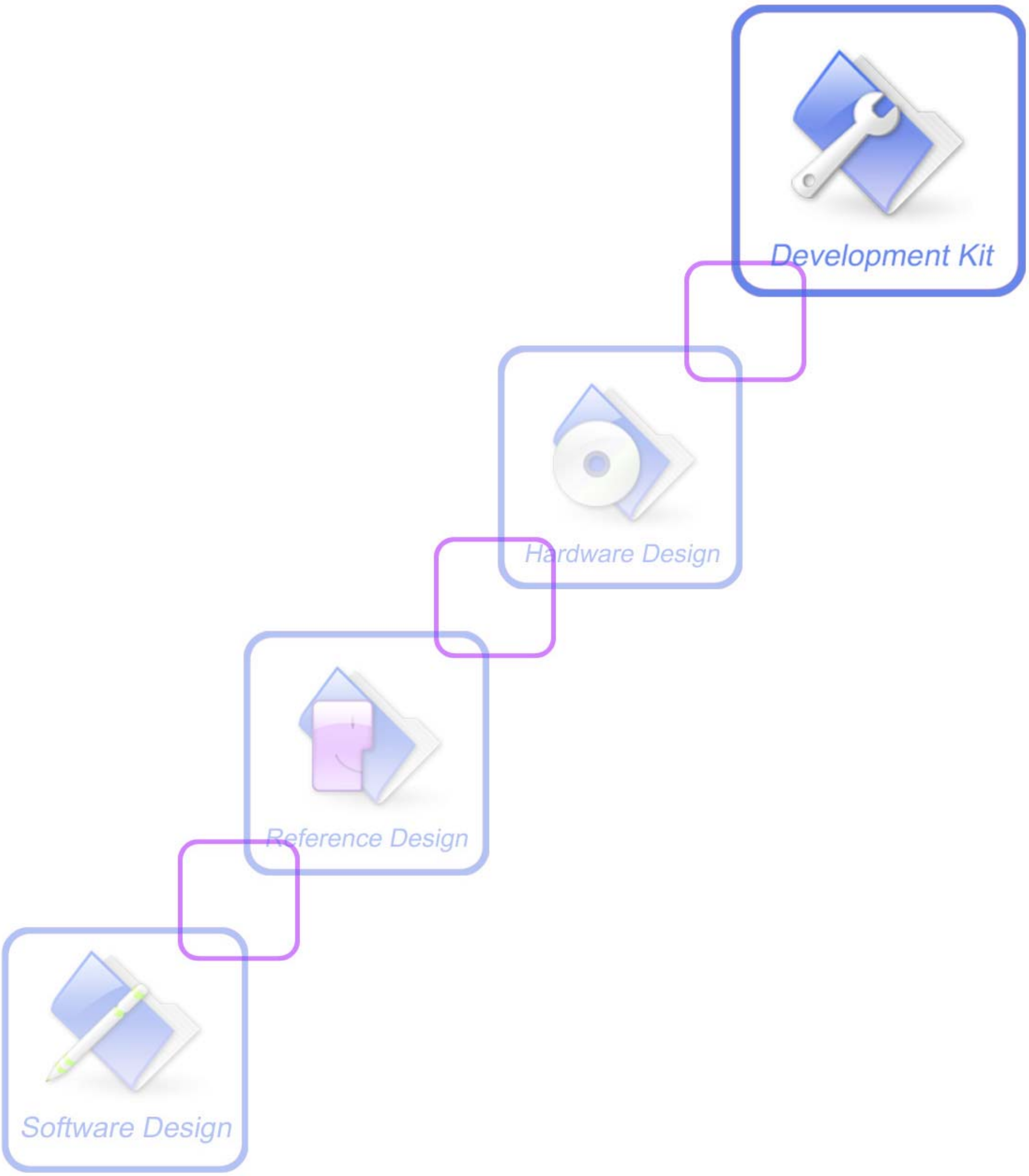
A company of SIM Tech

SIM900 Series Module Downloading Procedure _V1.30



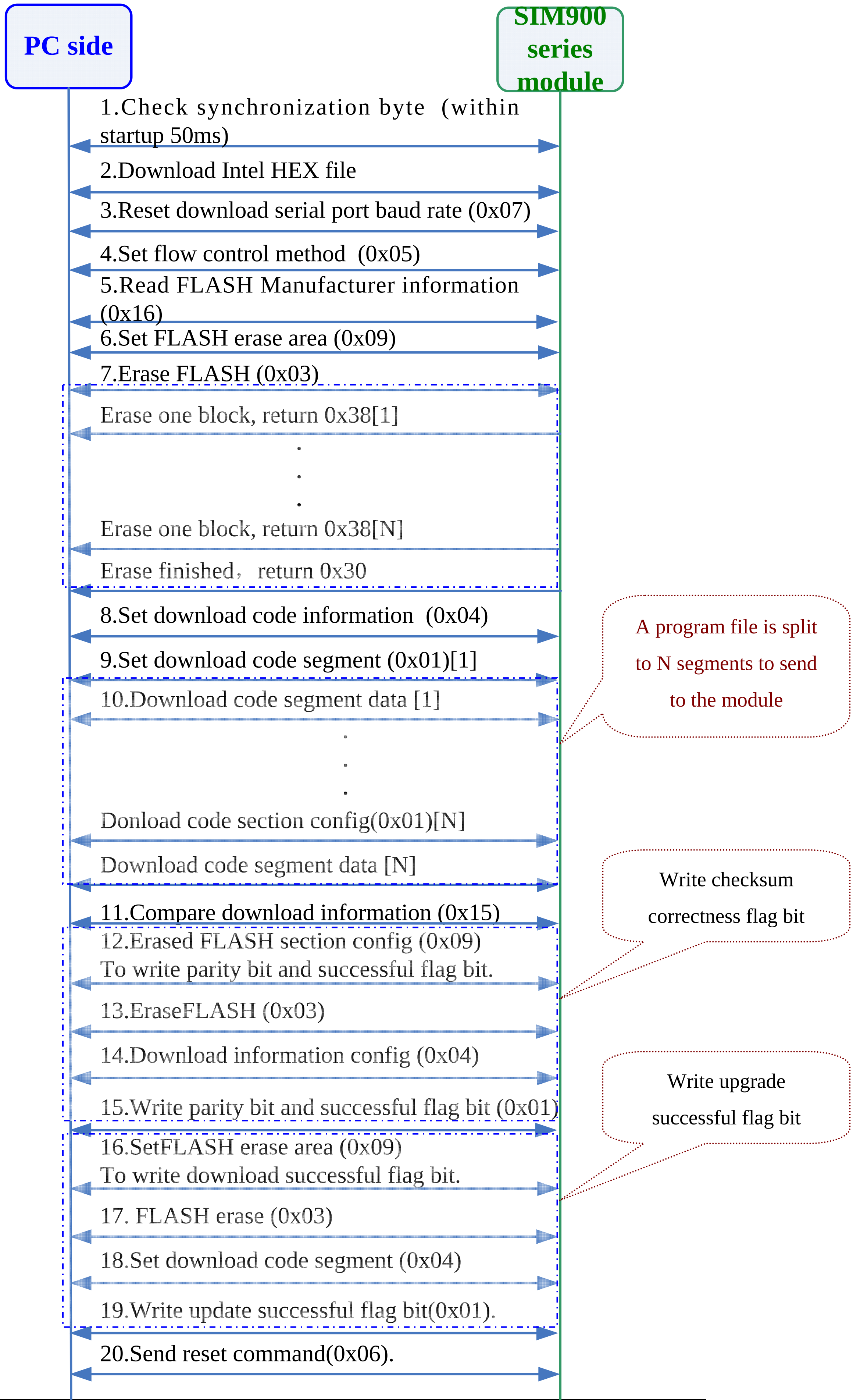
1 Summary

This document describes the procedure of downloading code to SIM900 series modules from PC side via serial port.

2 Procedure

Every time when SIM900 series module is powered on, the system will start from BOOT ROM.

The summary figure of program downloading procedure is as following:



PC side

SIM900 series module

1.Check synchronization byte (within startup 50ms)

2.Download Intel HEX file

3.Reset download serial port baud rate (0x07)

4.Set flow control method (0x05)

5.Read FLASH Manufacturer information (0x16)

6.Set FLASH erase area (0x09)

7.Erase FLASH (0x03)

Erase one block, return 0x38[1]

.
.
.

