UNICORE 64bit

QEMU & Linux Kernel Upgrade

UC64A

胡越予 高煜 章嘉晨

QEMU

Background

- Initial Version
  - Makefile

```
@cd $(DIR_WORKING)/qemu;                    \
        git br unicore64 0b8db8f ;              \
        git co unicore64 ;                  \
        git am $(QEMU_PATCHES)/*
```

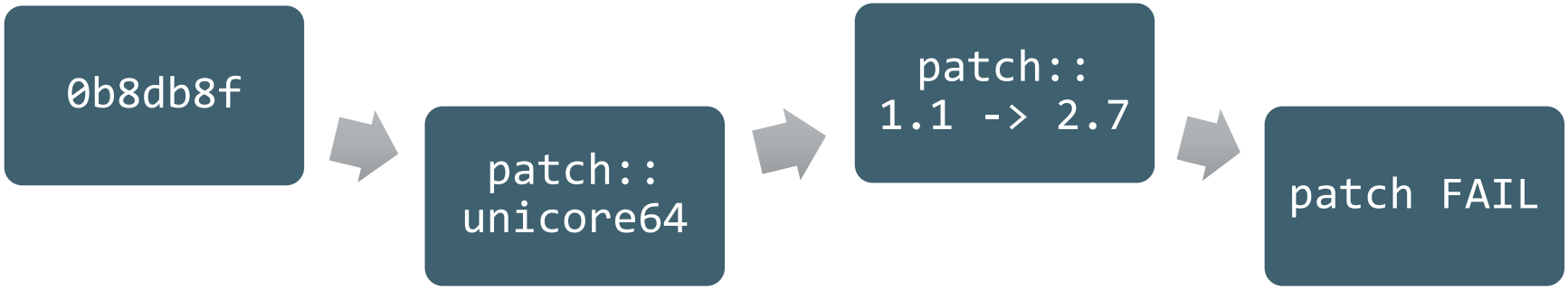
➜ qemu git:(unicore64) cat VERSION
1.1.50

Experiment :: Patches

Round 0

Result : Non-applied

Round 1



- Generate patches
  - > git format-patch 0b8db8f
  - About 20000+ patches
  - Remove old unicore32 patches

Round 1

```
Applying: linux-user: Fix SNDCTL_DSP_MAP{IN, OUT}BUF ioctl definitions
Applying: linux-user: Move target_to_host_errno_table[] setup out of ioctl loop
Applying: arm: Move some ARM devices into libhw
error: patch failed: hw/Makefile.objs:74
error: hw/Makefile.objs: patch does not apply
Patch failed at 0095 arm: Move some ARM devices into libhw
The copy of the patch that failed is found in: .git/rebase-apply/patch
When you have resolved this problem, run "git am --continue".
If you prefer to skip this patch, run "git am --skip" instead.
To restore the original branch and stop patching, run "git am --abort".
➜  qemu-1 git:(25a02c7)
```

Round 2

- Generate patches
- Directly apply to 0b8db8f
  - For verification

Round 2

```
Applying: qemu-ga: don't leak a file descriptor upon failed lockf
Applying: linux-user: do_msgrcv: don't leak host_mb upon TARGET_EFAULT failure
Applying: sheepdog: don't leak socket file descriptor upon connection failure
Applying: arm-semi: don't leak 1KB user string lock buffer upon TARGET_SYS_OPEN
Applying: softmmu-semi: fix lock_user* functions not to deref NULL upon OOM
Applying: virtio-blk: hide VIRTIO_BLK_F_CONFIG_WCE from old machine types
error: patch failed: hw/pc_piix.c:375
error: hw/pc_piix.c: patch does not apply
error: patch failed: hw/virtio-blk.c:533
error: hw/virtio-blk.c: patch does not apply
Patch failed at 0287 virtio-blk: hide VIRTIO_BLK_F_CONFIG_WCE from old machine types
The copy of the patch that failed is found in: .git/rebase-apply/patch
When you have resolved this problem, run "git am --continue".
If you prefer to skip this patch, run "git am --skip" instead.
To restore the original branch and stop patching, run "git am --abort".
➜  qemu-1 git:(5d6afc0)
```

patch 道路无法救中国

- 通过和助教交流：
  - `git format-patch` 会把两个 `revision` 之间所有的 `commit` 转为 `patch`. 但是因为 `git` 有 `merge` 的功能，如果在 `merge` 的时候产生冲突，`git` 会把冲突的 `commit` 提交到要合并的分支，然后再加上一个手动解决冲突合并提交，所以产生的一系列 `patch` 按顺序打不一定都能打上去。

