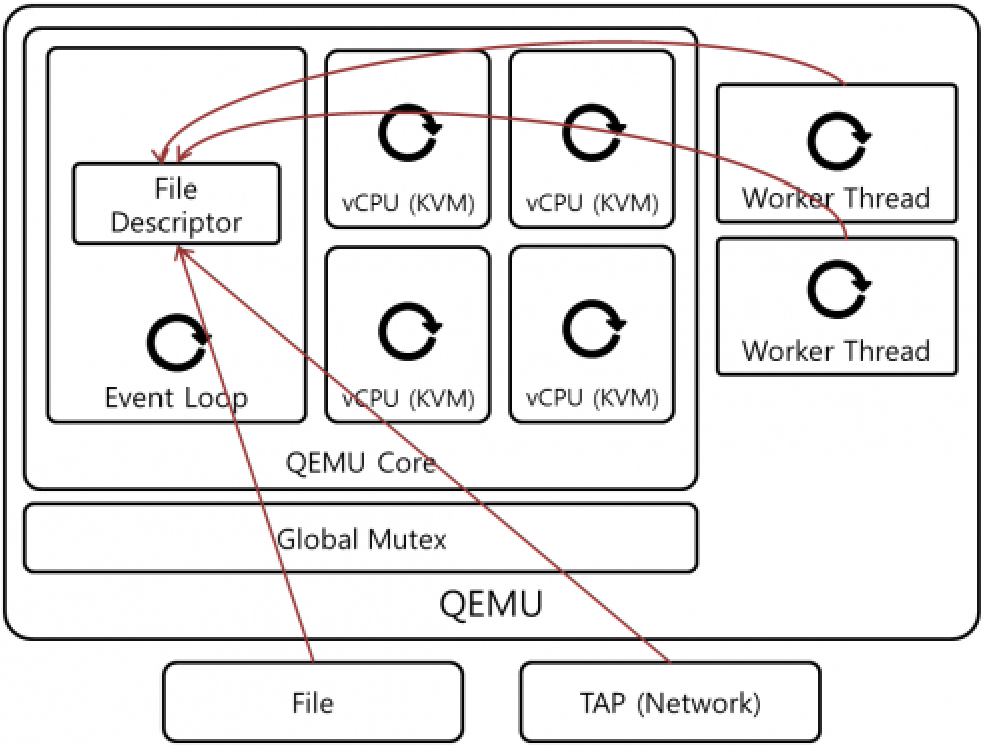
QEMU

- QEMU is **machine emulator** or **virtualizer** for hypervisor.
- QEMU could be run with KVM or Xen.

Contents

1 QEMU + KVM Architecture (with iothread)

- KVM use QEMU for I/O Virtualization.
- QEMU emulates physical devices, virtio devices.

