LMX9838 Firmware Release Note

National Semiconductor
Application Note 1706
Markus Roemer
September 2007

1.0 Introduction

The National Semiconductor LMX9838Bluetooth® Serial Port module is a highly integrated radio, baseband controller, memory device, crystal, antenna and loop filter and internal EEPROM. All hardware and the on-chip ROM firmware is included to provide a complete solution from antenna through the complete lower and upper layers of the Bluetooth stack, up to the application including the Generic Access Profile (GAP), the Service Discovery Application Profile (SDAP), and the Serial Port Profile (SPP). The module includes a configurable service database to fulfil service requests for additional profiles on the host.

LMX9838 is optimized to handle the data and link management processing requirements of a Bluetooth node. The firmware supplied within this device offers a complete Bluetooth (v2.0) stack including profiles and command interface. This firmware features point-to-point and point-to-multipoint link management supporting data rates up to the theoretical maximum over RFComm of 704 kbps. The internal memory supports up to 7 active Bluetooth data links and 1 active SCO link.

Due to our continuously ongoing quality tests and firmware improvements, several changes to the firmware have been made to provide highest reliability and performance.

This document describes all release changes within the LMX9838 firmware.

This document is based on:

TABLE 1. LMX9838 Module Configuration

Item	Version
Hardware	LMX9838
Firmware	v2.12
Actual Firmware Release in production	v2.12

2.0 Key Considerations on Converting From v2.12 to Latest Revision

Since the LMX9838 is ROM based, firmware upgrades can only be done by complete ROM spins, which result in a new chip delivered by National Semiconductor.

Software developers should keep the following considerations in mind to prepare the host software for future upgrades of the LMX9838 ROM code. National Semiconductor, of course, will try keep 100% backwards compatibility to avoid problems when replacing existing devices in your products.

However, some important issues need to be considered in software.

2.1 FIRMWARE VERSION IN READY EVENT

Each LMX9838 comes up with a certain “Ready” Event, which indicates the completed boot process of the device. This event also includes the firmware version of the device. The “Ready” appears after boot or after a software reset.

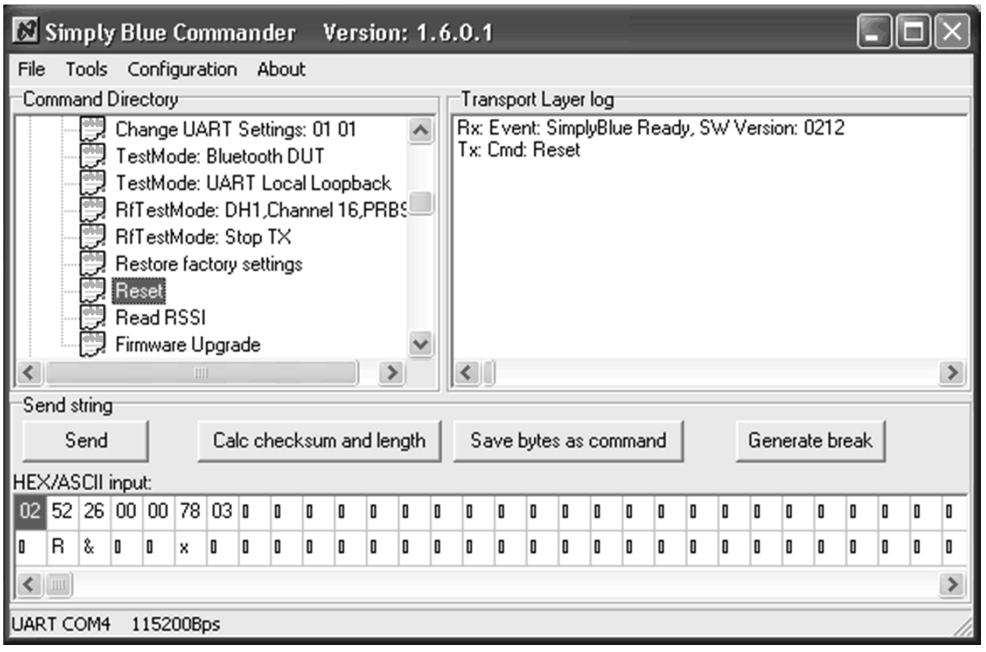
See *Figure 1* for a screenshot of the event in Simply Blue Commander.

