

# QEMU

Christian Laursen

Århus  
Januar 2008

# Agenda

- 1 Introduktion
- 2 QEMU system emulator
- 3 QEMU user space emulator
- 4 Afslutning

# Hvad er QEMU?

- Open source
- Emulator
- Virtuel maskine

## Hvad kan QEMU?

- Benytter dynamic translation til emulering
- Kan køre kode direkte på host CPU'en med kernemodul (KQEMU)

## Emulerede platforme

- x86
- x86\_64
- ARM
- SPARC
- PowerPC
- MIPS
- m68k (Coldfire)

# QEMU system emulator

- Emulerer en hel maskine
- Kræver et fuldt operativsystem

## Emuleret hardware

- RAM
- Diske - fysiske diske eller images
- CD-ROM - fysisk eller image
- Floppy - fysisk eller image
- Grafikkort - Cirrus Logic GD5446 eller standard VESA
- Netkort - NE2000, Realtek, en række Intel-kort m.fl.
- Lydkort - SoundBlaster 16 m.fl.
- USB - Mus, tablet, disk, passthrough

## Konfiguration

- Sker udelukkende via kommandolinje
- Mulighed for runtime-konfiguration af nogle options
- Understøttelse af konfigurationsfil på tegnebrædtet



## Konfiguration - eksempel

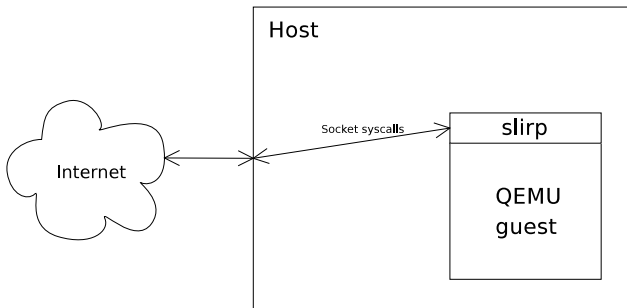
```
qemu -m 512 -localtime -redir tcp:3389::3389 -usb -usbdevice  
tablet -cdrom xp.iso -boot c disk
```

## Netværk - emulerede netkort

- i82551
- i82557b
- i82559er
- ne2k\_pci (default)
- ne2k\_isa
- pcnet
- rtl8139
- smc91c111
- lance
- mcf\_fec

## Netværk - user mode

Baseret på slirp:



## Netværk - user mode

Fordele:

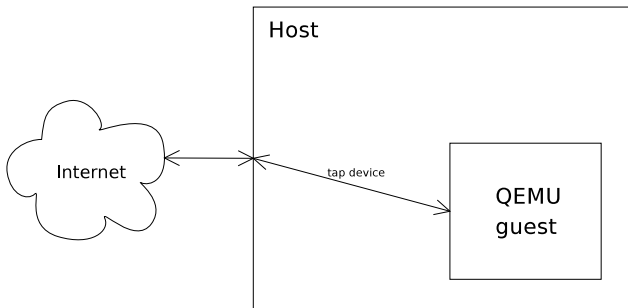
- Kræver ikke root-privilegier
- Ingen konfiguration

Ulemper:

- Diverse begrænsninger

## Netværk - tap

Benytter tap device til at forbinde host og guest:



## Netværk - tap

Fordele:

- Mere fleksibilitet (NAT, bridge, statisk route)
- Ingen begrænsninger

Ulemper:

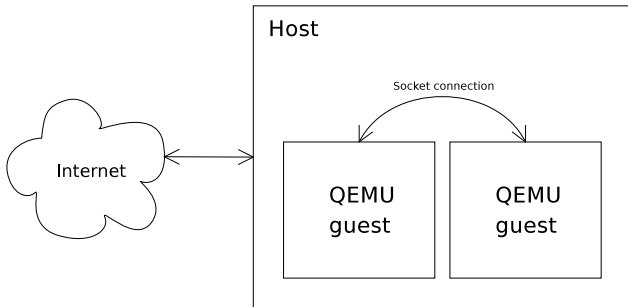
- Kræver root-privilegier
- En del opsætning er nødvendig

## Netværk - tap

```
qemu -net nic -net tap,script=/etc/qemu-ifup disk
```

## Netværk - socket

Forbinder QEMU-instanser via sockets:





## Netværk - socket

- Mulighed for netværk mellem QEMU-instanser adskilt fra det rigtige netværk
- Fleksibelt
- Nok mest til test

## Netværk - tap

```
qemu -net nic -net socket,listen=127.0.0.1:4242 disk  
qemu -net nic -net socket,connect=127.0.0.1:4242 disk
```

