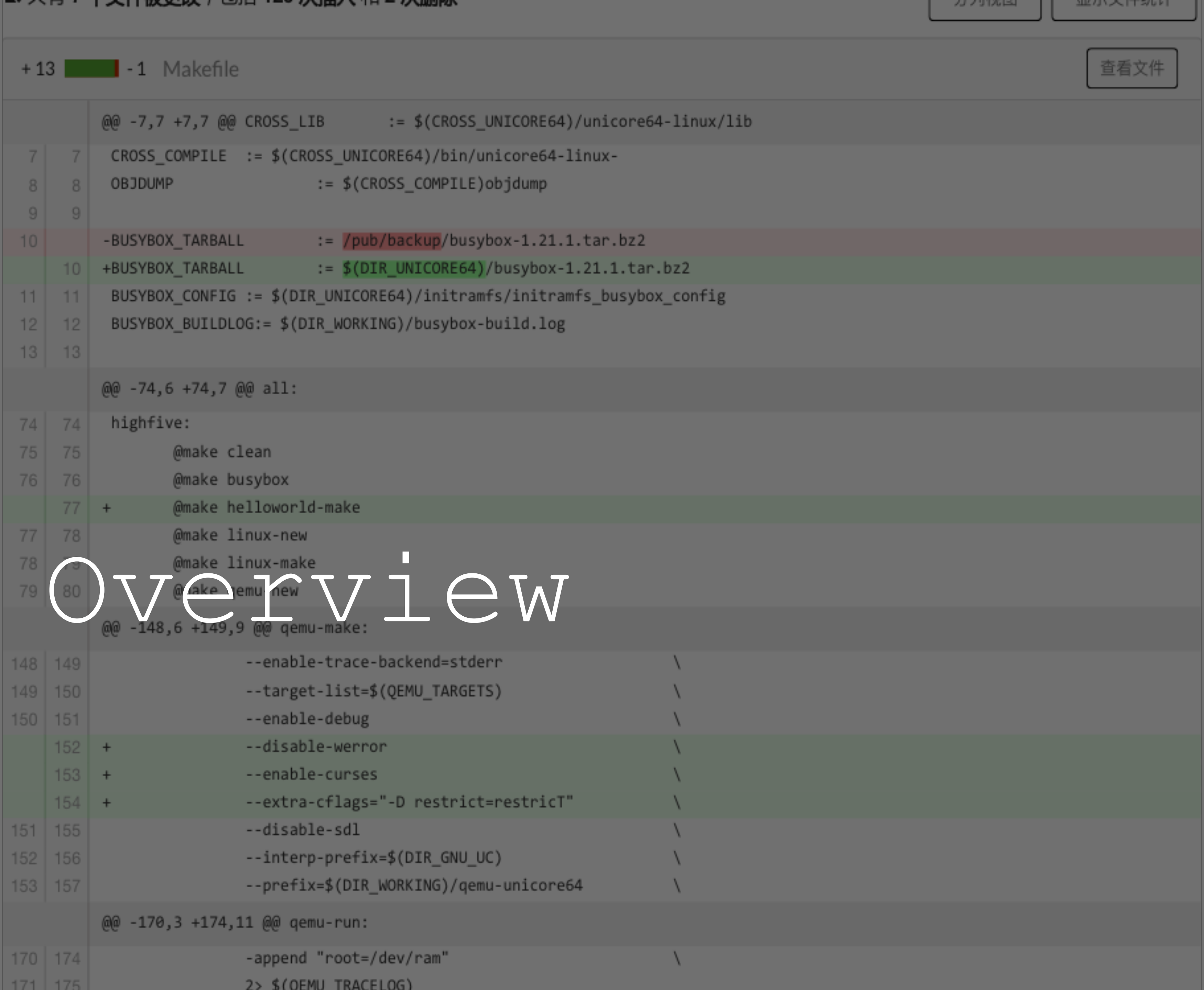
UNICORE 64bit

QEMU Development

UC64A

胡越予　高煜　章嘉晨

Overview



共有 1 个文件被更改，包括 13 次插入和 1 次删除

+13 -1 Makefile

```
@@ -7,7 +7,7 @@ CROSS_LIB       := $(CROSS_UNICORE64)/unicore64-linux/lib
 CROSS_COMPILE  := $(CROSS_UNICORE64)/bin/unicore64-linux-
 OBJDUMP                := $(CROSS_COMPILE)objdump

-BUSYBOX_TARBALL        := /pub/backup/busybox-1.21.1.tar.bz2
+BUSYBOX_TARBALL        := $(DIR_UNICORE64)/busybox-1.21.1.tar.bz2
 BUSYBOX_CONFIG := $(DIR_UNICORE64)/initramfs/initramfs_busybox_config
 BUSYBOX_BUILDLOG:= $(DIR_WORKING)/busybox-build.log

@@ -74,6 +74,7 @@ all:
 highfive:
        @make clean
        @make busybox
+       @make helloworld-make
        @make linux-new
        @make linux-make
        @make qemu-new
@@ -148,6 +149,9 @@ qemu-make:
                --enable-trace-backend=stderr                   \
                --target-list=$(QEMU_TARGETS)                   \