Experiment :: Hands on

Round 3

- 基于2.7版本
- 移植原来0b8db8f版本的unicore64相关文件
- 在2.7版本，全局搜索unicore关键字
- 根据unicore32来对应在一些全局文件中修改
  - configure cpu.h …
- 根据32的文件变更历史来改64的老文件
- 根据报错来填补缺失的文件

主要修改

```
---
arch_init.c                                |   2 +
config.h                                   | 404 +++
configure                                  |   2 +
default-configs/unicore64-linux-user.mak   |   2 +
default-configs/unicore64-softmmu.mak      |   5 +
fpu/softfloat.h                            | 754 +++++
hw/gpio/puv4_io_ctl.c                      |  79 +
hw/intc/puv4_intc.c                        | 140 +
hw/puv4.h                                  |  22 +
hw/puv4_csr.c                              |  93 +
hw/puv4_intc.c                             | 140 +
hw/puv4_io_ctl.c                           |  79 +
hw/puv4_ost.c                              | 142 +
hw/timer/puv4_ost.c                        | 142 +
hw/unicore64/Makefile.objs                 |   8 +
hw/unicore64/cp0_intc.c                    | 105 +
hw/unicore64/cp0_itm.c                     |  56 +
hw/unicore64/puv4.c                        | 116 +
```

主要修改

```
include/elf.h                                |    2 +-
include/hw/unicore64/puv4.h                  |   22 +
include/sysemu/arch_init.h                   |    1 +
linux-user/elfload.c                         |   28 +
linux-user/main.c                            |   17 +
linux-user/syscall_defs.h                    |    8 +-
linux-user/unicore64/syscall_nr.h            |  311 ++
linux-user/unicore64/target_cpu.h            |  238 ++
linux-user/unicore64/target_signal.h         |   22 +
linux-user/unicore64/target_structs.h        |   52 +
linux-user/unicore64/target_syscall.h        |   52 +
linux-user/unicore64/termbits.h              |    2 +
qemu-char.c                                  | 4678 ------------------------------
```

主要修改

```
---
 hw/gpio/puv4_io_ctl.c                 |  79 ----------------
 hw/intc/puv4_intc.c                   | 140 ------------------------------
 hw/puv4.c                             | 116 ++++++++++++++++++++++++
 hw/puv4.h                             |  22 -----
 hw/timer/puv4_ost.c                   | 142 ------------------------------
 hw/unicore64/puv4.c                   | 116 ------------------------
 include/qapi/qmp/qobject.h            |   4 +-
 linux-user/syscall.c                  |   1 +
 linux-user/unicore64/target_signal.h  |   3 +-
 linux-user/unicore64/target_syscall.h |   9 +-
 qemu-log.h                            | 159 ++++++++++++++++++++++++++++++++++
 target-unicore64/translate.c          |   2 +-
 12 files changed, 288 insertions(+), 505 deletions(-)
```