## Disk images

- Fysiske drev
- Floppy images
- CD-ROM images
- Harddisk images

## Disk images - filformater

- raw
- qcow2
- vmdk
- cloop

## Disk images - qemu-img

```
qemu-img create -f qcow2 disk.img 3G
```

## QEMU monitor

- Som standard tilgængelig med alt-ctrl-2
- Styling af CD-ROM og floppy-images
- Screenshots
- Sending af tastetryk og musebevægelser
- Tilføjelse eller fjernelse af USB-enheder
- Gemme afspillet lyd til wave-fil

## QEMU monitor - savevm / loadvm

- savevm gemmer den virtuelle maskines tilstand
- loadvm gendanner tilstand gemt med savevm
- Kræver et qcow2 image

## USB passthrough

```
info usbhost  
usb_add host:05ac:8300  
-usbdevice host:0a12:0001
```



## Snapshot

- Ændringer skrives til midlertidig fil
- Aktiveres med “-snapshot”
- Data kan skrives til disk med kommandoen “commit”

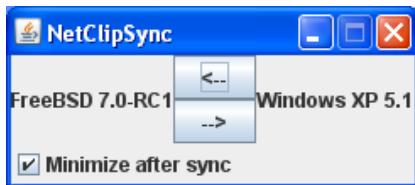
## Desktop-integration

- -no-frame
- -usbdevice tablet

## Desktop-integration - clipboard sharing

- x2x
- x2vnc
- NetClipSync

## Desktop-integration - clipboard sharing



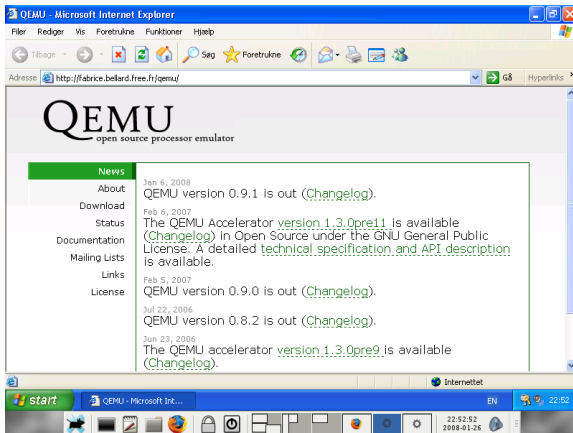
## Desktop-integration - fildeling

- `-smb ~/shared-files`
- `-redir tcp:445::445`

## Desktop-integration - rdesktop

- Hvis der er brug for vilkårlige skærmstørrelser
- -redir tcp:3389::3389

## Desktop-integration - rdesktop



## QEMU user space emulator

- Kører enkeltstående program beregnet til en anden arkitektur
- Kræver shared libraries tilhørende programmets arkitektur
- Virker kun på Linux og Mac OS X/Darwin



## Kommandolinje

```
qemu-sparc -L ~/sparclibs ~/apps/bin/xeyes
```

## Sammenligning med andre programmer

- Bochs
- VirtualBox
- VMWare
- Parallels
- Xen

## Sammenligning Bochs

- Kører på mange platforme
- Understøtter kun x86 og x86\_64 som guest arkitektur
- Ren emulering (Langsomt)
- En del kodeudveksling med QEMU
- Open source

## Sammenligning VirtualBox

- Kører kun på MacOS, Linux og Windows
- Understøtter kun x86 og x86\_64 som guest arkitektur
- God performance
- Open source

## Sammenligning VMWare

- Kører kun på MacOS, Linux og Windows
- Understøtter kun x86 og x86\_64 som guest arkitektur
- God performance
- Enterprise features
- Closed source

## Sammenligning Parallels

- Kører kun på MacOS, Linux og Windows
- Understøtter kun x86 og x86\_64 som guest arkitektur
- Closed source

## Sammenligning Xen

- Kører ikke på et host OS men direkte på maskinen
- En dom0 guest
- Flere domU guests
- Kan både paravirtualisering og rigtig virtualisering (Med VT-x eller AMD-V)
- Open source

## Fremtiden for QEMU

- Ny kodegenerator
- Bedre performance
- Flere emulerede enheder (?)
- Brug af VT-x/AMD-V i KQEMU (?)



## Spørgsmål?

# Spørgsmål?

## Yderligere information

- QEMU hjemmesiden: <http://www.qemu.org/>
- Dette foredrag: <http://borderworlds.dk/slides/qemu/>