                --enable-debug                                  \
+               --disable-werror                                \
+               --enable-curses                                 \
+               --extra-cflags="-D restrict=restricT"           \
                --disable-sdl                                   \
                --interp-prefix=$(DIR_GNU_UC)                   \
                --prefix=$(DIR_WORKING)/qemu-unicore64          \
@@ -170,3 +174,11 @@ qemu-run:
                -append "root=/dev/ram"                         \
                2> $(QEMU_TRACELOG)
```

Bug Fixing

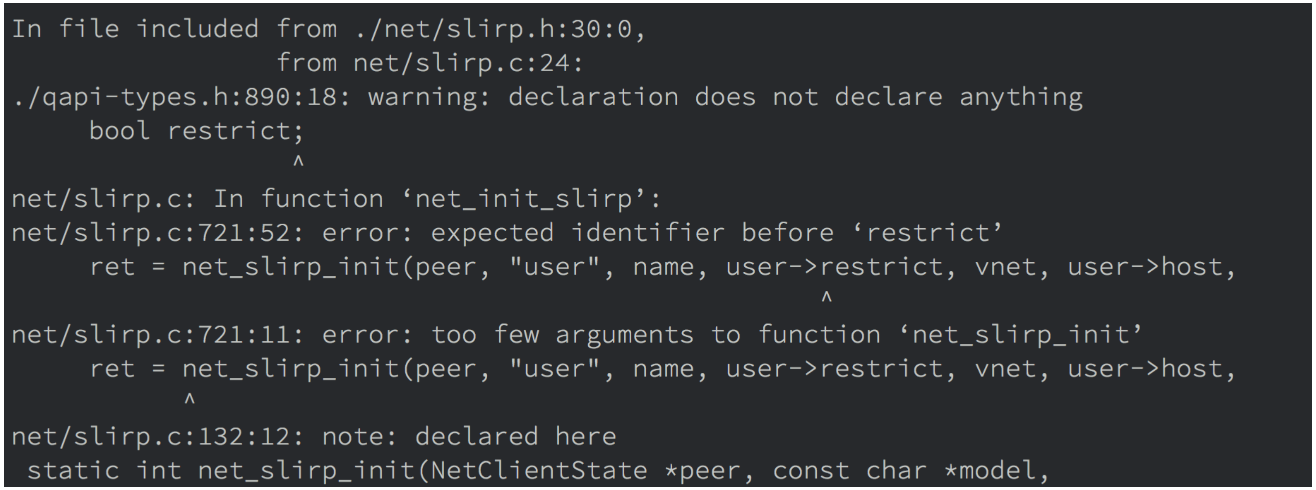
- Qemu
  - Fix error when compiling with gcc-5
  - Fix error in linking
  - Fix minor code error
- Linux
  - Patch perl script error

Modification

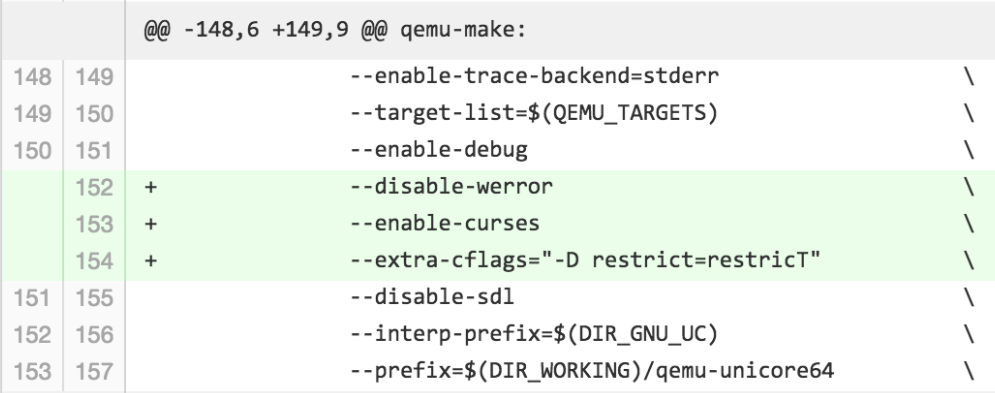
- Makefile
  - Add helloworld target
  - Modify Environment Setting
- Self-contained Busybox