For example, the LMX9838 will come up with the hexadecimal code:

Rx(RAW): 02,69,25,05,00,93,04,**30,32,31,32,**03

on which the bold bytes indicate the firmware version (in this case 0212).

In order to avoid any future upgrade problems, please make sure your software does not use this parameter as part of the decision to continue. The parameter should just be used for informational purposes.



30036301

FIGURE 1. "SimplyBlue Ready" in Simply Blue Commander

2.2 PATCHES

The LMX9838 includes the functionality of patching, which allows small bug fixing and firmware modifications. Latest patches are distributed and can be downloaded at the Simply Blue Developers Website at http://www.national.com. Please see *Section 5.0 Firmware Release History* for patches available at release of this document.

Since patches are specific to each firmware release, the patches should only be applied to those devices. To avoid, that a wrong patch is applied to the firmware, the patch includes the firmware version information, which is verified by the LMX9838 firmware at the beginning of the patching process.

2.2.1 Patch in pre-programmed EEPROM

The LMX9838 includes an internal EEPROM, in which the patch can be stored and will be fetched on each boot process. On normal boot-up, the LMX9838 will check the existence of the EEPROM and will apply the data stored.

2.2.2 Patch in EEPROM, but supplied via command interface

In case the EEPROM is not pre-programmed or requires a Patch newer than the one already stored, the patch would need to be stored via the command interface from either the host or a manufacturing device.

In case a patch needs to be supplied using the "Write ROM Patch" command, the mechanism to take care of requires a specific command flow to be followed. See *Figure 2* for the general patch flow. The complete process is also described in the "LMX9838 Software Users Guide", AN-1699.

Since the patch is stored in EEPROM, this only needs to be done once.

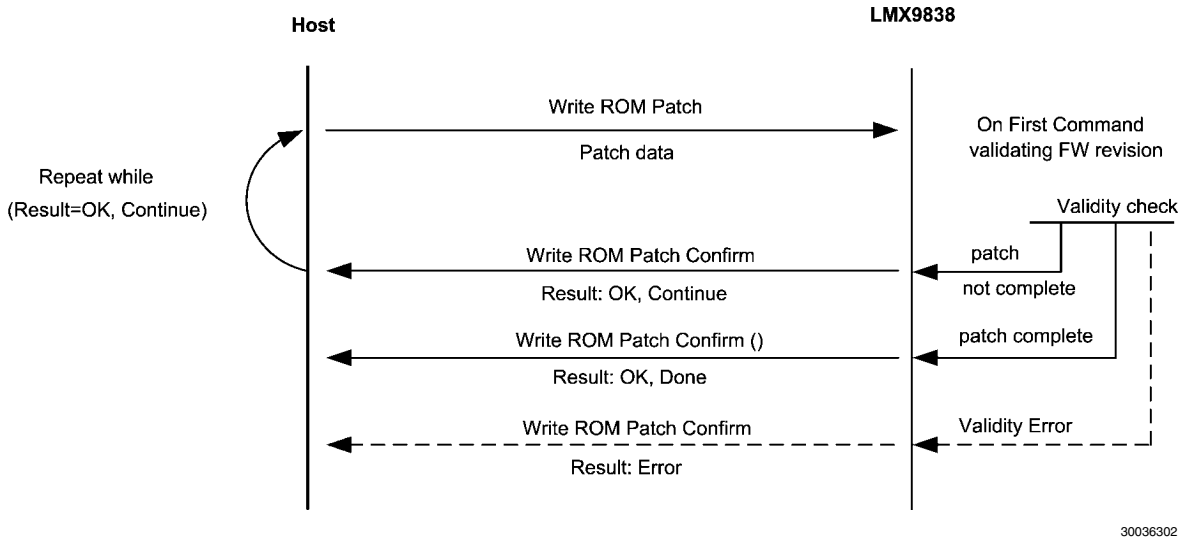


FIGURE 2. Write ROM Patch Flow

The Write ROM patch mechanism includes a validity check of the ROM pushed to the device. In case, no error is found the error code is either 0x01 for continue or 0x00 for OK, Done.