Erase one block, return 0x38[N]

Erase finished， return 0x30

8.Set download code information (0x04)

9.Set download code segment (0x01)[1]

10.Download code segment data [1]

.
.
.

Donload code section config(0x01)[N]

Download code segment data [N]

11.Compare download information (0x15)

12.Erased FLASH section config (0x09)
To write parity bit and successful flag bit.

13.EraseFLASH (0x03)

14.Download information config (0x04)

15.Write parity bit and successful flag bit (0x01)

16.SetFLASH erase area (0x09)
To write download successful flag bit.

17. FLASH erase (0x03)

18.Set download code segment (0x04)

19.Write update successful flag bit(0x01).

20.Send reset command(0x06).

A program file is split to N segments to send to the module

Write checksum correctness flag bit

Write upgrade successful flag bit

Figure 2-1 Summary Figure of program downloading procedure

2.1 Power on Startup

The power on startup procedure is as following:

1) Start module PC side serial port download program, confirm module power supply and download port (MAIN port or DEBUG port) are connected well.

2) Start PC side download.

3) Reset module, system starts from BOOT ROM.

Note：

1. Here the setting of the module and the PC side download serial port are both as following: 115200bps, 8 bit, No parity bit, 1 stop bit, no flow control.

2.2 Check Synchronization Byte (0x16)

When the code in BOOT ROM starts to run:

If the module receives synchronization byte (0x16) sent from PC side within 50 ms, then it goes into file download process, and returns this synchronization byte to PC side immediately to confirm the set up of download connection. Once PC side receives this byte, it should stop the periodical sending of synchronization byte.

If the module does not detect the synchronization byte (0x16)sent from PC side within 50 ms, then BOOT ROM code will be terminated, the program pointer jumps to Flash start address (0x90000000), it will go to the normal module startup procedure.

So to insure synchronization, PC side should send synchronization byte within 50 ms time interval, such as 30 ms.

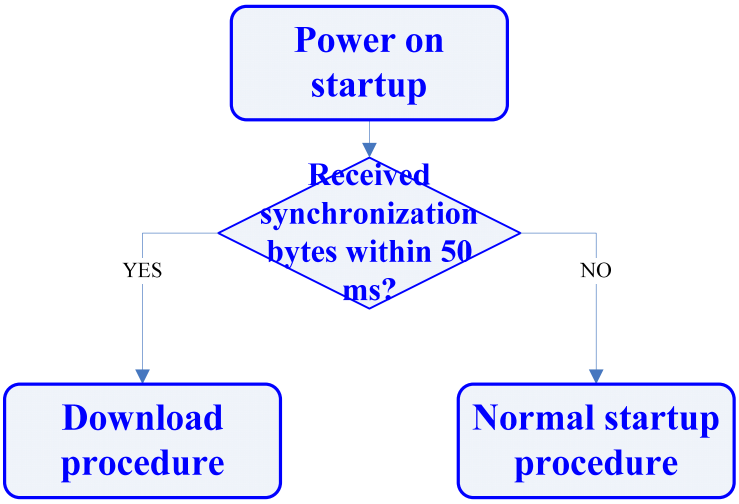


Figure 2-2 Module is powered on and is waiting for synchronization byte

Refer to Figure 2-3 for command flow process:

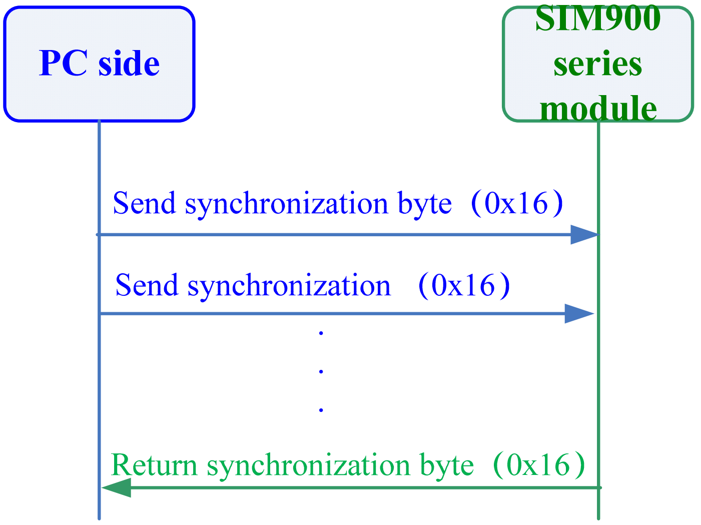

PC side
SIM900 series module
Send synchronization byte（0x16）
Send synchronization （0x16）
.
.
.
Return synchronization byte（0x16）

Figure 2-3 Process of synchronization byte check

2.3 Download Intel HEX File (Void)

PC side send the array in the file “flash_nor_16bit_hwasic_evp_4902_rel.h” to the module in sections (For instance, the segment size is 512 bytes), and then the module download this part of code to on-chip RAM address of ARM. A typical download consuming time is about 3 seconds. Refer to the following figure for command process:

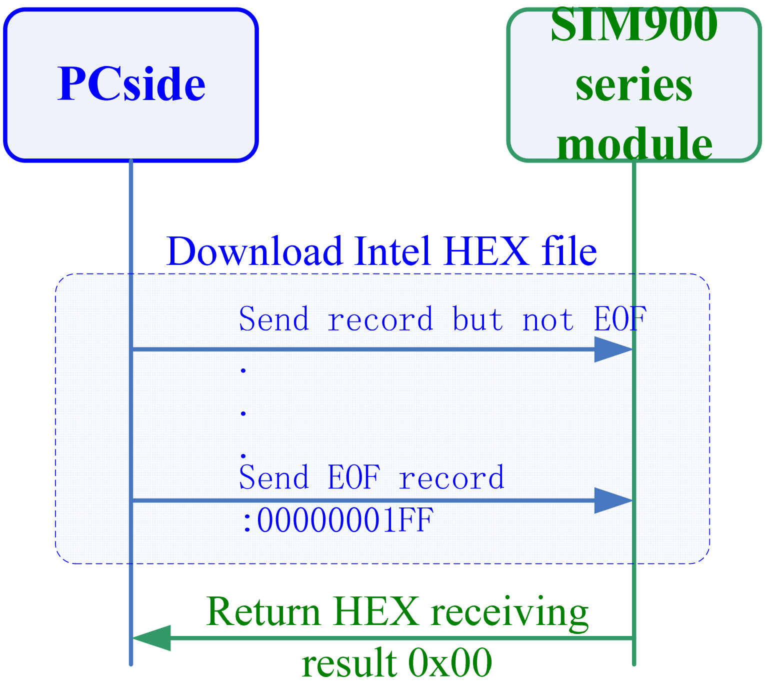


Figure 2-4 Process of downloading Intel Hex file

Download will be considered successful if PC side receives the return value listed in the following table from the module.

Table 2-1 Module Response

Hex file download result	Module response value(Hex)
Success	0x30,0x00
	0x00

2.4 Reset download serial port baud rate (0x07)

If command process "Download HEX file" is successful, then PC side could reset module download serial port baud rate:

PC side will send command "Reset download serial port baud rate" to the module with old baud rate (115200bps), if the module decides this baud rate is effective, it will send change successful response to PC side immediately with old baud rate.

After that, module download port will be actively changed to this new baud rate, the possible baud rate settings are: 9600,19200, 38400, 57600,115200,230400,460800， 921600.

(The setting of serial port will not be changed, it is: 8 bit, No parity bit, 1 stop bit, no flow control.)