Detail

Qemu Compile Error



```
In file included from ./net/slirp.h:30:0,
                 from net/slirp.c:24:
./qapi-types.h:890:18: warning: declaration does not declare anything
     bool restrict;
                  ^
net/slirp.c: In function ‘net_init_slirp’:
net/slirp.c:721:52: error: expected identifier before ‘restrict’
     ret = net_slirp_init(peer, "user", name, user->restrict, vnet, user->host,
                                                    ^
net/slirp.c:721:11: error: too few arguments to function ‘net_slirp_init’
     ret = net_slirp_init(peer, "user", name, user->restrict, vnet, user->host,
           ^
net/slirp.c:132:12: note: declared here
 static int net_slirp_init(NetClientState *peer, const char *model,
```

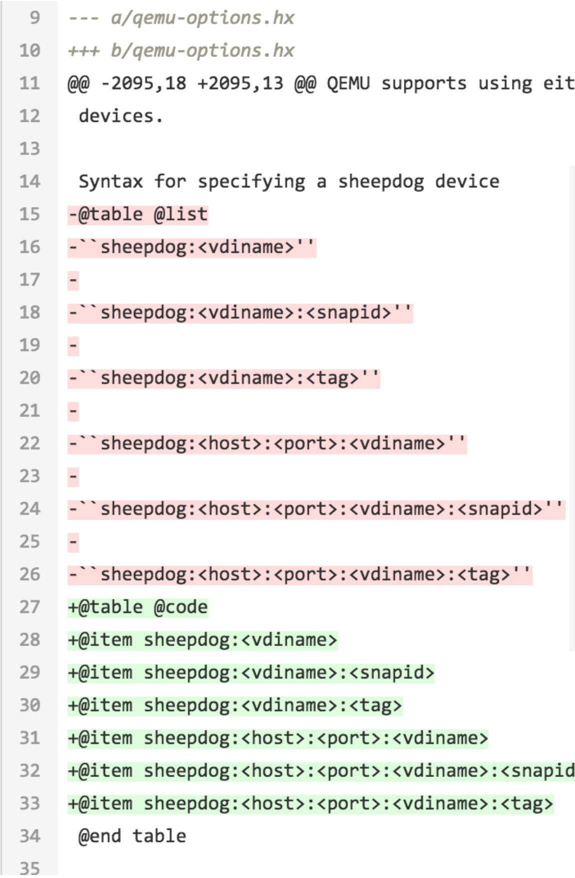


```
@@ -148,6 +149,9 @@ qemu-make:
              --enable-trace-backend=stderr          \
              --target-list=$(QEMU_TARGETS)          \
              --enable-debug                         \
+             --disable-werror                       \
+             --enable-curses                        \
+             --extra-cflags="-D restrict=restricT"  \
              --disable-sdl                          \
              --interp-prefix=$(DIR_GNU_UC)          \
              --prefix=$(DIR_WORKING)/qemu-unicore64 \
```