当前结果

```
                                    ^
In file included from /home/huzi/work2/UniCore64/working/qemu/include/qom/object.h:17:0,
                 from /home/huzi/work2/UniCore64/working/qemu/include/ui/console.h:5,
                 from /home/huzi/work2/UniCore64/working/qemu/hw/unicore64/../puv4.c:1:
/home/huzi/work2/UniCore64/working/qemu/qapi-types.h:42:5: error: unknown type name ‘QObject’
     QObject *value;
     ^
/home/huzi/work2/UniCore64/working/qemu/qapi-types.h:51:5: error: unknown type name ‘bool’
     bool value;
     ^
/home/huzi/work2/UniCore64/working/qemu/qapi-types.h:1941:5: error: unknown type name ‘bool’
     bool has_device;
     ^
/home/huzi/work2/UniCore64/working/qemu/qapi-types.h:1965:5: error: unknown type name ‘bool’
     bool has_sig;
     ^
/home/huzi/work2/UniCore64/working/qemu/qapi-types.h:1967:5: error: unknown type name ‘bool’
     bool has_rev;
     ^
/home/huzi/work2/UniCore64/working/qemu/qapi-types.h:1969:5: error: unknown type name ‘bool’
     bool has_oem_id;
     ^
```

```
In file included from /home/huzi/work2/UniCore64/working/qemu/include/qapi/qmp/qobject.h:35:0,
                 from /home/huzi/work2/UniCore64/working/qemu/include/qapi/qmp/qdict.h:16,
                 from /home/huzi/work2/UniCore64/working/qemu/include/qemu/option.h:30,
                 from /home/huzi/work2/UniCore64/working/qemu/include/hw/qdev-core.h:5,
                 from /home/huzi/work2/UniCore64/working/qemu/include/qom/cpu.h:23,
                 from /home/huzi/work2/UniCore64/working/qemu/target-unicore64/cpu-qom.h:14,
                 from /home/huzi/work2/UniCore64/working/qemu/target-unicore64/cpu.c:7:
/home/huzi/work2/UniCore64/working/qemu/qapi-types.h:42:5: error: unknown type name ‘QObject’
     QObject *value;
     ^
/home/huzi/work2/UniCore64/working/qemu/qapi-types.h:51:5: error: unknown type name ‘bool’
     bool value;
     ^
/home/huzi/work2/UniCore64/working/qemu/qapi-types.h:60:5: error: unknown type name ‘int16_t’
     int16_t value;
     ^
/home/huzi/work2/UniCore64/working/qemu/qapi-types.h:69:5: error: unknown type name ‘int32_t’
     int32_t value;
     ^
/home/huzi/work2/UniCore64/working/qemu/qapi-types.h:78:5: error: unknown type name ‘int64_t’
     int64_t value;
     ^
/home/huzi/work2/UniCore64/working/qemu/qapi-types.h:87:5: error: unknown type name ‘int8_t’
     int8_t value;
     ^
/home/huzi/work2/UniCore64/working/qemu/qapi-types.h:96:5: error: unknown type name ‘int64_t’
     int64_t value;
     ^
```

Linux Kernel

linux4.4内核的更新

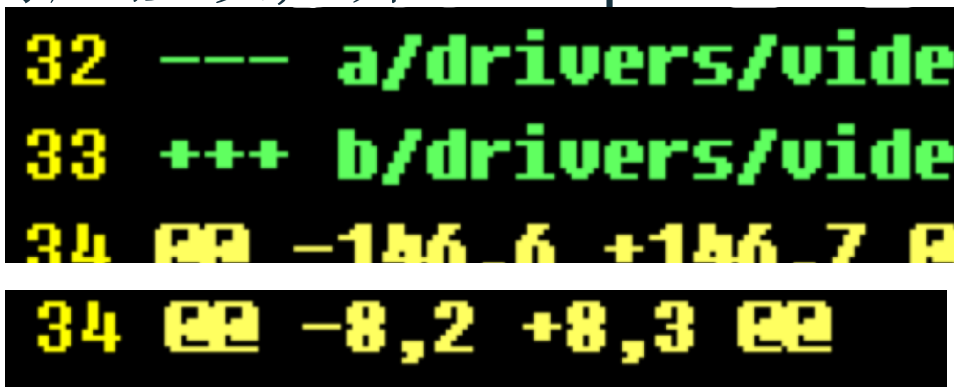
- 首先从获取了linux4.4版本的内核，在之前的工作中有让linux3.7支持unicore64的patch包，尝试对4.4版本直接应用该patch。部分patch成功，部分patch失败。对失败的patch逐个处理。

0106-UniCore64-Add-unicore64-kernel.tmpl-Modify-Makefile.patch

- 修改了Documentation里的Makefile，在列表中加入unicore64-kernel.xml。对应linux4.4中该文件作对应修改即可。

0591-de2-architecture.patch 0602-UniCore64-Rename-unifb2-to-fb-puv4.patch

- 0591-patch对/drivers/video/Makefile进行修改，在146行加入了一行，但4.4中既找不到这段的上下文，也没有那么多行，所以在该文件的最后加入该行。
- 但之后602-patch对这一行进行修改，2变为4，于是删除602-patch对应修改，并591-patch中这行改为最终结果。



0626-UniCore64-create-4M-noncached-region-for-swiotlb.patch
0630-UniCore64-Warning-fix-for-dma.patch
0632-UniCore64-Use-new-noncached-region-in-dma.patch
0635-UniCore64-Force-to-use-swiotlb.patch