Refer to the following figure for command process:

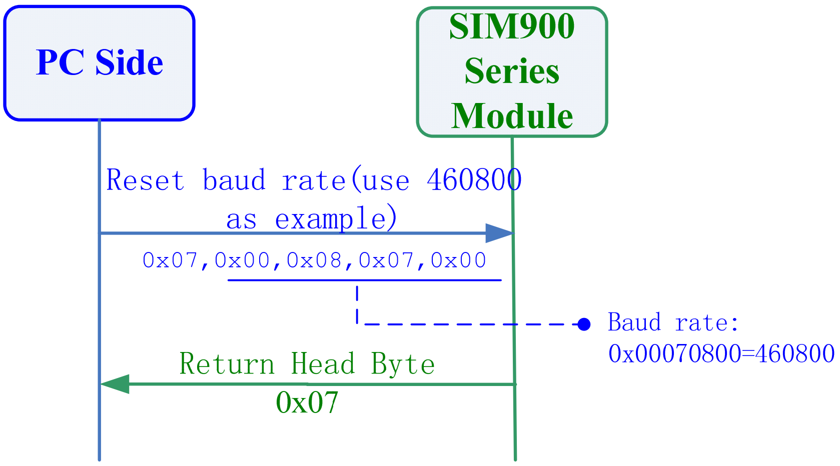


Figure 2-5 Reset Download Port Baud rate

2.5 Set Flow Control Method (0x05)

When the command process "Reset download serial port baud rate" is finished, PC side will send command "Set flow control method" to set flow control method, here it is set to 0, which means no flow control. Refer to the following figure for command process:

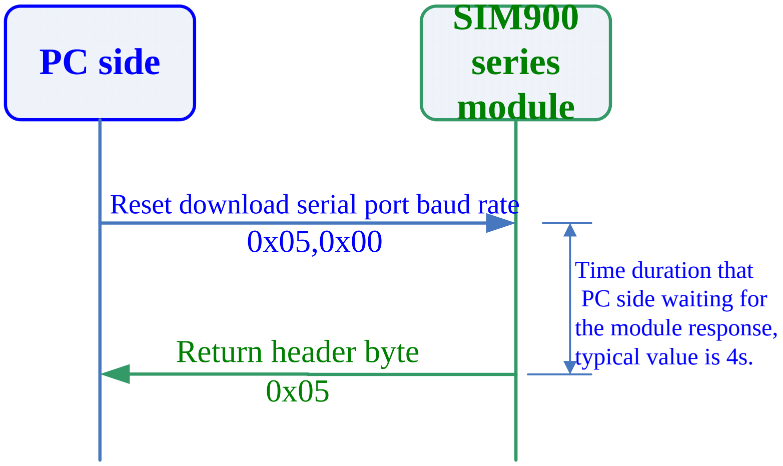

PC side
SIM900 series module
Reset download serial port baud rate
0x05,0x00
Return header byte
0x05
Time duration that PC side waiting for the module response, typical value is 4s.

Figure 2-6 Set flow control method

2.6 Read FLASH Manufacturer Information (0x16)

When the command process "Set flow control method" is successful，PC side may send command "Read FLASH manufacturer information" to read FLASH information, and set FLASH parameters. Refer to the following figure for command process:

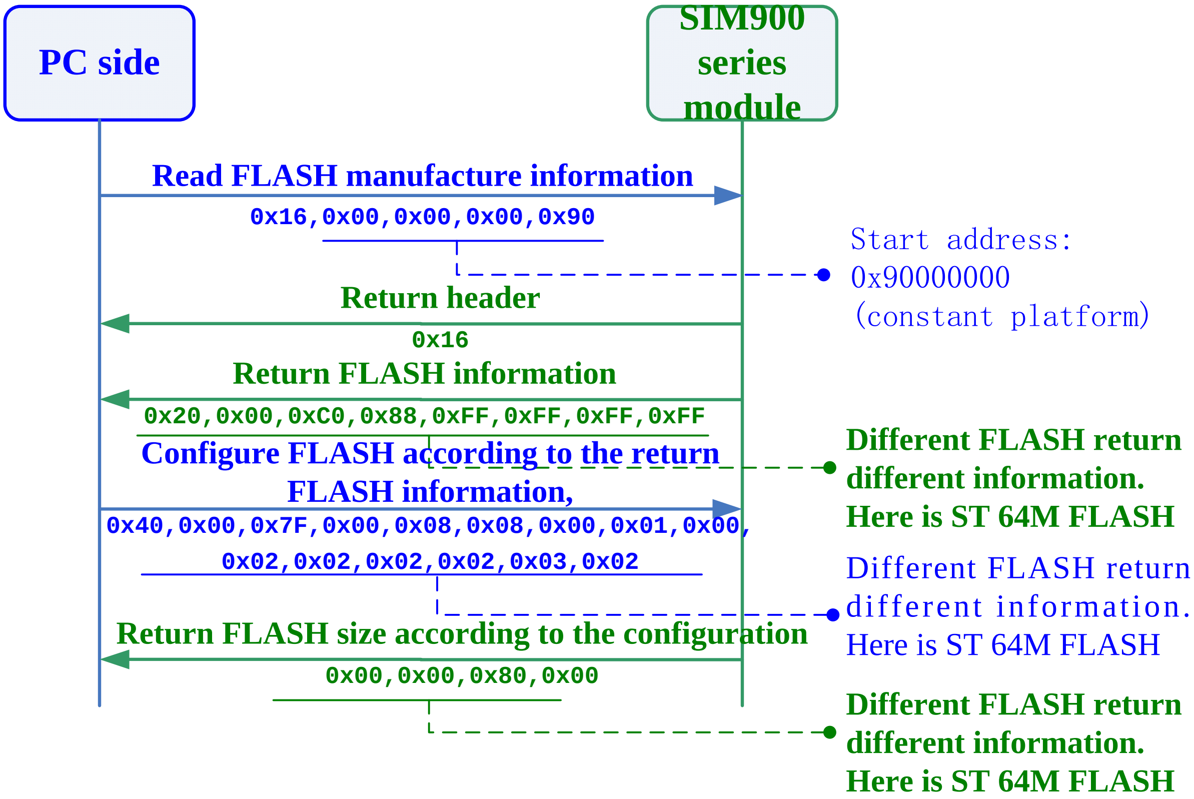

PC side
SIM900 series module
Read FLASH manufacture information
0x16,0x00,0x00,0x00,0x90
Start address: 0x90000000 (constant platform)
Return header
0x16
Return FLASH information
0x20,0x00,0xC0,0x88,0xFF,0xFF,0xFF,0xFF
Different FLASH return different information. Here is ST 64M FLASH
Configure FLASH according to the return FLASH information,
0x40,0x00,0x7F,0x00,0x08,0x08,0x00,0x01,0x00,
0x02,0x02,0x02,0x02,0x03,0x02
Different FLASH return different information. Here is ST 64M FLASH
Return FLASH size according to the configuration
0x00,0x00,0x80,0x00
Different FLASH return different information. Here is ST 64M FLASH

Figure 2-7 Read FLASH Manufacturer Information

2.7 Set FLASH Erase Area (0x09)

When the command process "Read FLASH manufacturer information" is finished;

User needs to execute command process “SET FLASH ERASE AREA” and “FLASH ERASE” sequentially to finish FLASH area erase.

PC side uses command “SET FLASH ERASE AREA” to set target start address of FLASH ERASE area (32bit,LE) and erase size (32bit,LE).

When module receives this command, it will return 0x09 immediately to confirm setting successful.

Refer to the following figure for command process:

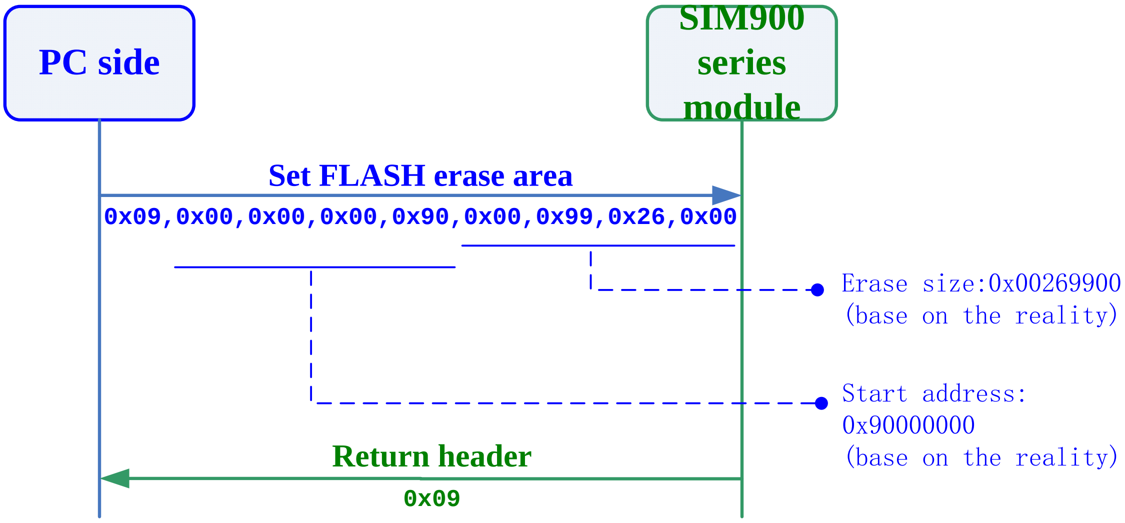


Figure 2-8 SET FLASH ERASE AREA

2.8 FLASH Erase (0x03)

When PC side sends command “FLASH ERASE”, module will return 0x03 immediately;

After that, module will perform actual erase work to the FLASH area; Every time a FLASH block is erased, module will send an '8' to PC side, until all blocks are erased completely.

