What's new in QEMU

Alex Bennée

Linaro Connect BUD17-221
Agenda

- QEMU releases & new features
- IoT/uController discussion
Since Last Connect

- QEMU 2.8.0 (Dec 20th, 2016)
- QEMU 2.9.0 (April 4th, 2017)*
- Releases at 3-4 month cadence
- Next release in August?
QEMU 2.8

See changelog for full notes
ITS (Interrupt Translation Service)

- MSI controller
- Virtual MSIs with VMs with GICv3
- Required on GICv3 guests for
  - VHOST
  - Device pass-through (SR-IOV)
TCG Updates

• New TCGOps for:
  ▫ Atomic operations
  ▫ Barriers/fences
New exclusive mechanism

- Support oversized atomics
- Thread safe tb-flush (finally!)
What's new in QEMU 2.9

See changelog for full notes
TCG EL2 Support

- AArch64 only
- Requires GICv3

```bash
qemu-system-aarch64 ${QEMU_OPTS} \
  -machine gic-version=3 \
  -machine virtualization=true
```
MTTCG

• Finally thread-per-vCPU for system emulation!
• Long term project involving many groups
• Linaro has been leading the work for a year
MTTCG Supported Combinations

- Default for ARMv7/AArch64 on x86_64
- Known to work for
  - x86-on-x86
  - x86-on-AArch64 (slowly)

```
$QEMU$QEMU_OPTS -accel tcg,thread=multi
```
Cortex M fixes
QEMU and IoT
M-profile cores are different

- M-profile means micro-controllers
- Different memory model (MPU)
- Different memory model (MPU)
- Different exception model (NVIC)
- Often running an RTOS
Current M-profile models

- TI Stellaris (Cortex M3)
  - LM3S6965EVB
  - LM3S811EVB
- Netduino 2 (Cortex M3)
Current Issues

- Very little attention
  - Linaro has been very focused on A-profile
  - No community maintenance and little bugfixing
- Long standing un-fixed bugs
- Missing important features
- No support for newer CPUs (FPU, v6M)
Modelling Hardware

• Boring hardware
  ▪ mostly just CPU, flash and GPIOs
  ▪ some models **may** have a screen
• Unconnected GPIO/PWM/ADC/DACs
Ongoing work

- NVIC/Exception handling (fixed in 2.9)
  - Bare metal *m-series tests*
- MPU (add missing emulation)
- FPU (enable existing instructions, new exception model)
- v6m (Cortex M0, M0+1, M1) and v8m
What do members want from QEMU IoT support

• Priorities
  ▪ Use cases?
  ▪ Hardware?
  ▪ Other requirements?
Some options for new M-profile board?

- **BBC microBit**
  - Cortex-M0
  - number of built-in peripherals
  - widespread real hardware

- **96boards Carbon**
  - Cortex-M4
  - built in Bluetooth
  - supports Zephyr
Thank You

#BUD17

For further information: www.linaro.org

BUD17 keynotes and videos on: connect.linaro.org