Modern QEMU Devices
A Hands-On Approach

Andreas Färber, B.Sc.
Expert Virtualization
SUSE LINUX Products GmbH
What To Expect Today
Outline Of This Presentation

• Brief introduction to device modeling
• Live conversion of a device into modern form
• Discussion of further upcoming changes
Devices
The Initial Approach: PC Decomposition By Functions

- Floppy (-fda)
- IDE disk (-hda)
- ATAPI CD (-cdrom)
- Network (-net nic)
- Sound (-soundhw)
- Graphics (-vga)
- CPU (-cpu)
Why Rethink Device Modeling?
Compare The Classic PC To Embedded Chipsets!

- Composition
- Encapsulation
- Buses
- Maintenance
- Management
- Competitors

Experts: How many do you recognize?
Device Evolution
Major Modeling Approaches

Abstraction

qdev

0.11 (05/2009)
Device on bus; SysBus!
Declaration bus-specific

2011, M. Armbruster

qdev

1.1 (01/2012)
Device is an Object,
child/link properties

2012, A. Färber

QOM

3.10 (04/2013)
KVM device
control API

Anthony Liguori,
IBM

Scott Wood,
Freescale

ad hoc

0.11 (05/2009)
Device on bus; SysBus!
Declaration bus-specific

2011, M. Armbruster

0.11 (05/2009)
Device on bus; SysBus!
Declaration bus-specific

2011, M. Armbruster

1.1 (01/2012)
Device is an Object,
child/link properties

2012, A. Färber

1.1 (01/2012)
Device is an Object,
child/link properties

2012, A. Färber

3.10 (04/2013)
KVM device
control API

Anthony Liguori,
IBM

Scott Wood,
Freescale

3.10 (04/2013)
KVM device
control API

Anthony Liguori,
IBM

Scott Wood,
Freescale
Demonstration
Demo 1
Selecting A Candidate And Converting From Ad-hoc To QOM

- git grep --files-without-match type_init -- hw/*.c
  - hw/bt/hci-csr.c
  - hw/char/mcf_uart.c
  - hw/char/omap_uart.c
  - hw/char/sh_serial.c
  - hw/display/vga-isa-mm.c
  - ...

- Helpful:
  - QTest test cases for automated regression testing
  - Linux kernel or image for quick functional testing
Demo 2
Properties In Qdev Versus QOM

- qemu-system-m68k -qmp unix:foo,server,nowait
- qom-list -s foo /
- qom-get -s foo /machine/unassigned/device[0].type
Upcoming Changes
Realization
Two-stage Initialization

instance_init
realized = true
instance_finalizer
realized = false

instance_init
realized = true
instance_finalizer
realized = false
Update your devices please & supply integrated test cases!
www.qemu-project.org

Thank you.
We adapt. You succeed.