When erase is finished, module sends character '0' to PC side to show erase successful.

It can go to the next procedure.

Note:

1. The time consuming to erase FLASH is different according to different area size. For example: To erase an area of 2.4M may cost about 30 seconds.

Refer to the following figure for command process:

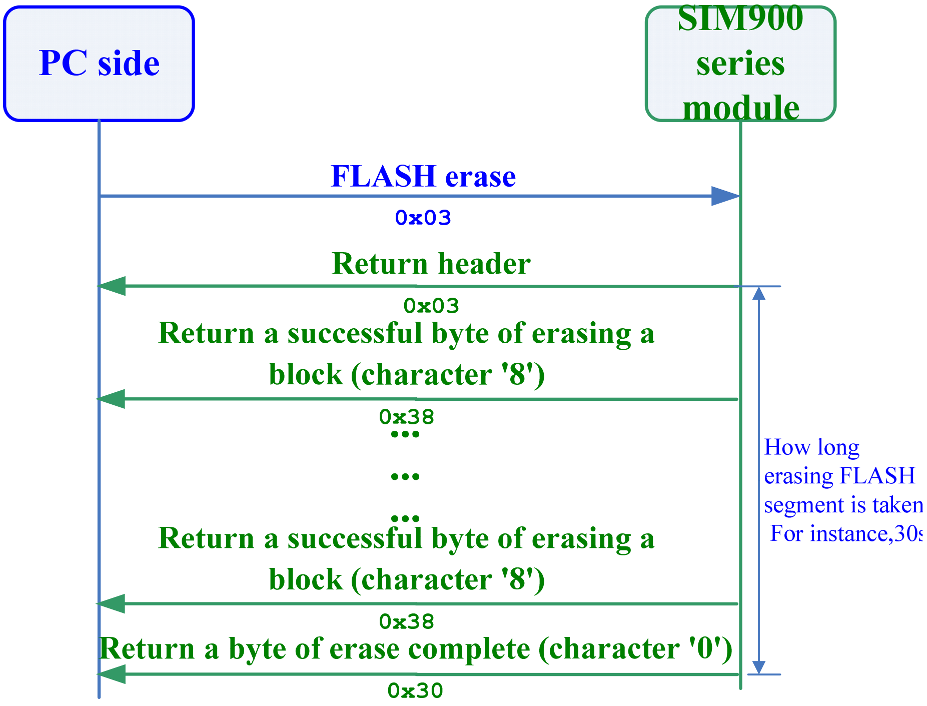

PC side
SIM900 series module
FLASH erase
0x03
Return header
0x03
Return a successful byte of erasing a block (character '8')
0x38
…
…
…
Return a successful byte of erasing a block (character '8')
0x38
Return a byte of erase complete (character '0')
0x30
How long erasing FLASH segment is taken
For instance,30s

Figure 2-9 FLASH Erase

2.9 Set Download Code Information (0x04)

When command process "FLASH ERASE" is finished;

PC side uses command "Set Download Code Information" to set start address of target file (32bit,LE) and code size (32bit,LE).

After PC side sends this command, the module will return 0x04 immediately to confirm setting successful.

Refer to the following figure for command process:

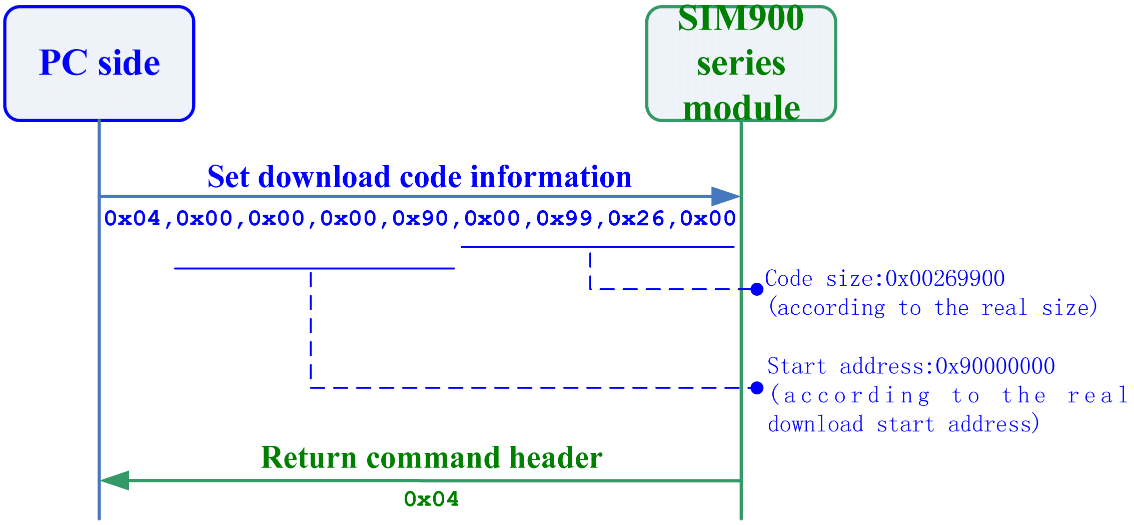

PC side
SIM900 series module
Set download code information
0x04,0x00,0x00,0x00,0x90,0x00,0x99,0x26,0x00
Code size:0x00269900
(according to the real size)
Start address:0x90000000
(according to the real download start address)
Return command header
0x04

Figure 2-10 Set Download Code Information

2.10 Set Download Code Segment (0x01)

When PC side finishes command process “Set Download Code Information”, the length information of the command “Download Code Segment Data” can be set，the maximal value of this length is 2048 (0x800). The length should be even number, it cannot be odd number. Refer to Figure 2-12.

2.11 Download Code Segment Data (Void)

Every time when the command process “Set Download Code Segment” is finished, it should “Download Code Segment Data”.

Now PC side only needs to send data of the designated length which is set by command “Set Download Code Segment”.

When module receives designated length and return (0x2E,0x30)，it means receiving code segment data successful.

Refer to Figure 2-12 for command process.