- 这若干个patch都有对lib/swiotlb.c的修改，由于4.4里该文件不同，因此全部失败了，下面是对这些修改的整合。

0626-UniCore64-create-4M-noncached-region-for-swiotlb.patch
0630-UniCore64-Warning-fix-for-dma.patch
0632-UniCore64-Use-new-noncached-region-in-dma.patch
0635-UniCore64-Force-to-use-swiotlb.patch

- 1）首先是0626修改了这个变量的初始化。
- `io_tlb_overflow_buffer = UC64_VM_NONCACHED_START + SZ_4M - PAGE_ALIGN(io_tlb_overflow);`
- 在0630中增加了(void*)前缀，0632中最后将该行修改为
- `io_tlb_overflow_buffer = (void *)UC64_VM_DMAOVERFLOW_START;`
- 于是在对应位置加入这部分初始化。

0626-UniCore64-create-4M-noncached-region-for-swiotlb.patch
0630-UniCore64-Warning-fix-for-dma.patch
0632-UniCore64-Use-new-noncached-region-in-dma.patch
0635-UniCore64-Force-to-use-swiotlb.patch

- 2）0626对这个变量的初始化
- `io_tlb_start = UC64_VM_NONCACHED_START;`
- 本来也只要在对应位置修改，0630里对该行增加了(char*)前缀，0636中最后将该行改为
- `io_tlb_start = (char *)UC64_VM_DMA_START;`

- 于是在对应位置加入这部分初始化。

0626-UniCore64-create-4M-noncached-region-for-swiotlb.patch
0630-UniCore64-Warning-fix-for-dma.patch
0632-UniCore64-Use-new-noncached-region-in-dma.patch
0635-UniCore64-Force-to-use-swiotlb.patch

- 3）
- 0626中修改该行
- swiotlb_init_with_default_size(64 * (1<<20), verbose); /* default to 64MB */
- 为
- swiotlb_init_with_default_size(SZ_4M - io_tlb_overflow, verbose);
- 但0632中又将该行改了回来，因此删除这两部分。

0626-UniCore64-create-4M-noncached-region-for-swiotlb.patch
0630-UniCore64-Warning-fix-for-dma.patch
0632-UniCore64-Use-new-noncached-region-in-dma.patch
0635-UniCore64-Force-to-use-swiotlb.patch

- 4)0626减少了一些中free_bootmem_late的调用，但在linux4.4已经没有该函数的定义，因此没有对应这部分的修改。

没有应用的patch

- 0601-UniCore64-adjust-video-Kconfig-for-de2.patch
- 0603-UniCore64-make-de2-default-y.patch
- 这两个patch修改a/drivers/video/Kconfig，但没有看懂里面的内容应该如何添加，所以没有应用这些patch。
- 0636-Fix-perl-error.patch
- 同样，找不到对应位置，没有应用该patch。

其它问题

- 修改完所有patch，使所有patch都能应用成功以后开始编译内核。
- 第一个错误是提示preempt.h不存在，搜索以后发现它在以下位置
- ./linux/include/linux/preempt.h
- ./linux/include/asm-generic/preempt.h
- ./linux/arch/x86/include/asm/preempt.h
- 其中include/linux/preempt.h就是编译出错的库，因此需要的库要么是asm-generic中的，要么是x86中的 。我们选择了asm-generic中的库，然后发现还有其它库提示错误，因此我们将asm-generic中的所有库都复制了。

其它问题

- 之后继续编译发现了
- include/asm-generic/atomic-long.h: In function 'atomic_long_read_acquire':
- include/asm-generic/atomic-long.h:45: error: implicit declaration of function 'smp_load_acquire'
- include/asm-generic/atomic-long.h: In function 'atomic_long_set_release':
- include/asm-generic/atomic-long.h:57: error: implicit declaration of function 'smp_store_release'
- 这些错误，问了老师以后知道这些定义在barrier.h，于是仿照x86体系结构修改了barrier.h，之后还产生了一些缺少定义的错误，发现都在barrier.h中定义，于是仿照x86继续修改。

其他问题

- 在这之后还发生了一系列其他问题有非常多的error，我们觉得可能之前的一些步骤出错或者需要unicore64在linux4.4的一些基础库的支持才能完成。

Q&A

Thanks

胡越予 1400012817
高煜 1400012705
章嘉晨 1300012792