QEMU for SuperH

Magnus Damm

IGEL Co., Ltd.
www.igel.co.jp

June 2008

Outline

Outline

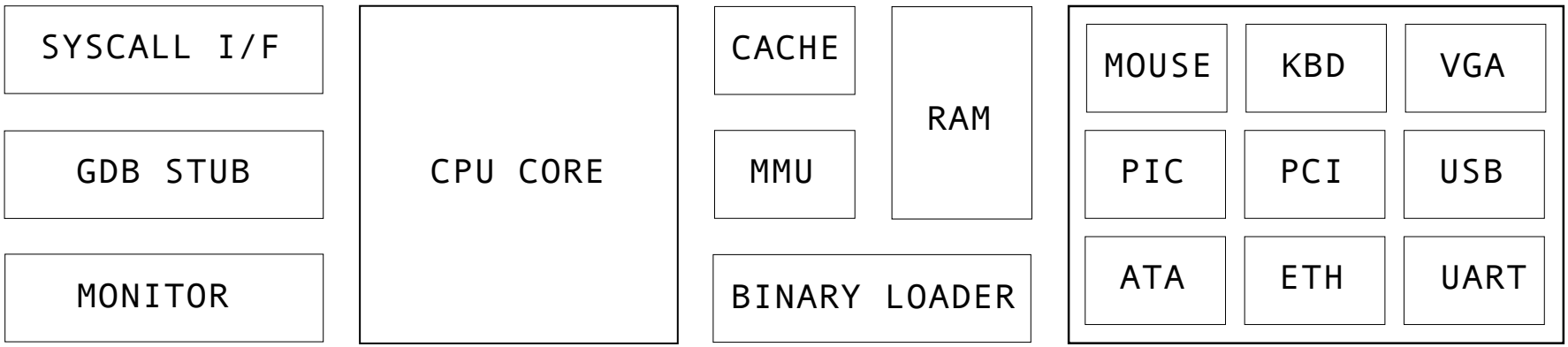
What is QEMU?

QEMU - An Open Source CPU and I/O Device Emulator

Key Applications

- System Emulation:
  - Desktop - Windows XP guest OS inside QEMU
  - Embedded - Android Emulator
- Application Emulation:
  - Desktop - Macromedia Flash x86 binary on PowerPC
  - Embedded - Sbox2 development environment

Emulator Overview



Main Components

- CPU Core Emulator
- I/O Device Emulator
- Debug and Glue Code

Hardware Support

Processors

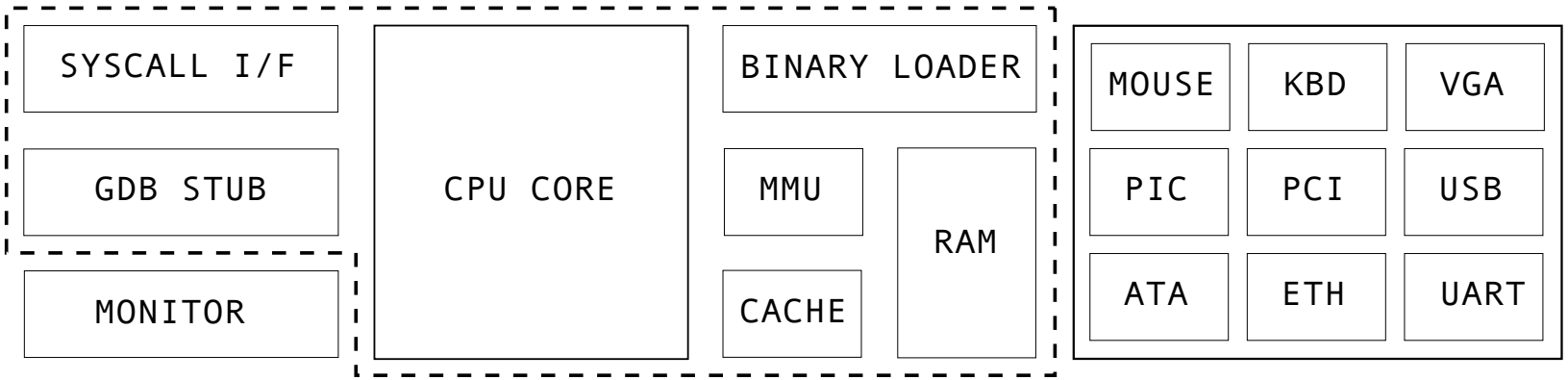
- Alpha, ARM, x86, m68k, Mips, PPC, SH4 and Sparc

I/O Devices

- VGA, Keyboard, Mouse, Sound, Ethernet, ATA, USB...