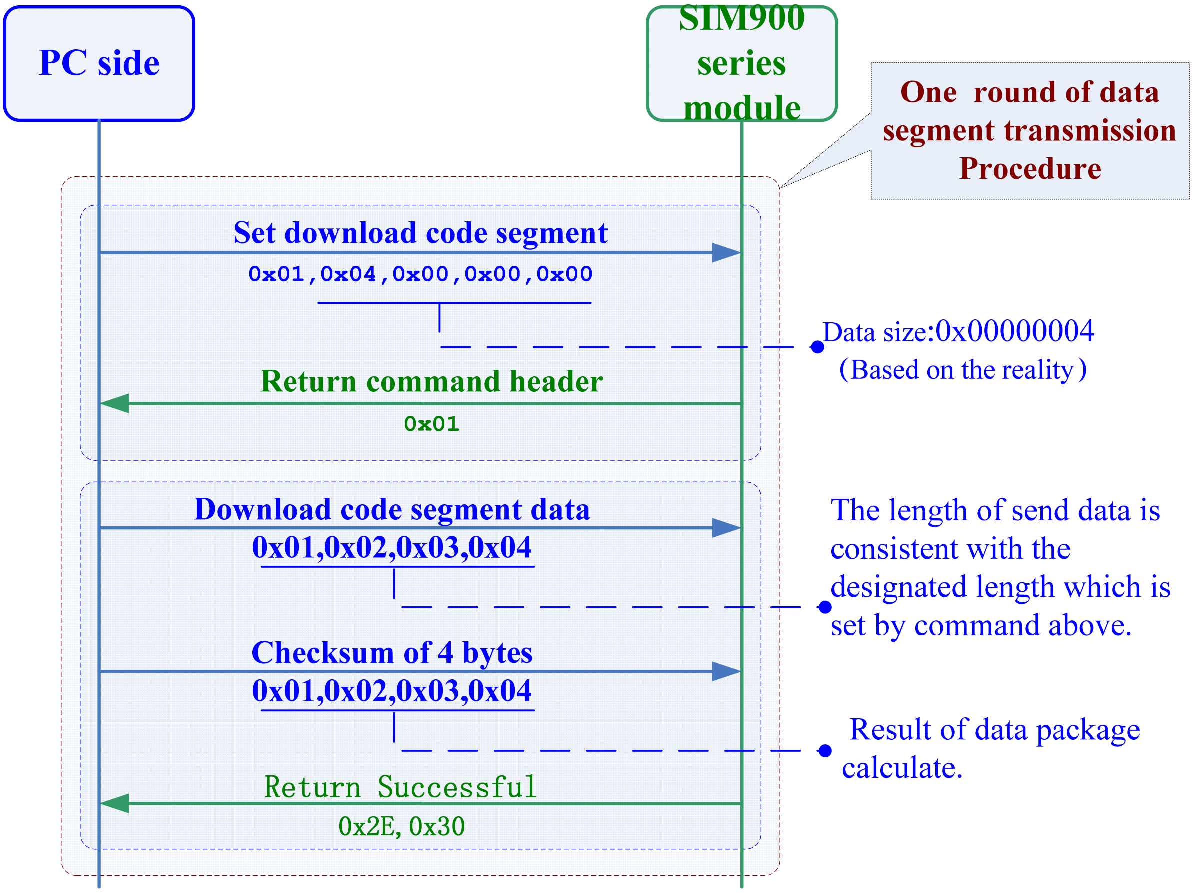

PC side
SIM900 series module
One round of data segment transmission Procedure
Set download code segment
0x01,0x04,0x00,0x00,0x00
Data size:0x00000004
(Based on the reality)
Return command header
0x01
Download code segment data
0x01,0x02,0x03,0x04
The length of send data is consistent with the designated length which is set by command above.
Checksum of 4 bytes
0x01,0x02,0x03,0x04
Result of data package calculate.
Return Successful
0x2E, 0x30

Figure 2-11 Download code segment

Note:
1. For one round of download procedure, the sum of all data length designated in "Download Code Segment Data" command should equal to the actual download data size. Downloaded data will be saved in FLASH area sequentially during "Download Code Segment Data" process.

2.12 Compare Download Information (0x15)

After downloaded file data, PC side send “compare download information” instruction, and send download start address(32bit,LE), checksum(32bit,LE), file size (32bit,LE) to the module.
When module received this instruction, it will return the newly generated checksum (32bit,LE) by the file it received to PC side. If two results are identical (0x30), that means successfully download, otherwise, download failed.
Refer to the following figure for command process:

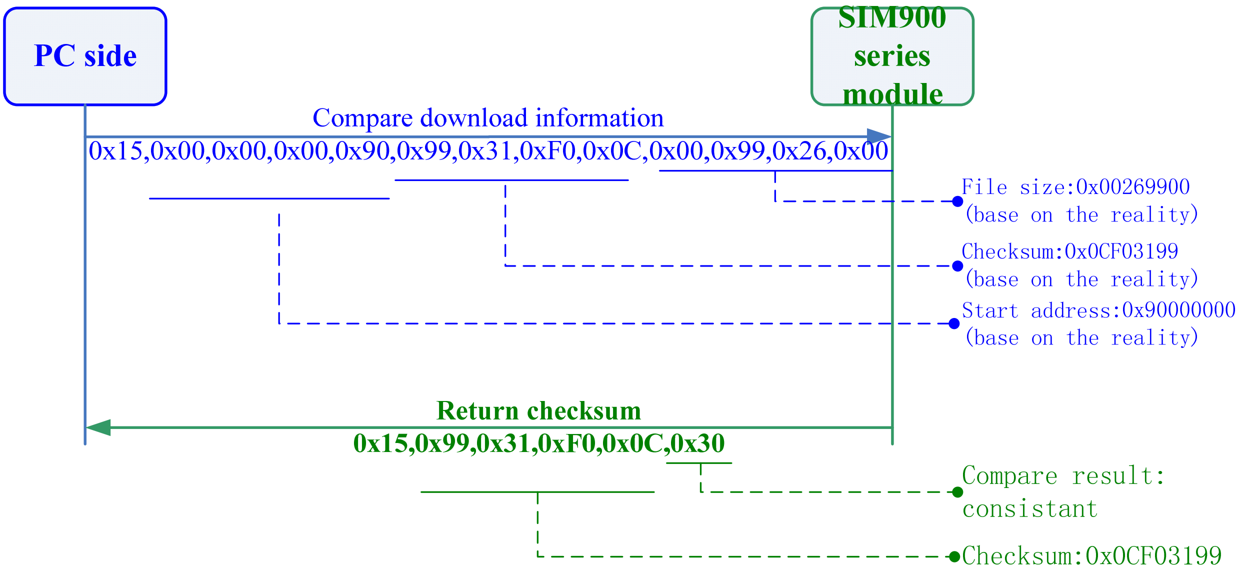


Figure 2-12 Check Download Information

2.13 Write checksum correctness flag bit

2.13.1 Set FLASH Erase Area (0x09)

After PC side send “Compare download information” command, executing “SET FLASH ERASE AREA” and “FLASH ERASE” commands in turn to accomplish erasing checksum correctness flag bit in FLASH area. PC side uses command “SET FLASH ERASE AREA” to set target start address of FLASH ERASE area (32bit,LE) and erase size (32bit,LE).
When module receives this command, it will return 0x09 immediately to confirm setting successful.
Refer to the following figure for command process:

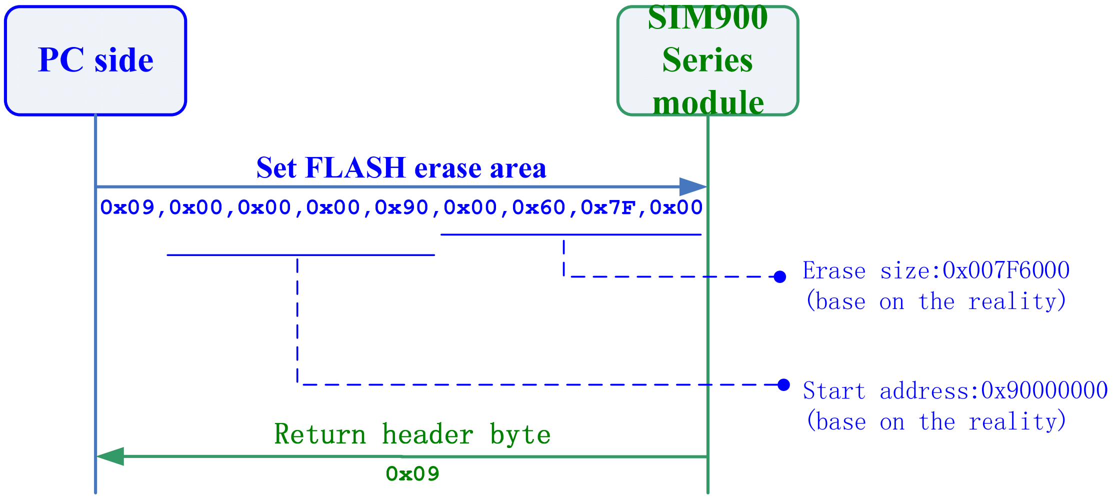


Figure 2-14 Set Flash Erase Area

2.13.2 FLASH Erase (0x03)

When PC side sends command “FLASH ERASE”, module return 0x03 immediately;
After that, module will perform actual erase work to the FLASH area;Every time a FLASH block is erased, module will send an ‘8’ to PC side, until all blocks are erased completely.
When erase is finished, module sends character '0' to PC side to show erase successful.
It can go to the next procedure. Refer to the following figure for command process:

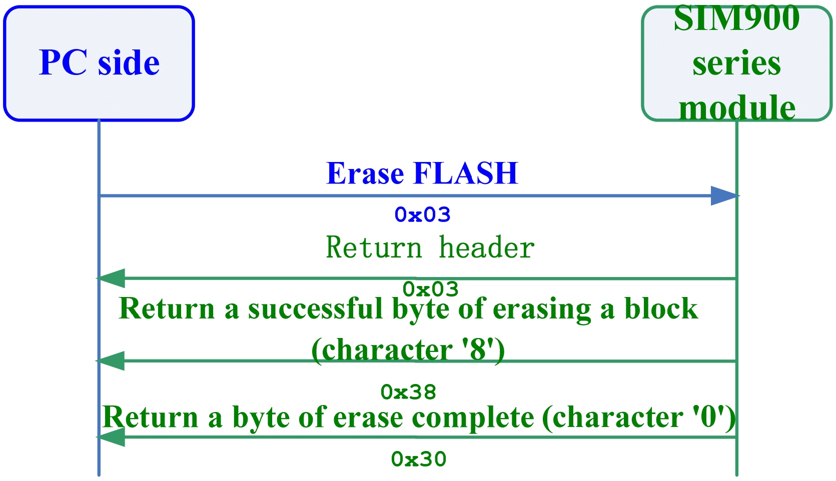

PC side
SIM900 series module
Erase FLASH
0x03
Return header
0x03
Return a successful byte of erasing a block (character '8')
0x38
Return a byte of erase complete (character '0')
0x30

Figure 2-15 FLASH ERASE

2.13.3 Set Download Code Information (0x04)

When command process “FLASH ERASE” is finished;
PC side uses command “Set Download Code Information” to set start address of target file (32bit,LE) and code size (32bit,LE).
When pc side sends this command, module will return 0x04 immediately to confirm setting successful.