In case the error code is different to those two, some error must have occurred. The following error codes are defined:

- 0x00 = Ok, Done.
- 0x01 = Ok, Continue.
- 0x80 = Error, Not enough info to continue download (a "global" or "segment" meta data group appears to be split).
- 0x81 = Error, Not enough resources to continue download.
- 0x82 = Error, Patch too big.
- 0x83 = Error, Unsupported Patch format revision.
- 0x84 = Error, Patch not applicable to firmware in device.
- 0x85 = Error, Patch CRC check failed.
- 0x86 = Error, Patch NVS validation failed.
- 0x87 = Error, RAMAddr or VarAddr out of RAM area.
- 0xFF = Error, Unspecified error.

So in case the host tries to apply a patch released for firmware 2.12, to another firmware, the confirm will respond with error message 0x84.

Therefore the software needs to be prepared to handle this error code correctly by either continuing with the normal boot process without the patch, or to try to apply a patch for another firmware version.

To be prepared for future upgrades, the host application should not stop the execution due to this error code.

3.0 Known Bugs

3.1 VERSION 2.12

TABLE 2. List of Known Bugs on Firmware v2.12

Bug Type	Description	Workaround
Transmission Problem in command mode	When the module is in command mode, Data pending are not flushed when the RFCOMM connection is terminated by link time-out.	Patch 2
SDAP_SERVICE_REQUEST command confirm wrong	Confirm includes additional wrong byte after the correct handle on position 3+4*Length (Last byte of payload).	Ignore Last Payload Byte
EEPROM locked up by hardware reset	The EEPROM might lock up in case the LMX9838 Reset is pulled low during a read cycle. This mainly can happen on power up or after a software or hardware reset.	See *Section 4.1 SAFE RESET TIMING* for preventing lockup and *Section 4.2 RECOVER FROM EEPROM LOCKUP* for recovering from lockup

4.0 Workarounds

4.1 SAFE RESET TIMING

The LMX9838 stores all non-volatile information like Service Database, Local name, Bluetooth Device Address and patches into an integrated EEPROM. The EEPROM is connected to the internal baseband controller through a serial interface.

On power-up, after hardware or software reset, the EEPROM content is read back from the baseband controller.

Applying the Hardware Reset (using pin Reset#) of the LMX9838 only resets the baseband controller within the device. The EEPROM keeps the last status and is only “reset” by power cycling the complete module.

In case the Hardware Reset is applied while the EEPROM is accessed by the baseband controller, it may occur that the EEPROM locks up on the serial interface a

nd can not be accessed from the baseband controller anymore. The result of this is, that the LMX9838 will respond with the “Await initialization” Event, which indicates, that the bluetooth address could not be read from the EEPROM.

To avoid this scenario, the LMX9838 RESET# must not be pulled low between one of the following events and the device sending the “Ready” Event on the UART interface:

- on power-up (after pulling Reset# high)
- after a hardware reset (using the pin Reset#)
- after a software reset (using the command “Reset”)

In case it is not possible to read back the “Ready” Event (e.g. it is not possible to parse the LMX9838 events), the workaround can be implemented by waiting for about 1 second, before re-applying the hardware reset again. The estimated maximum time for the firmware to initialize is about 900milliseconds, so 1 second should give enough margin.