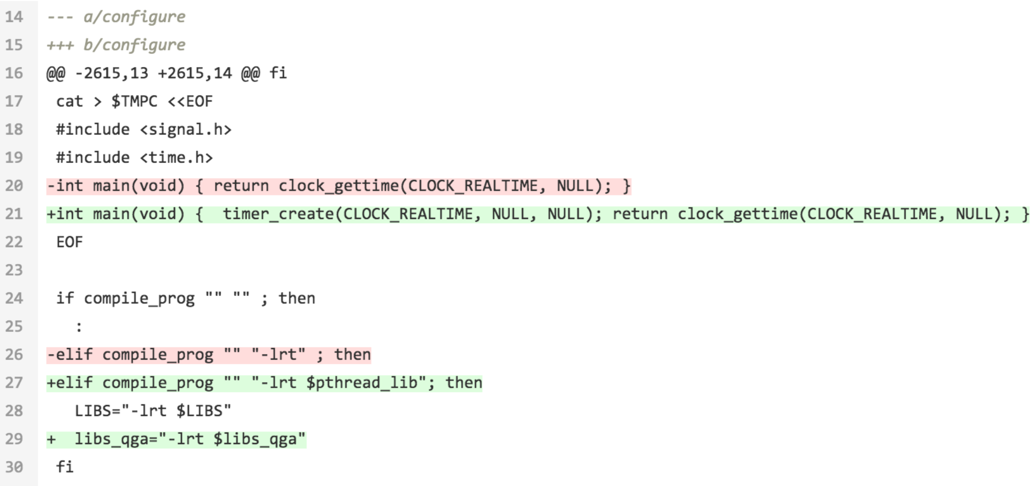
！：

gcc-5 中 restrict 为保留字

Qemu Other Error

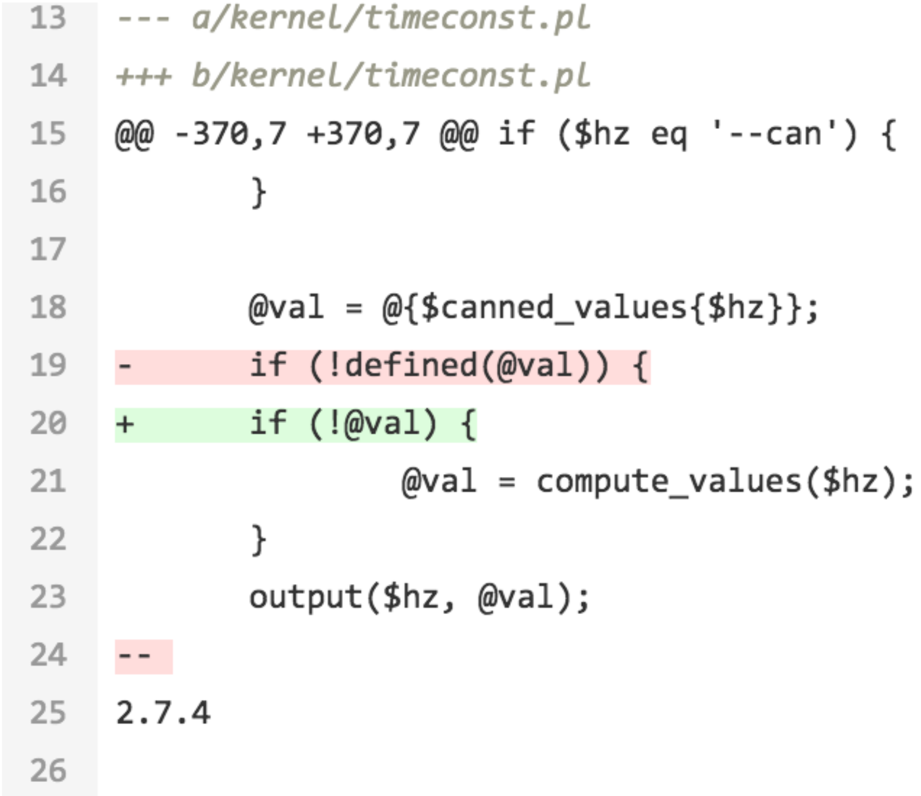


```
--- a/qemu-options.hx
+++ b/qemu-options.hx
@@ -2095,18 +2095,13 @@ QEMU supports using either local sheepdog devices or remote networked
 devices.

 Syntax for specifying a sheepdog device
-@table @list
-``sheepdog:<vdiname>''
-
-``sheepdog:<vdiname>:<snapid>''
-
-``sheepdog:<vdiname>:<tag>''
-
-``sheepdog:<host>:<port>:<vdiname>''
-
-``sheepdog:<host>:<port>:<vdiname>:<snapid>''
-
-``sheepdog:<host>:<port>:<vdiname>:<tag>''
+@table @code
+@item sheepdog:<vdiname>
+@item sheepdog:<vdiname>:<snapid>
+@item sheepdog:<vdiname>:<tag>
+@item sheepdog:<host>:<port>:<vdiname>
+@item sheepdog:<host>:<port>:<vdiname>:<snapid>
+@item sheepdog:<host>:<port>:<vdiname>:<tag>
 @end table

```



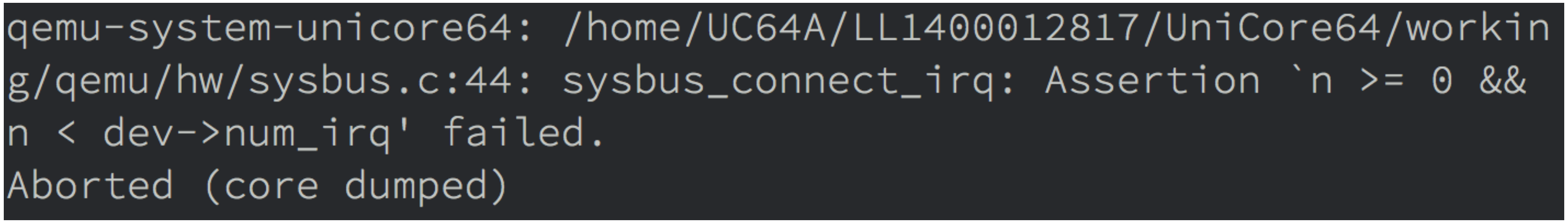
```
--- a/configure
+++ b/configure
@@ -2615,13 +2615,14 @@ fi
 cat > $TMPC <<EOF
 #include <signal.h>
 #include <time.h>
-int main(void) { return clock_gettime(CLOCK_REALTIME, NULL); }
+int main(void) {  timer_create(CLOCK_REALTIME, NULL, NULL); return clock_gettime(CLOCK_REALTIME, NULL); }
 EOF

 if compile_prog "" "" ; then
   :
-elif compile_prog "" "-lrt" ; then
+elif compile_prog "" "-lrt $pthread_lib"; then
   LIBS="-lrt $LIBS"
+  libs_qga="-lrt $libs_qga"
 fi
```