Refer to the following figure for command process:

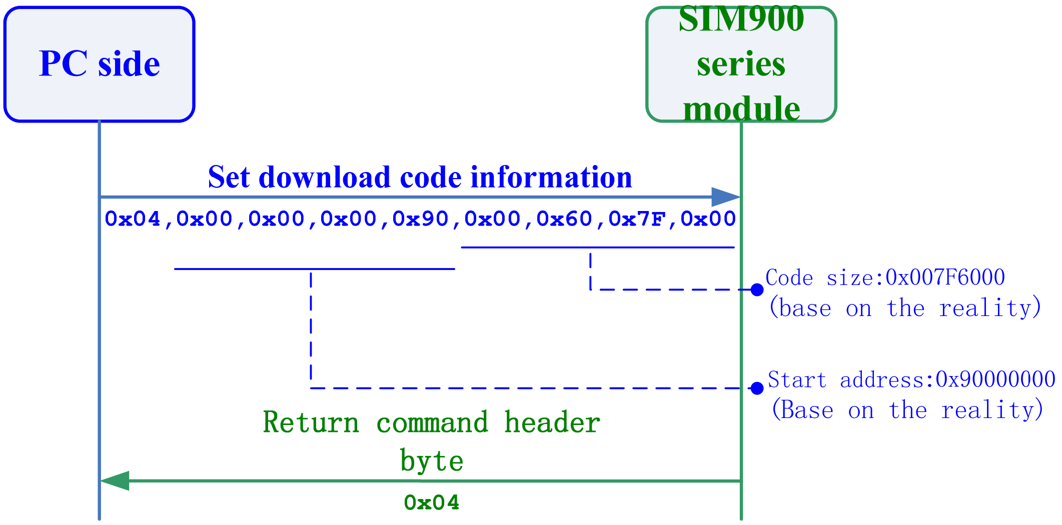


Figure 2-16 Set Download Code Information

2.13.4 Set Download Code Segment (0x01)

When the "Set Download Code Information" procedure is finished;
The length information of the command "Download Code Segment Data" of current transmission can be set. The typical value is 2048(0x800). Refer to the following figure.

2.13.5 Download Code Segment Data (Void)

Every time when command process "Download Code Segment Setting" is finished, it needs to Download Code Segment Data with the length designated by the command "Download Code Segment Setting".
When the module receives the data with the specified length, it will return (0x2E,0x30), that means receiving code segment data successful. Refer to Figure 2-12 for command process:

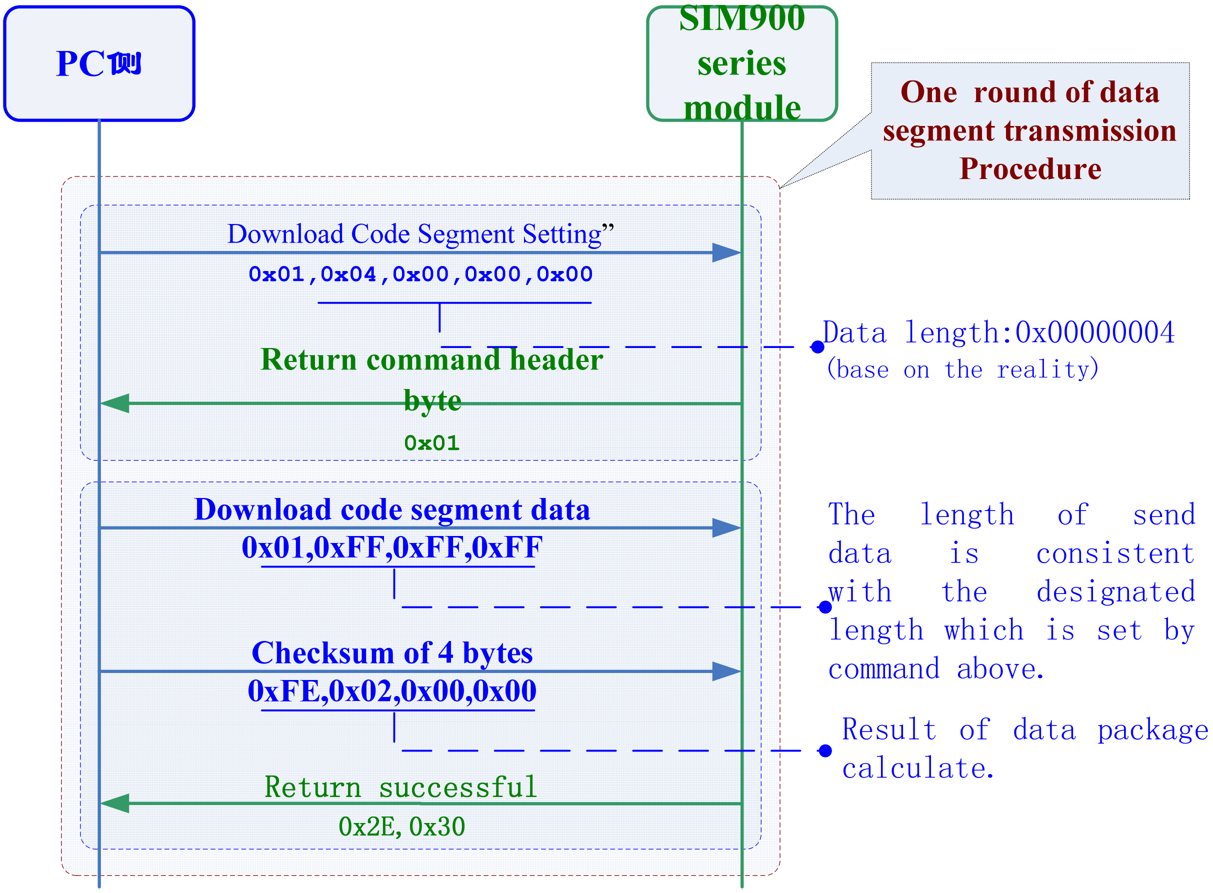

PC侧
SIM900 series module
One round of data segment transmission Procedure
Download Code Segment Setting”
0x01,0x04,0x00,0x00,0x00
Data length:0x00000004 (base on the reality)
Return command header byte
0x01
Download code segment data
0x01,0xFF,0xFF,0xFF
The length of send data is consistent with the designated length which is set by command above.
Checksum of 4 bytes
0xFE,0x02,0x00,0x00
Result of data package calculate.
Return successful
0x2E, 0x30

Figure 2-17 Set Download Code Information

2.14 Write upgrade successful flag bit

2.14.1 Set FLASH Erase Area (0x09)

PC side sends “Compare download information” command, then execute ”SET FLASH ERASE AREA” and ”FLASH ERASE” procedure in turn to accomplish erasing checksum correctness flag bit.

PC side uses “SET FLASH ERASE AREA” command to set target start address of FLASH ERASE area (32bit,LE) and erase size(32bit,LE).

When module receives this command, it will return 0x09 immediately to confirm setting successful.