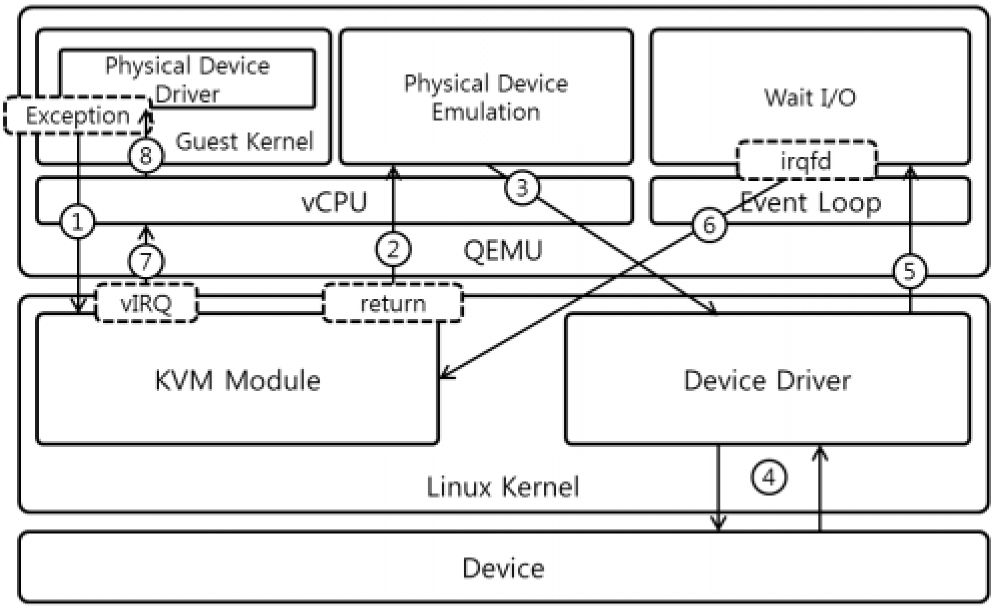


- Event loop
  - Wait file descriptor to receive events.
  - When file descriptor receives events, execute callback functions.
- Callback function
  - Do not run blocking functions and CPU intensive code.
  - Send/Receive packets.
  - Read/Write file.
  - Emulate physical device.
- vCPU Thread
  - Run guest code.
  - Emulate physical device emulation.
- QEMU Core
  - A set of threads that emulate physical/virtio device.
  - Emulation code of physical/virtio device is not thread safe.
  - **Global mutex** is used to serialize emulation code of physical/virtio device.

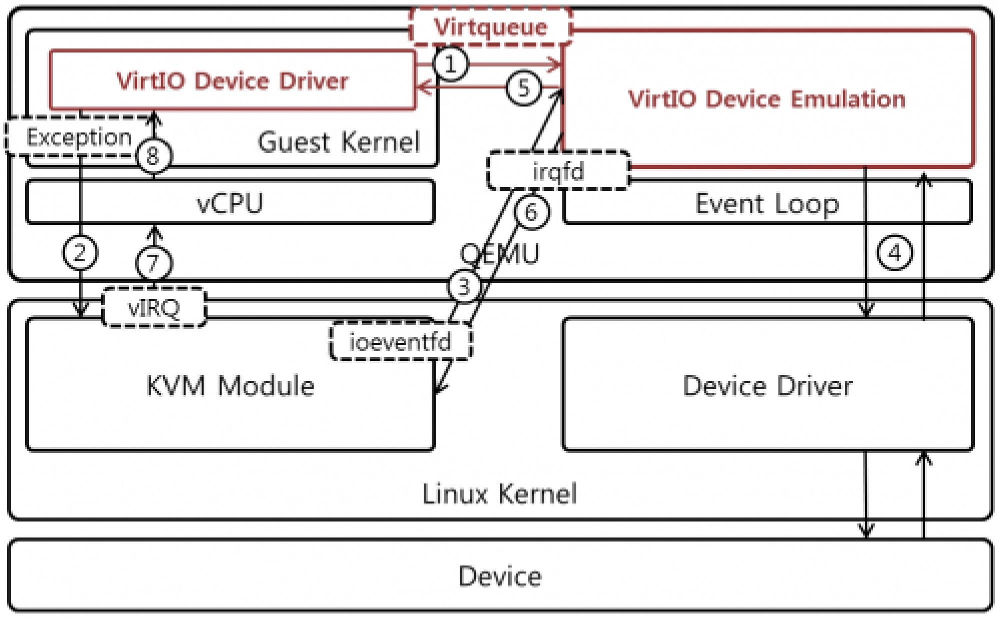
- Worker thread
    - Run Blocking function or CPU Intensive code that cannot be executed in callback functions.
    - Send a event to event loop to notify completion of code execution.