Outline

The QEMU Application / User Space Emulator



QEMU Application Emulator Components

- Binary Loader
- RAM
- CPU Core
- System Call Interface Translator
- GDB Stub

QEMU Application Emulation Examples

Execute a static i386 binary

```
qemu-i386 busybox-i386
```

Execute a static SH4 Big Endian binary

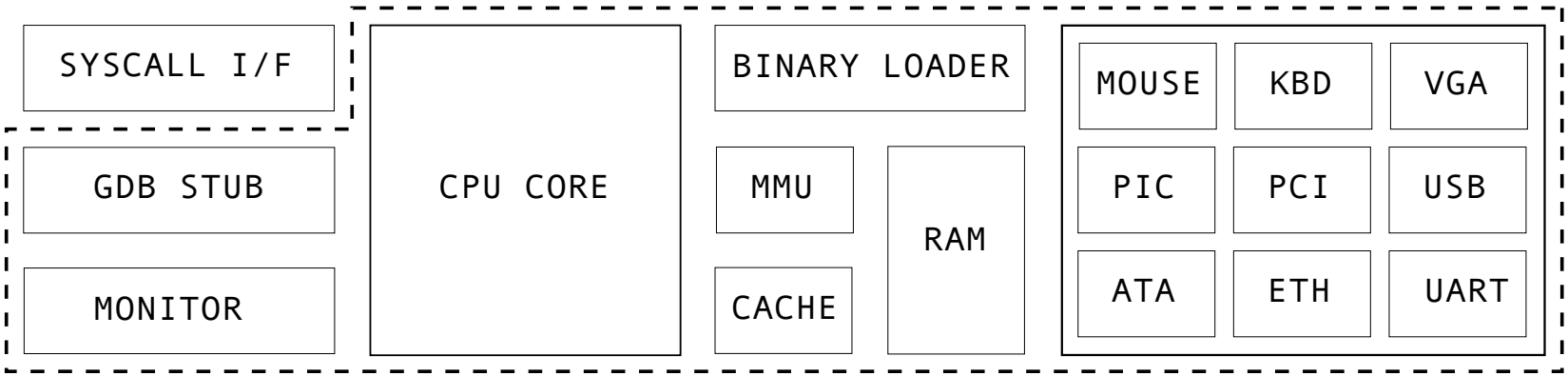
```
qemu-sh4eb busybox-sh4eb
```

Execute a dynamically linked SH4 Little Endian binary

```
qemu-sh4 -L /path/to/sh4/root busybox-sh4
```

Outline

The QEMU System Emulator



QEMU System Emulator Components

- Binary Loader
- RAM
- CPU Core
- I/O Devices
- GDB Stub + Monitor

QEMU System Emulation Examples

Boot x86 software from a virtual CDROM

```
qemu -boot d -cdrom winxp.iso /dev/zero
```

Boot x86 linux kernel using serial console

```
qemu -nographic -kernel bzImage /dev/zero
```

Boot SH4 linux kernel

```
qemu-system-sh4 -M r2d -kernel zImage
```

Outline

CPU Core Emulator

Current Status

A subset of the SH7750 CPU Core is currently emulated. Simple applications are today emulated by the QEMU Application Emulator. The QEMU System Emulator is not fully functional yet.

TODO

- Add Supervisor / User instruction awareness
- Improve FPU and DSP instruction emulation
- Add instruction set test suite
- Fix MMU support
- Cache emulation and statistics gathering
- SMP support
- Convert code to user TCG / SuperH host support

I/O Device Emulator

Current Status

INTC, TMU and SCI(F) are partially emulated.

TODO

- PCIC
- Add interrupt priority support
- Improve SCIF emulation

Fix upstream GDB support.