Refer to the following figure for command process:

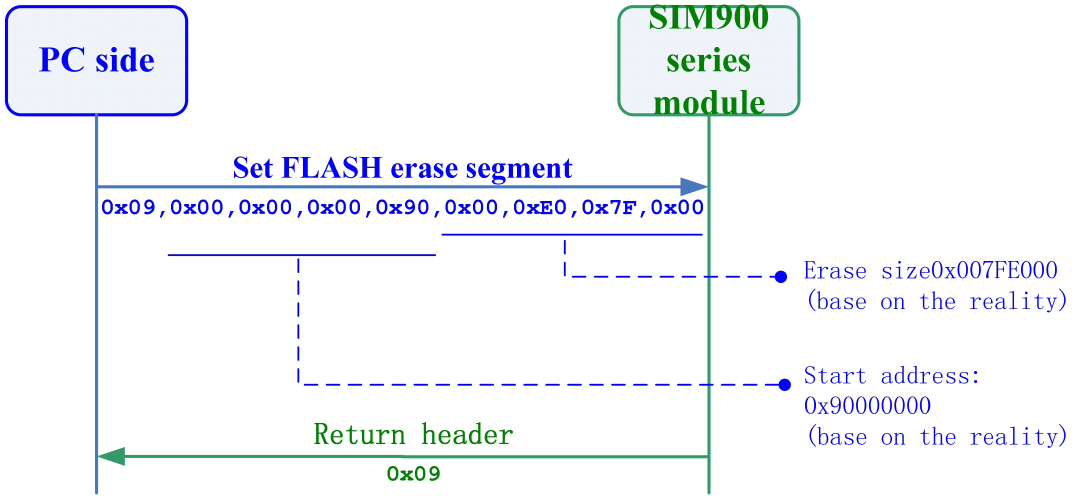


Figure 2-18 Set FLASH ERASE AREA

2.14.2 FLASH Erase (0x03)

When PC side sends "FLASH ERASE" command, the module will return 0x03 immediately;
Then, the module performs actual erase work; once a block of FLASH is erased, the module will return a successful byte (character '8') to PC side until all blocks are erased.
After erasing all blocks, the module will return a byte (character '0') to indicate successful erasing.
It can go to the next procedure. Refer to the following figure for command process:

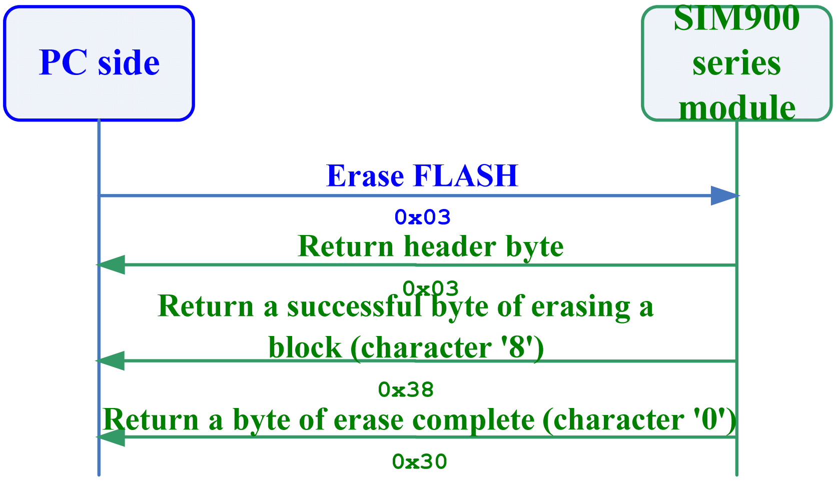

PC side
SIM900 series module
Erase FLASH
0x03
Return header byte
0x03
Return a successful byte of erasing a block (character '8')
0x38
Return a byte of erase complete (character '0')
0x30

Figure 2-19 FLASH ERASE

2.14.3 Set Download Code Information (0x04)

When the command process "FLASH ERASE" is finished;
PC side uses "Set Download Code Information" command to set target start address of downloading file and code size(32bit,LE).
When PC side sends this command, module will return 0x04 immediately to confirm setting successful.
Refer to the following figure for command process:

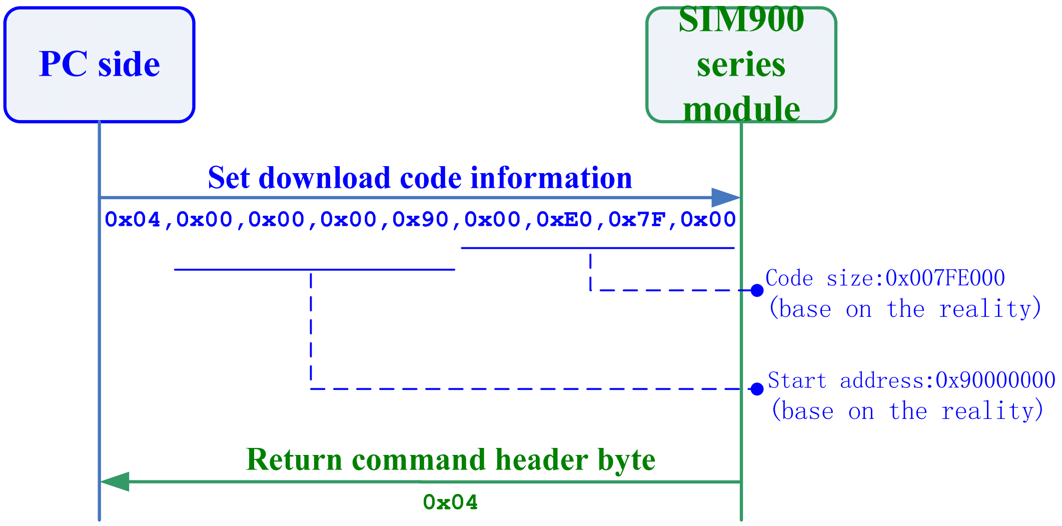


Figure 2-20 Set Download Code Information

2.14.4 Set Download Code Segment (0x01)

Refer to the following figure: When PC side finishes command process "Set Download Code Information", the length information of the command "Download Code Segment Data" can be set，the typical value of this length is 2048 (0x800).

2.14.5 Download Code Segment Data (Void)

Every time when the command process "Set Download Code Segment Setting" is finished, it should Download Code Segment Data.

Now PC side only needs to send data of the designated length which is set by command "Set Download Code Segment".

When module receives designated length and return (0x2E,0x30)，it means receiving code segment data successful. Refer to Figure 2-21 for command process:

