Working with the MDM9x4x platform

The bootloader runtime (NPRG) running using the MBM9x4x (download mode) SBL (download) interface has an unfortunate feature. It consists in the lack of the ability to get full access to the registers of the NAND controller, which is the main condition for the operation of qtools utilities designed for direct work with the flash drive, including qrflash and qwdirect. It is possible that it is still possible to obtain such access, but numerous experiments in this direction have not yet been successful.

Despite this, running a patched NPRG on such a platform is not completely useless. At a minimum, it can be used to read and write data—the contents of the memory and registers of the platform—in some areas of the application processor's address space, either by using the qcommand utility or by using the qrmem utility. In addition, such a loader allows you to run custom appalets, with the help of which an experienced qtools user can implement almost any algorithm for working with the platform, taking into account the restrictions imposed by the restrictions of access rights to resources configured in SBL.

One of the interesting applications of data read/write capabilities is the ability to "programmatically" (without resorting to "barbaric" methods such as locking a point on the device board or erasing the SBL partition) access the PBL interface. For the platform family under discussion, this can be done by writing a value of 1 to the platform's BOOT_MISC_DETECT register (0x193d100 address) and then rebooting. The reboot, in this case, should not be carried out in the normal way (a command 0xb the bootloader), but by performing an operation in the address space that causes an exception - for example, reading data to an address that does not correspond to any of the components of the platform, or data that is protected from reading.

As a result, we get the following approximate scenario of full-fledged work with a flash drive on MDM9x4x platforms:

1. Running NPRG using the SBL interface:

```
./qdload -p/dev/ttyUSB1 -k10 -q

 Waiting for the Hello package from the device...

 Boot Image ID: 00000007

 Load loaders/NPRG9x45p.bin...

 Transfer the loader to the device...

 Loader Handover Successfully
Hello ok, flash memory: MT29F4G08ABBDA3W
```

2. Writing 1 in BOOT_MISC_DETECT:

```
./qcommand -p/dev/ttyUSB1 -c "m 193d100 1"
```

3. Attempt to read to a read-protected address:

```
./qcommand -p/dev/ttyUSB1 -c "d 7980000 4"
```

and interrupt the utility (at this time the system detects the PBL port):

```
^C
```

4. Running ENPRG using the PBL interface:

```
./qdload -p/dev/ttyUSB2 -k10 -i

 Waiting for the Hello package from the device...

 Download image ID: 0000000d

 Load loaders/ENPRG9x45p.bin...

 Pass the bootloader to the device...

 Loader Handover Successfully

 HELLO protocol version: 3
 Chipset: MDM9x4x
 NAND Controller Base Address: 079b0000
 Flash: Micron MT29F4G08ABBDA3W, NAND 512MiB 1.8V 8-bit
 Sector size: 516 bytes
 Page size: 2048 bytes (4 sectors)
 Number of pages per block: 64
 OOB size: 64 bytes
 Type ECC: BCH, 4 bit
 ECC size: 7 bytes
 Spare: 4 bytes
 Defective Block Marker Position: user+1d1
 Total Flash Memory Size = 4096 Blocks (512 MB)
```

Further work with the flash drive on this platform is carried out normally.
For example, viewing the partition table:

```
./qrflash -p/dev/ttyUSB2 -k10 -s@ -m

 #   Start    size   A0 A1 A2 F# format ------ Name------
============================================================
00       0  00000a   ff 01 00 00   LNX   0:SBL
01       a  00000a   ff 01 ff 00   LNX   0:MIBIB
02      14  0000b4   ff 01 ff 00   LNX   0:EFS2
03      c8  000008   ff 01 00 00   LNX   0:TZ
04      d0  000005   ff 01 00 00   LNX   0:RPM
05      d5  000008   ff 01 00 00   LNX   0:aboot
06      dd  000052   ff 01 00 00   LNX   0:boot
07     12f  000002   ff 01 00 00   LNX   0:SCRUB
08     131  000236   ff 01 00 00   LNX   0:modem
09     367  00000c   ff 01 00 00   LNX   0:misc
10     373  000053   ff 01 00 00   LNX   0:recovery
11     3c6  000006   ff 01 00 00   LNX   0:fota_none
12     3cc  0000b6   ff 01 00 00   LNX   0:recoveryfs
13     482  000449   ff 01 00 00   LNX   0:system
14     8cb  00007c   ff 01 00 00   LNX   0:PAD1
15     947  0000a2   ff 01 00 00   LNX   0:USERRW
16     9e9  0001d6   ff 01 00 00   LNX   0:HDATA
17     bbf  0003ae   ff 01 00 00   LNX   0:NTGFOTA
18     f6d  000050   ff 01 00 00   LNX   0:CUST
19     fbd  000030   ff 01 00 00   LNX   0:PERSIST
============================================================
 Partition Table Version: 4
```

Reading the section:

```
./qrflash -p/dev/ttyUSB2 -k10 -s@ -f1

 #   Start    size   A0 A1 A2 F# format ------ Name------
============================================================
01       a  00000a   ff 01 ff 00   LNX   0:MIBIB
 * R: Block 000013 [start+009] (100%)
```

Partition Entry:

```
./qwdirect -p/dev/ttyUSB2 -k10 -fo -b12f pattern.bin

 Entry from pattern.bin file, starter block 12f, size 002
 Recording Mode: Linux Format on a USB Flash Drive
 Block: 0130 Page: 3f
```

and so on.