Linux Perl Script Error

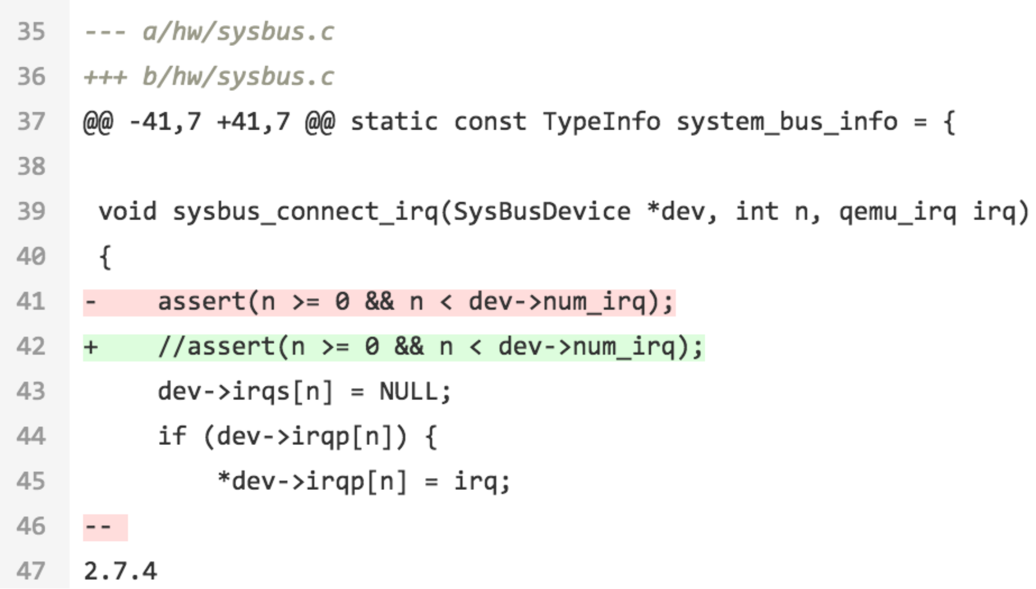


```
--- a/kernel/timeconst.pl
+++ b/kernel/timeconst.pl
@@ -370,7 +370,7 @@ if ($hz eq '--can') {
       }

       @val = @{$canned_values{$hz}};
-      if (!defined(@val)) {
+      if (!@val) {
               @val = compute_values($hz);
       }
       output($hz, @val);
--
2.7.4

```

make qemu-run



```
qemu-system-unicore64: /home/UC64A/LL1400012817/UniCore64/workin
g/qemu/hw/sysbus.c:44: sysbus_connect_irq: Assertion `n >= 0 &&
n < dev->num_irq' failed.
Aborted (core dumped)
```



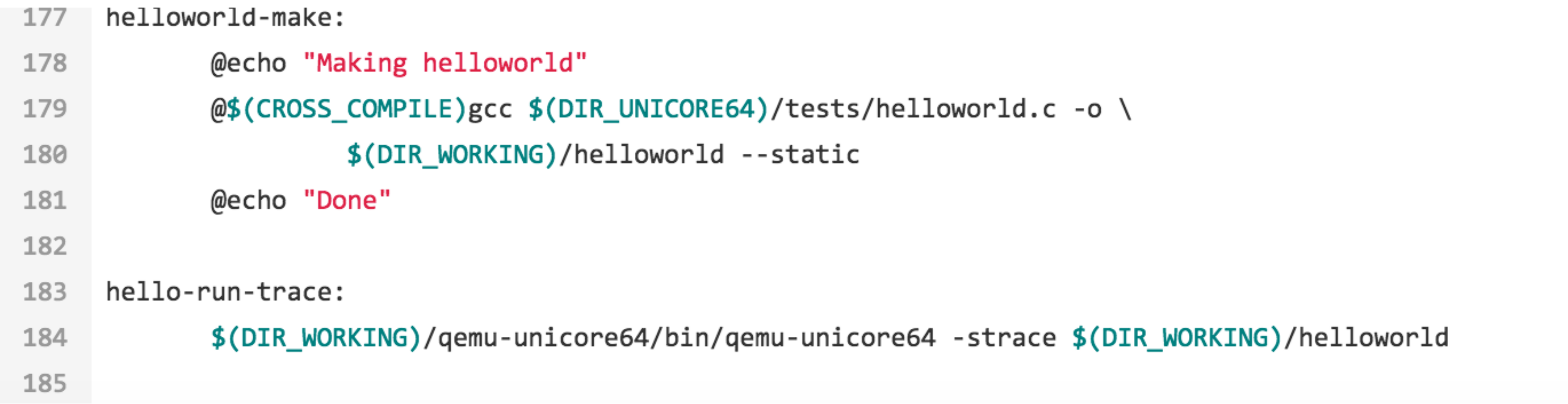
```
--- a/hw/sysbus.c
+++ b/hw/sysbus.c
@@ -41,7 +41,7 @@ static const TypeInfo system_bus_info = {

 void sysbus_connect_irq(SysBusDevice *dev, int n, qemu_irq irq)
 {
-    assert(n >= 0 && n < dev->num_irq);
+    //assert(n >= 0 && n < dev->num_irq);
     dev->irqs[n] = NULL;
     if (dev->irqp[n]) {
         *dev->irqp[n] = irq;
--
2.7.4
```