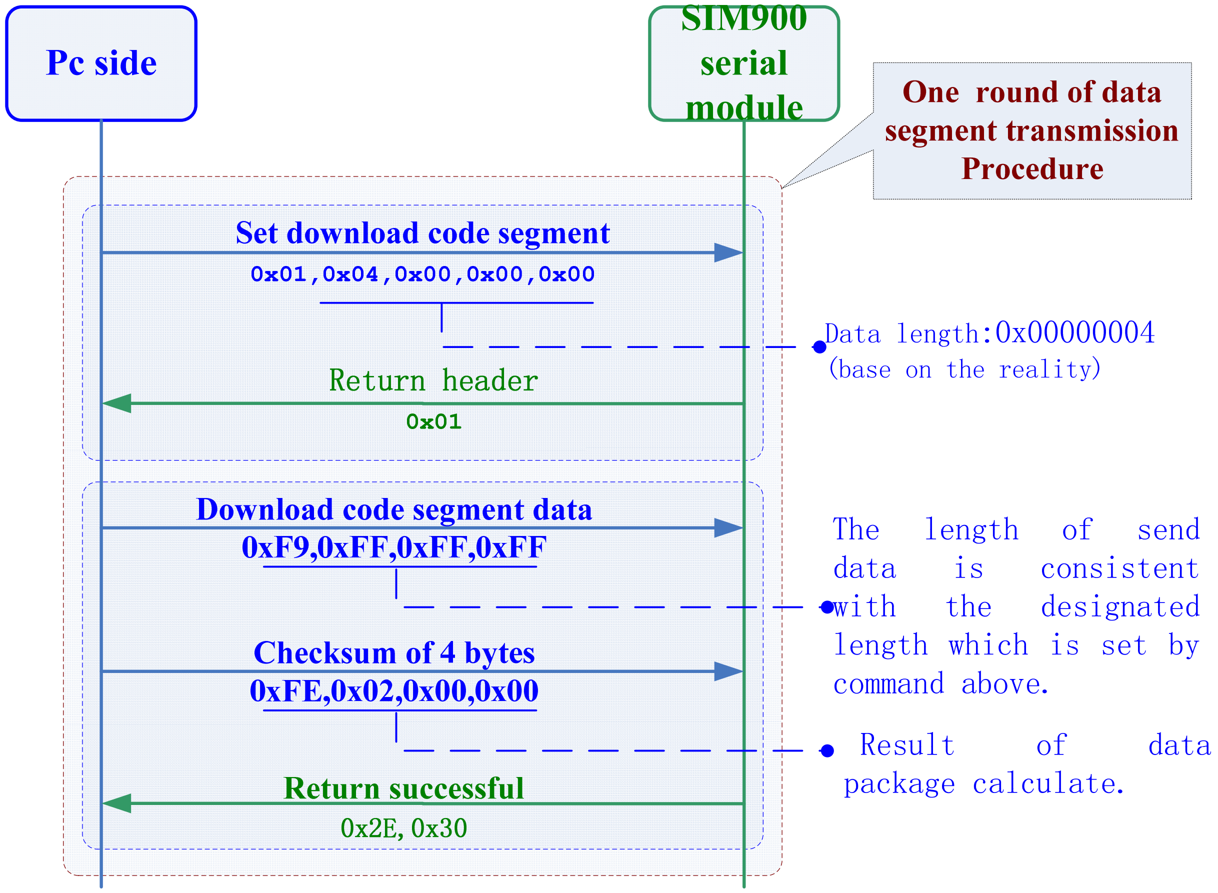

Pc side
SIM900 serial module
One round of data segment transmission Procedure
Set download code segment
0x01,0x04,0x00,0x00,0x00
Data length:0x00000004 (base on the reality)
Return header
0x01
Download code segment data
0xF9,0xFF,0xFF,0xFF
The length of send data is consistent with the designated length which is set by command above.
Checksum of 4 bytes
0xFE,0x02,0x00,0x00
Result of data package calculate.
Return successful
0x2E, 0x30

Figure 2-21 Set Download Code Information

2.15 Send Reset Command (0x06)

Reset instruction can be sent after PC side accomplished “write update successful flag”. About 10seconds later, the module will reset itself, Refer to the following figure:

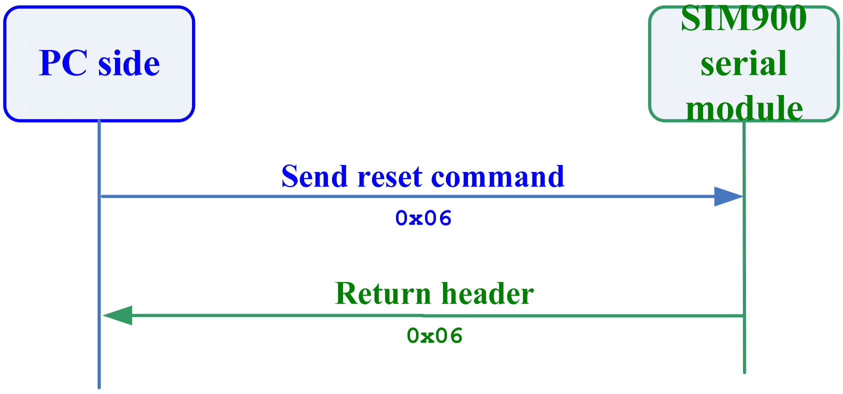


Figure 2-22 Set Download Code Information

2.16 Module Reset

Reset module, if the synchronization byte (0x16) is not received within 50 ms, module will go into normal procedure and start to run the newly downloaded program.

3 Command

Downloading code from PC side to SIM900 series module needs a series of commands interaction through serial port; Command always started from PC side, and the module response the corresponding command; Refer to the following commands:

Table 3-1 Table of PC Command and Module Response

Serial Number	**PC side Command**				**Module Response**				
	Command Type	Head Byte	Content		Head Byte	Content			
1	Check synchronized byte	0x16	--		0x16				
2	Download Intel HEX file	--	base on the real HEX data		--	Hex file download result (8bit,or two 8bit)			--
3	Reset download serial port baud rate	0x07	baud rate (32bit,LE)		0x07	--			--
4	Set flow control method	0x05	Fixed data 0x00(8bit)		0x05	--			--
5	Read FLASH manufacturer information	0x16	Start address (32bit,LE)		0x16	vender number (16bit,LE)	device number (16bit,LE)	extended number 1 (16bit,LE)	extended number 2 (16bit,LE)
		--	15 bytes configuration information (refer to comment7)		--	FLASH size(32bit,LE)			
6	SET FLASH ERASE AREA	0x09	Start address (32bit,LE)	Erase size(32bit,LE)	0x09	--			--
7	Execute FLASH ERASE	0x03	--		0x03	--			--
		--	--		--	0x38…0x38…0x38…0x30			
8	Set Download	0x04	Start address (32bit,LE)	File size (32bit,LE)	0x04	--			--

	Code Information							
9	Download Code Segment Setting	0x01	Data Length (32bit,LE)			0x01	--	--
10	Download Code Segment Data	--	Data			--	0x2E,0x30	--
11	Compare download information	0x15	Start address (32bit,LE)	Checksum (32bit,LE)	File size(32bit,LE)	0x15	Checksum(32bit,LE)	Compare result
12	Reset Command	0x06	--			0x06	--	--
Comment	1. 32bit means 32bit data, LE means little edian, small end in the front. For example: “0x12,0x34,0x56,0x78” represents HEX value0x78563412. 2. 16bit means 16 bit data, LE means little edian, small end in the front. For example: “0x12,0x34” represents HEX 0x3412. 3. FLASH ERASE size equals to file size usually. 4. Consuming time for accomplishing “Execute FLASH ERASE” command has relation with the size to be erased. 5. In “Verify baud rate reset” command, “Verify data” value is fixed 0x00. 6. A typical waiting time from PC side sending command to the module response confirm information is 4 seconds. If exceed this time the module doesn’t response, it will be regarded as command failure. (For the file size is small, “Download Intel HEX file” command may takes 3 seconds totally because) 7. In “Read FLASH Manufacturer Information” command, after PC side received FLASH information, it must send FLASH related configuration to the module. This part of configuration information should be set according to different type of FLASH. Refer to table 3-3.							

Table 3-2 PC side command and module response example

Serial Number	PC side Command		Module Response
	Command Type	Content(hex)	Content(hex)
1	Check synchronization byte	0x16	0x16
2	Download Intel HEX file	based on the actual HEX data	0x30,0x00
3	Reset download serial port baud rate	0x07,0x00,0x08,0x07,0x00	0x07
4	Verify baud rate reset	0x05,0x00	0x05
5	Read FLASH manufacture information	0x02	0x20,0x00,0xC0,0x88,0xFF,0xFF,0xFF,0xFF
		0x40,0x00,0x7F,0x00,0x08,0x08,0x00,0x01,0x00,0x02,0x02,0x02,0x02,0x03,0x02	0x00,0x00,0x80,0x00
6	SET FLASH ERASE AREA	0x09,0x00,0x00,0x00,0x90,0x00,0x99,0x26,0x00	0x09
7	FLASH ERASE	0x03	0x03
8	Set Download Code Information	0x04,0x00,0x00,0x00,0x90,0x00,0x99,0x26,0x00	0x04
9	Download Code Segment Setting	0x01,0x00,0x80,0x00,0x00	0x01
10	Download Code Segment Data	based on the actual code segment data	0x2E,0x30
11	Compare download information	0x15,0x00,0x00,0x00,0x90,0x99,0x31,0xF0,0x0C,0x00,0x99,0x26,0x00	0x15,0x99,0x31,0xF0,0x0C,0x30
12	Reset command	0x06	0x06

Table 3-3 FLASH Information Comparison Table

FLASH Type	Vender Number	Device Number	Extended Number1	Extended Number2	Configuration Information
ST 64M	0x0020	0x88C0	0xFFFF	0xFFFF	0x40,0x00,0x7F,0x00,0x08,0x08,0x00,0x01,0x00,0x02,0x02,0x02,0x02,0x03,0x02
ST 32M	0x0020	0x8828	0xFFFF	0xFFFF	0x40,0x00,0x3F,0x00,0x08,0x08,0x00,0x01,0x00,0x02,0x02,0x02,0x02,0x03,0x02
SPANSION 64M	0x0001	0x007E	0x0061	0x0001	0x40,0x00,0x7F,0x00,0x08,0x08,0x00,0x20,0x00,0x01,0x01,0x01,0x01,0x00,0x01
SAMSUNG 64M	0x00EC	0x2254	0x0000	0x0000	0x40,0x00,0x7F,0x00,0x08,0x08,0x00,0x01,0x00,0x05,0x01,0x01,0x01,0x00,0x01

Contact us:

Shanghai SIMCom Wireless Solutions Ltd.

Add: Building A，SIM Technology Building，No.633，Jinzhong Road，Changning District, Shanghai,P. R. China 200335
Tel: +86 21 3235 3300
Fax: +86 21 3235 3020
URL: www.sim.com/wm