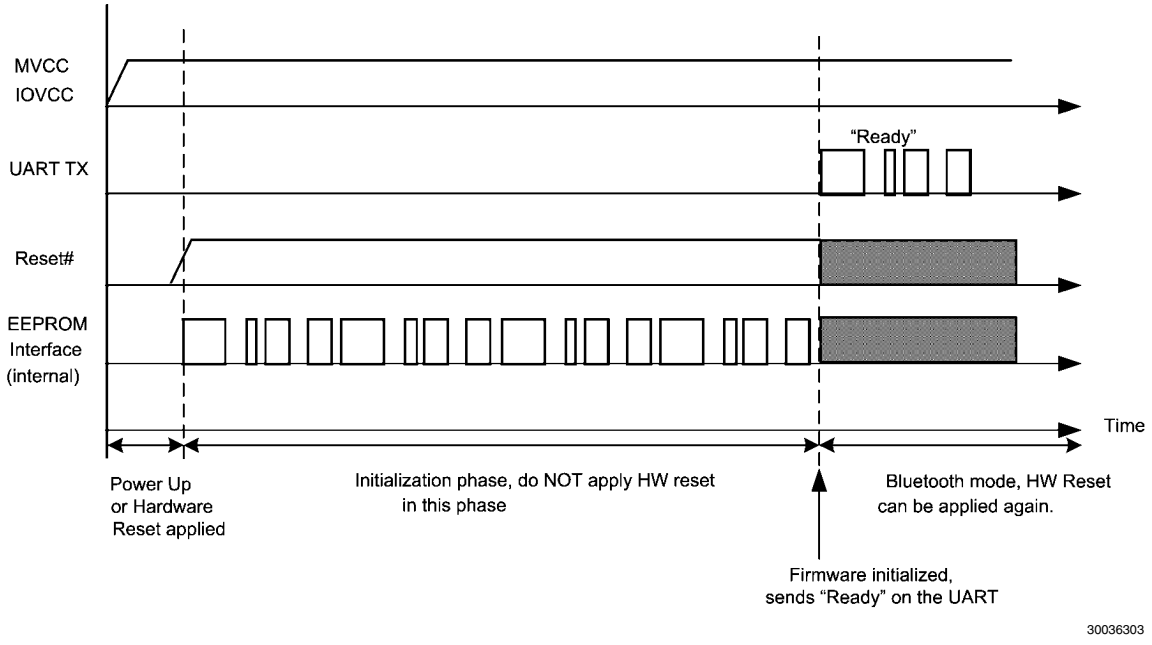


FIGURE 3. Safe Reset Timing on Power-up or After Hardware Reset

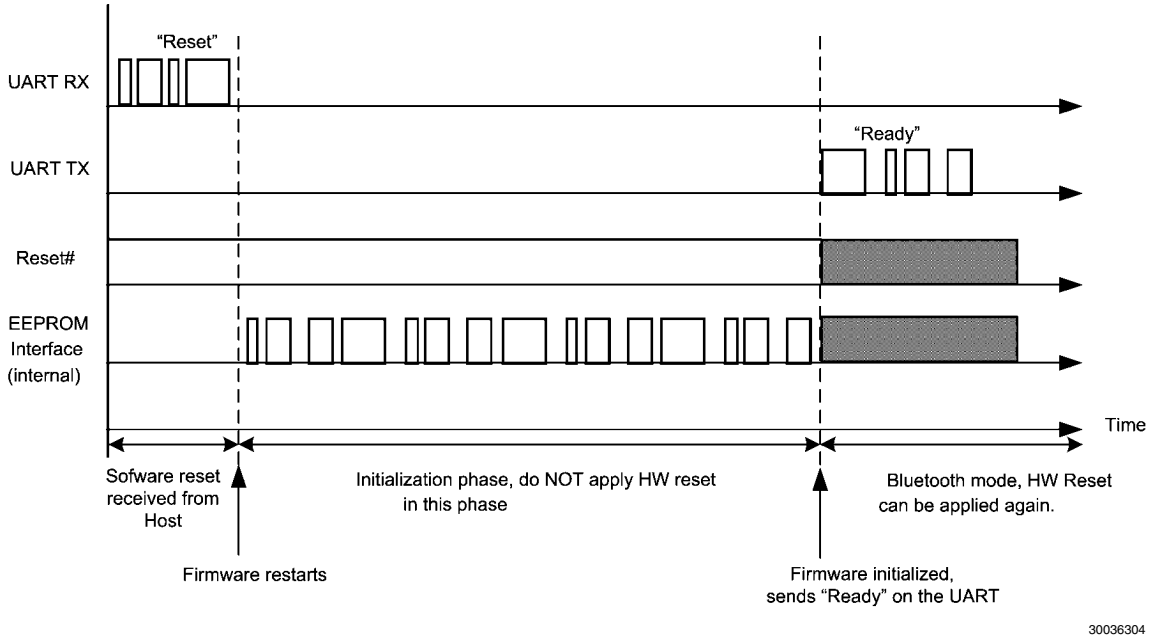


FIGURE 4. Safe Reset Timing on Software Reset

4.2 RECOVER FROM EEPROM LOCKUP

If a Hardware reset, Software reset or Power up occurs during the EEPROM initalization phase, the EEPROM might be unrecognized and might lock-up. If this situation happens, there is a way to recover and reset the module. On receiving the AWAIT_INITIALIZATION_EVENT perform the following steps:

1. Write BD_ADDR
2. Load the Patch 10
3. Send ENTER_BLUETOOTH_MODE command
4. Send RESET command

After sending the BD_ADDR write command, the SimplyBlue commander log window should look like the following.