2 I/O Process

2.1 QEMU + KVM (Physical Device Emulation)

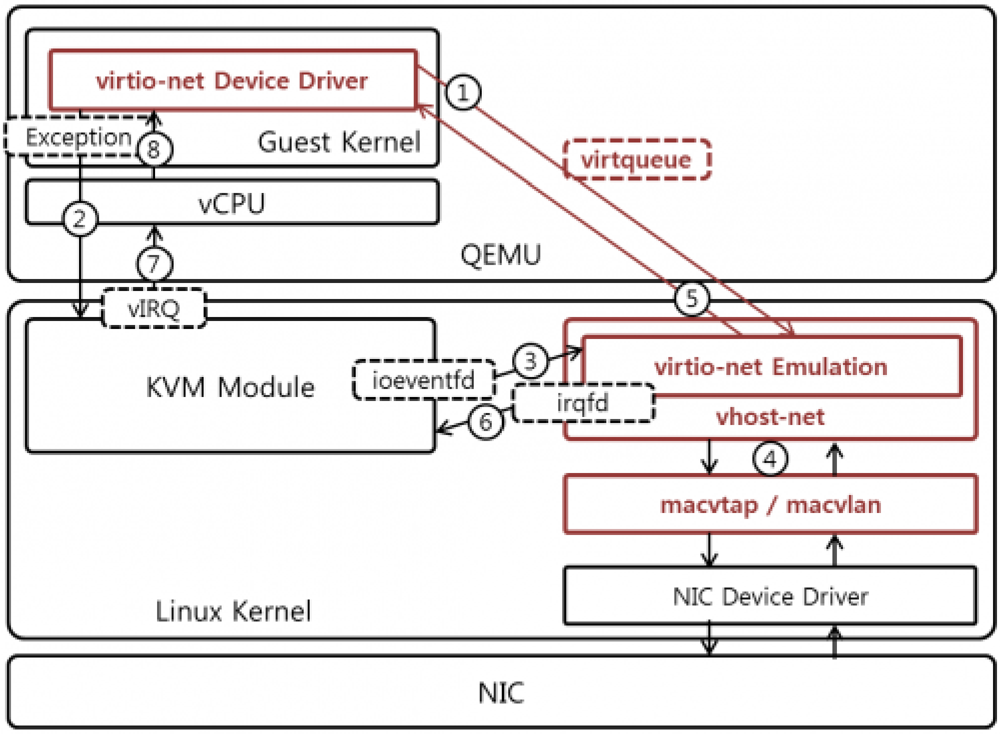


2.2 QEMU + KVM + virtio

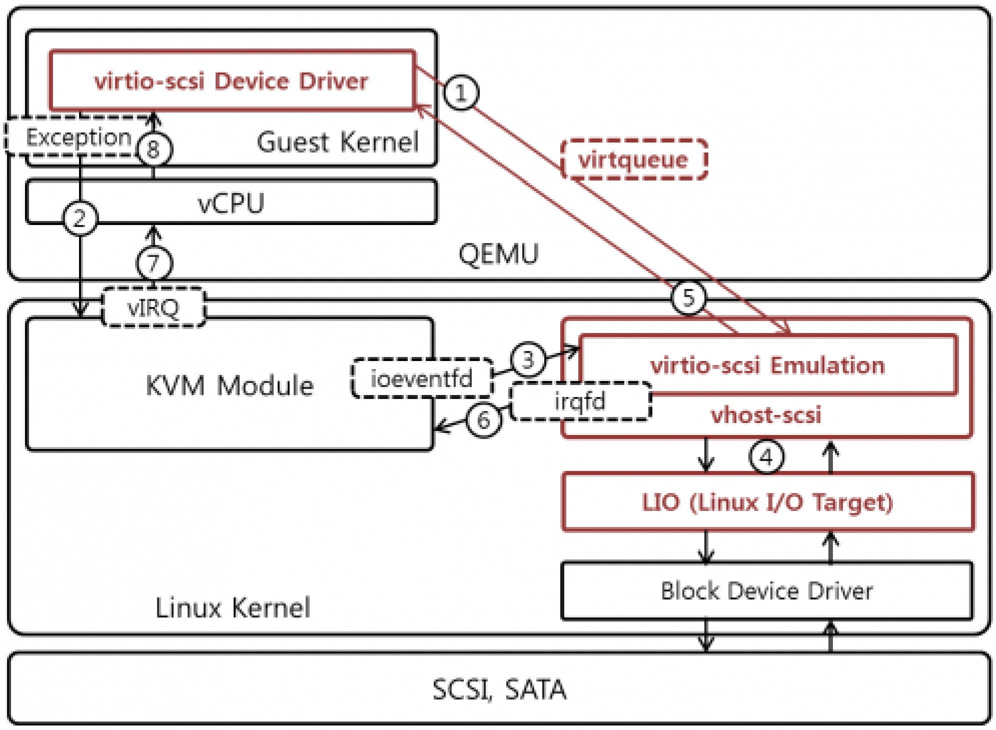


2.3 QEMU + KVM + virtio + vhost

- Network



- SCSI Controller



3 Reference

- QEMU - http://wiki.qemu.org/Main_Page
- QEMU Architecture - http://blog.vmsplice.net/2011/03/qemu-internals-overall-architecture-and.html

Retrieved from "http://ssup2.iptime.org/sup_wiki/index.php?title=QEMU&oldid=1829"

Category: TheoryAnalysis

- This page was last modified on 6 May 2016, at 18:34.