？：

考虑宿主机运行环境因素

Running

User-mode

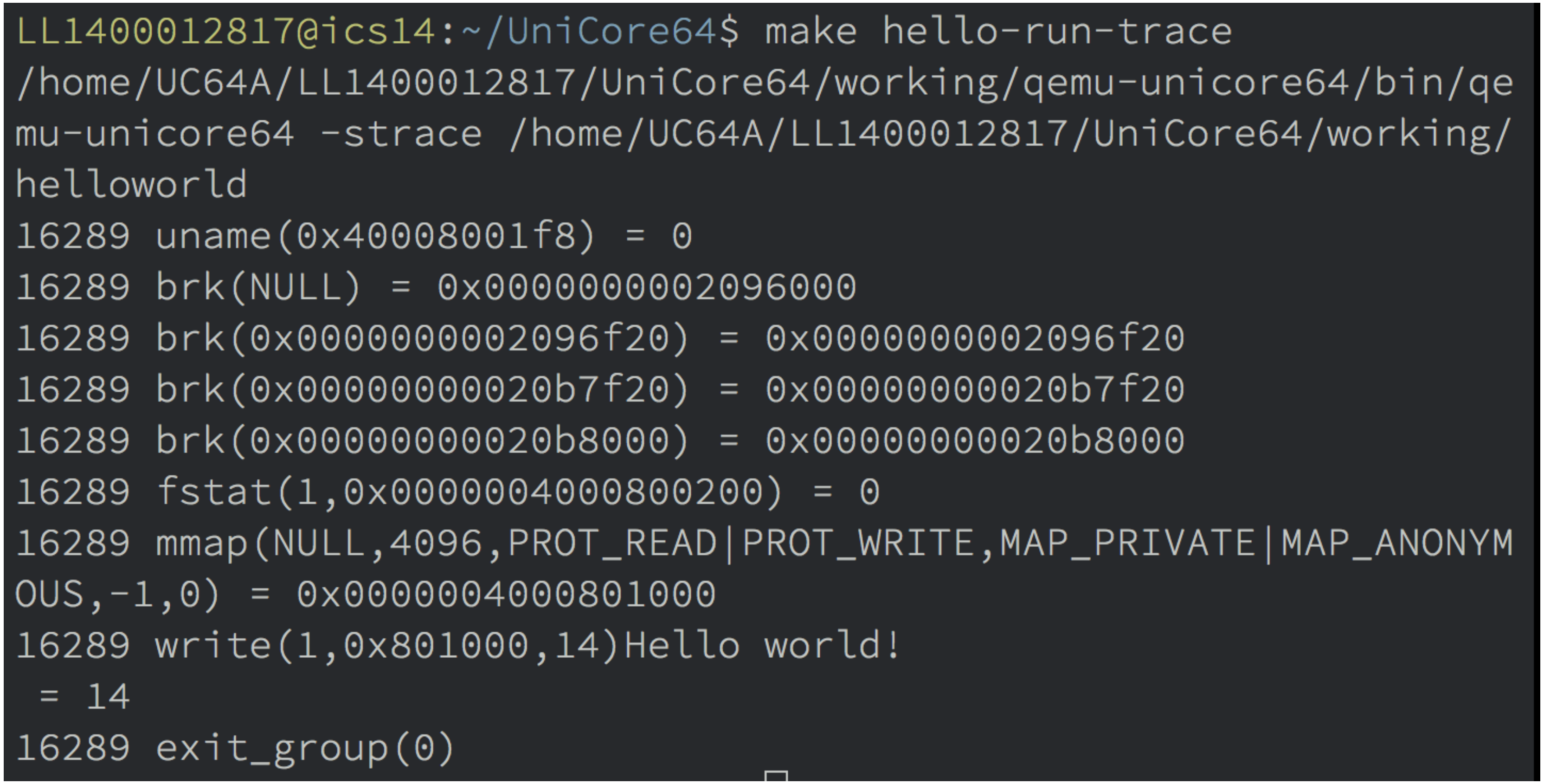


```
helloworld-make:
	@echo "Making helloworld"
	@$(CROSS_COMPILE)gcc $(DIR_UNICORE64)/tests/helloworld.c -o \
		$(DIR_WORKING)/helloworld --static
	@echo "Done"

hello-run-trace:
	$(DIR_WORKING)/qemu-unicore64/bin/qemu-unicore64 -strace $(DIR_WORKING)/helloworld