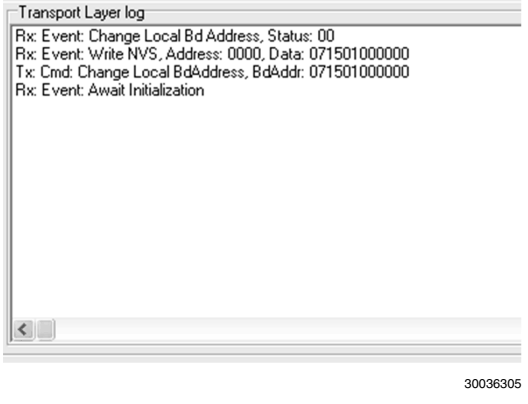


FIGURE 5. Step 1, Write BD_Addr

After sending the Patch 10 and Enter Bluetooth Mode command, the log window should show:

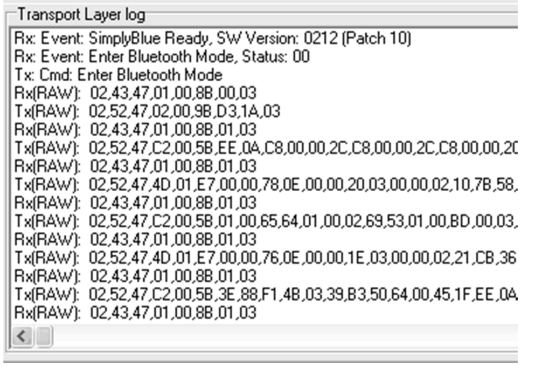


FIGURE 6. Step 2/3, Apply Patch 10 and Enter BT_Mode

Finally after software reset the module recovers and is back to its normal operation mode.

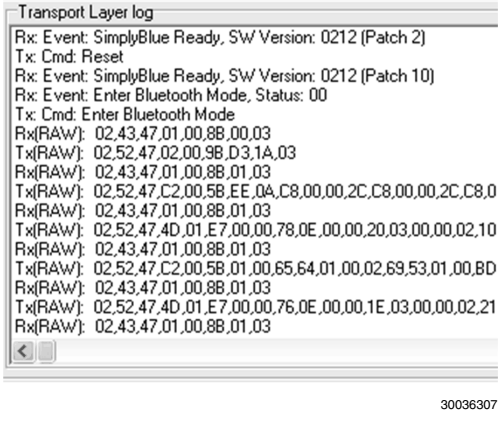


FIGURE 7. Step 4, Send Software Reset

5.0 Firmware Release History

Release date: January 2006

5.1 VERSON 2.12

TABLE 3. Firmware Release Changes 2.12

Issue	Type	Description
None	None	Initial release.

5.2 PATCH 10

Release date: September 2007

Note: This is a Patch workaround but not an EEPROM Patch. It should not be stored in EEPROM. See *Section 4.2 RECOVER FROM EEPROM LOCKUP* for details on how using this Patch.

TABLE 4. Firmware Patch 10 v2.12

Issue	Type	Description
EEPROM Lockup	Workaround	EEPROM not recognized: the module sends the “Await_Initlialization_Event” on boot-up. See *Section 4.2 RECOVER FROM EEPROM LOCKUP* for details.

5.3 PATCH 2

Release date: July 2006

TABLE 5. Firmware Patch 2 v2.12 Changes

Issue	Type	Description
Transmission Problem in command mode when link terminated by link time-out	Bug Fix	When the module is in command mode, Data pending are not flushed when the RFCOMM connection is terminated by link timeout. This could cause the device to be stuck.

5.4 PATCH 1 (TEST PATCH)

Release date: January 2006

TABLE 6. Firmware Patch 1 v2.12 Changes

Issue	Type	Description
None	Validation	Internal use. Test Patch for validation.

Notes

Notes

National Semiconductor Americas Customer Support Center
Email: new.feedback@nsc.com
Tel: 1-800-272-9959

National Semiconductor Europe Customer Support Center
Fax: +49 (0) 180-530-85-86
Email: europe.support@nsc.com
Deutsch Tel: +49 (0) 69 9508 6208
English Tel: +49 (0) 870 24 0 2171
Français Tel: +33 (0) 1 41 91 8790

National Semiconductor Asia Pacific Customer Support Center
Email: ap.support@nsc.com

National Semiconductor Japan Customer Support Center
Fax: 81-3-5639-7507
Email: jpn.feedback@nsc.com
Tel: 81-3-5639-7560