

# QEMU support for Xtensa

- Git tree (view): <http://jcmvbkbc.spb.ru/git/?p=dumb/qemu-xtensa.git;a=summary>
- Git tree (clone): <git:jcmvbkbc.spb.ru/~dumb/qemu-xtensa.git> ===== Things to do ===== \* core/basic opcodes implementation; \* [+] and/or/xor/neg/abs; \* [+] shifts; \* [+] add[x\*]/sub[x\*]/add.n/addi.n; \* [+] call0, callx0, j, b\*; \* [+] l32\*, s32\*; \* [+] accurate SR write semantics; \* [-] boolean registers/commands; \* windowed registers; \* [+] call\*/callx\*, retw, rotw, rfwo, rfwu; \* [+] simple overflow algorithm that's triggered from ENTER; \* [+] accurate overflow triggering; \* [+] loop option; \* [+] extended L32R option; \* [-] floating point; \* MMU; \* [+] no-mmu mode; \* [-] proper mem\_idx usage; \* [-] region protection (with/without translation); \* gdbserver; \* [+] xml register map, read/write register; \* [+] correct SR mapping; \* [+] debug exception, single step mode; \* [+] hw/sw breakpoints; \* [-] gdbserver for different processor types; \* [-] debug option; \* exceptions; \* [+] debug (only external); \* [-] break; \* [+] window overflow/underflow; \* [+] user/kernel (invalid insn, privileged insn, alignment, division by 0,...); \* [+] relocatable vectors; \* [+] external interrupts; \* [+] timer interrupts; \* [-] correct opcode timings?; \* [+] qemu timer to avoid busy looping in waiti; \* sample evaluation board; \* [+] memory mapping, ELF loader; \* [-] standard peripherals; \* simulation quality; \* [+] pass command line arguments to argc/argv SIMCALLs (DAN branch only); \* [+] TB chaining; \* [+] external configuration (a-la xtensa overlay)? \* [-] automatic regression test suite; ===== Events ===== \* 2011.04.20: C++ 'hello world' is working in qemu (stdio, stdlib, simcalls, windowed registers, loops, ext l32r) (: \* 2011.04.26: multithreaded ThreadX application is working in qemu (timer interrupts) \* 2011.04.30: preparation for qemu mainline submission started \* 2011.05.04: first RFC patchset sent to qemu-devel <http://lists.nongnu.org/archive/html/qemu-devel/2011-05/msg00242.html> \* 2011.05.18: first PATCH patchset sent to qemu-devel <http://lists.nongnu.org/archive/html/qemu-devel/2011-05/msg01525.html> qemu

From: <http://wiki.osll.ru/> - Open Source & Linux Lab

Permanent link: <http://wiki.osll.ru/doku.php/etc:users:jcmvbkbc:qemu-target-xtensa?rev=1306773038>

Last update: 2011/05/30 20:30

