Upgrading BIOS using spi-intel

Many Intel CPUs like Baytrail and Braswell include SPI serial flash host controller which is used to hold BIOS and other platform specific data. Since contents of the SPI serial flash is crucial for machine to function, it is typically protected by different hardware protection mechanisms to avoid accidental (or on purpose) overwrite of the content.

Not all manufacturers protect the SPI serial flash, mainly because it allows upgrading the BIOS image directly from an OS.

The spi-intel driver makes it possible to read and write the SPI serial flash, if certain protection bits are not set and locked. If it finds any of them set, the whole MTD device is made read-only to prevent partial overwrites. By default the driver exposes SPI serial flash contents as read-only but it can be changed from kernel command line, passing "spi_intel.writeable=1".

Please keep in mind that overwriting the BIOS image on SPI serial flash might render the machine unbootable and requires special equipment like Dediprog to revive. You have been warned!

Below are the steps how to upgrade MinnowBoard MAX BIOS directly from Linux.

1. Download and extract the latest Minnowboard MAX BIOS SPI image [1]. At the time writing this the latest image is v92.
2. Install mtd-utils package [2]. We need this in order to erase the SPI serial flash. Distros like Debian and Fedora have this prepackaged with name "mtd-utils".
3. Add "spi_intel.writeable=1" to the kernel command line and reboot the board (you can also reload the driver passing "writeable=1" as module parameter to modprobe).
4. Once the board is up and running again, find the right MTD partition (it is named as "BIOS"):

   ```
   # cat /proc/mtd
   dev:    size   erasesize  name
   mtd0: 00800000 00001000 "BIOS"
   ```

   So here it will be /dev/mtd0 but it may vary.
5. Make backup of the existing image first:

   ```
   # dd if=/dev/mtd0ro of=bios.bak
   16384+0 records in
   16384+0 records out
   8388608 bytes (8.4 MB) copied, 10.0269 s, 837 kB/s
   ```
6. Verify the backup:

   ```
   # sha1sum /dev/mtd0ro bios.bak
   fdbb011920572ca6c991377c4b418a0502668b73  /dev/mtd0ro
   fdbb011920572ca6c991377c4b418a0502668b73  bios.bak
   ```

   The SHA1 sums must match. Otherwise do not continue any further!
7. Erase the SPI serial flash. After this step, do not reboot the board! Otherwise it will not start anymore:

   ```
   # flash_erase /dev/mtd0 0 0
   Erasing 4 Kibyte @ 7ff000 -- 100 % complete
   ```
8. Once completed without errors you can write the new BIOS image:

   ```
   # dd if=MNW2MAX1.X64.0092.R01.1605221712.bin of=/dev/mtd0
   ```
9. Verify that the new content of the SPI serial flash matches the new BIOS image:

   ```
   # sha1sum /dev/mtd0ro MNW2MAX1.X64.0092.R01.1605221712.bin
   9b4df9e4be2057fceec3a5529ec3d950836c87a2  /dev/mtd0ro
   9b4df9e4be2057fceec3a5529ec3d950836c87a2 MNW2MAX1.X64.0092.R01.1605221712.bin
   ```

   The SHA1 sums should match.
10. Now you can reboot your board and observe the new BIOS starting up properly.

References

[1] https://firmware.intel.com/sites/default/files/MinnowBoard%2EMAX_%2EX64%2E92%2ER01%2Ezip

[2] http://www.linux-mtd.infradead.org/