```

! :

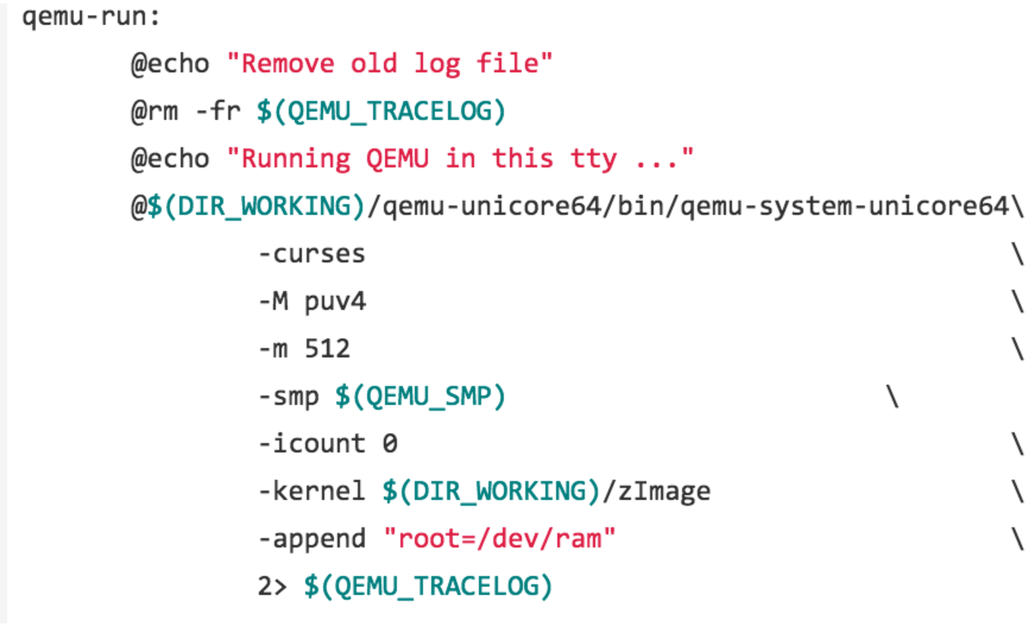
qemu将系统调用转交到宿主机kernel执行

User-mode



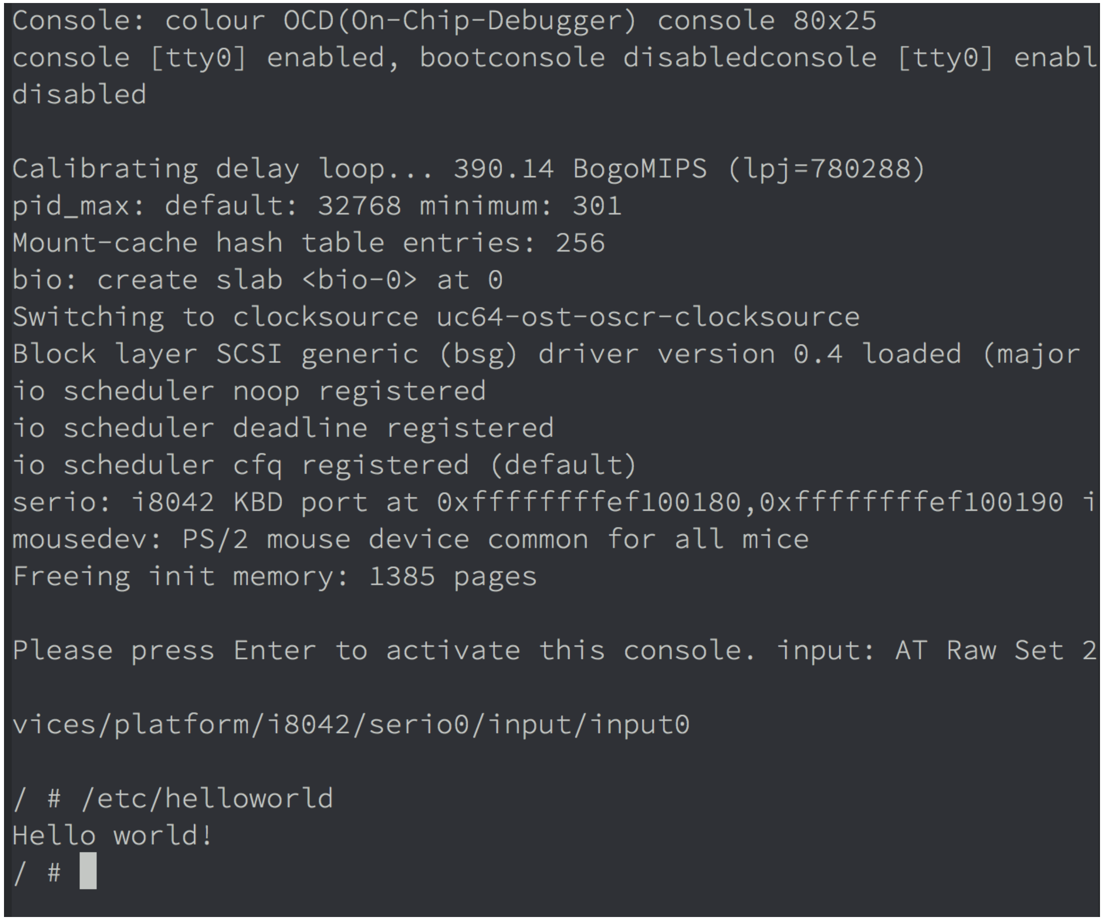
```
LL1400012817@ics14:~/UniCore64$ make hello-run-trace
/home/UC64A/LL1400012817/UniCore64/working/qemu-unicore64/bin/qe
mu-unicore64 -strace /home/UC64A/LL1400012817/UniCore64/working/
helloworld
16289 uname(0x40008001f8) = 0
16289 brk(NULL) = 0x0000000002096000
16289 brk(0x0000000002096f20) = 0x0000000002096f20
16289 brk(0x00000000020b7f20) = 0x00000000020b7f20
16289 brk(0x00000000020b8000) = 0x00000000020b8000
16289 fstat(1,0x0000004000800200) = 0
16289 mmap(NULL,4096,PROT_READ|PROT_WRITE,MAP_PRIVATE|MAP_ANONYM
OUS,-1,0) = 0x0000004000801000
16289 write(1,0x801000,14)Hello world!
 = 14
16289 exit_group(0)
```

System-mode



```
qemu-run:
       @echo "Remove old log file"
