MediaTek details: SoC startup

Jul 2, 2015

NOTE: This information was obtained from various sources and through reverse engineering. Don't take it as a reference!

I've decided to write down everything I know about MediaTek SoCs, maybe somebody can come up with a cool hack. The following information was checked against the MT6582 quad-core chip present in the bq Aquaris E4.5 and E5 Ubuntu Edition phones.

Memory map

Taken from the MT6575 datasheet:

Bank	Start address	End address	Size	Device(s)
0x0 to 0xB	0x00000000	0xBFFFFFFF	4 x 256 MB = 3GB	DDR memory controller
0xC	0xC0000000	0xC0FFFFFF	16 MB	Infrastructure, Mixmode & MCU system
0xC	0xC1000000	0xC1FFFFFF	16 MB	Peripheral system
0xC	0xC2000000	0xC2FFFFFF	16 MB	Multimedia system
0xC	0xC5000000	0xCFFFFFFF	192 MB	Reserved

Bank	Start address	End address	Size	Device(s)
0xD	0xD0000000	0xDFFFFFFF	256 MB	Modem system
0xE	0xE0000000	0xEFFFFFFF	256 MB	Reserved
0xF	0xF0000000	0xF000FFFF	64 kB	On-chip SRAM
0xF	0xF0010000	0xFFFEFFFF		Reserved
0xF	0xF8000000	0xF800000C	16 Bytes	Chip ID, hardware/software version
0xF	0xF8000010	0xFFFEFFFF		Reserved
0xF	0xFFFF0000	0xFFFFFFFF	64 kB	Boot ROM

Boot ROM

After the CPU has initialized itself, the internal SRAM controller pushes a jump instruction to address 0xFFFF0000. This is the Boot ROM every chip comes with, the contents can't be changed.

The Boot ROM contains a small piece of 32-Bit ARMv7 machine code that performs the following steps:

1. Initialise UART1 (the first serial port) to 8 bit, no parity, 1 stopbit and 9600/19200 baud (depending on the clock).
2. Initialise the internal flash storage.
3. Wait for a `Start` command for 150ms. If no START command is received, load the Preloader into the On-Chip SRAM and execute it.
4. Interpret commands sent by the host, until a JUMP is issued to continue execution elsewhere. This is usually used to download a Preloader into the flash and then boot it.

The Boot ROM supports the following commands:

- `Start`: Signals that there is an external host connected and keeps the Boot ROM from booting from flash.
- `Version`: Returns the security version of the Boot ROM, `0xFF` if it doesn't support security.
- `Serial Link`: Performs some kind of authentication to verify that the tool used by the host is "genuine". If the Boot ROM supports security, the availability of other commands is restricted until this command is completed.
- `Write` and `32 Bit Write`: Write a single 16 or 32 bit value to a 32 bit memory address.
- `Read` and `32 Bit Read`: Read a single 16 or 32 bit value from a 32 bit memory address.
- `Checksum`: Takes a 32 bit memory address and a 32 bit length field and calculates the XOR checksum of the given range.
- `Jump` and `Jump secure`: Continues execution at the given 32 bit memory address location. The secure version will take two additional values, a 32 bit signature memory address and a 32 bit signature length, which will be used by the Boot ROM to check the validity of the program at the jump target address.

I don't know if UART1 is connected to the PCB on the Aquaris E4.5, it might be connected to the headphone jack.

In the next article I will talk about the Preloader.

If you know better and/or something has changed, please find me on Launchpad.net or the Freenode IRC and do get in contact!

References

- Thunder-Kernel
- Boot ROM Design
- MT6575 datasheet

- Introduction of MTK Tools

Sturmflut's blog

Sturmflut's blog

Musings on various things.