       @rm -fr $(QEMU_TRACELOG)
       @echo "Running QEMU in this tty ..."
       @$(DIR_WORKING)/qemu-unicore64/bin/qemu-system-unicore64\
               -curses                                         \
               -M puv4                                         \
               -m 512                                          \
               -smp $(QEMU_SMP)                        \
               -icount 0                                       \
               -kernel $(DIR_WORKING)/zImage                   \
               -append "root=/dev/ram"                         \
               2> $(QEMU_TRACELOG)
```

System-mode

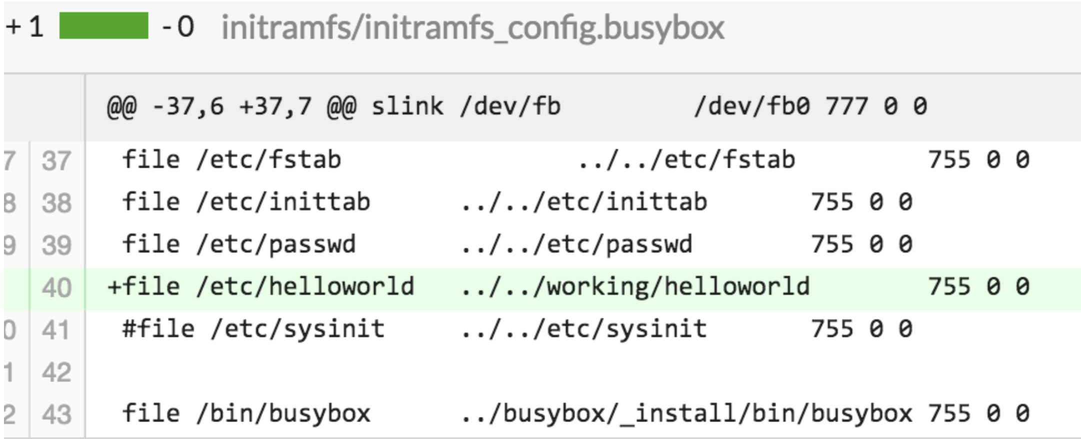


```
Console: colour OCD(On-Chip-Debugger) console 80x25
console [tty0] enabled, bootconsole disabledconsole [tty0] enabl
disabled

Calibrating delay loop... 390.14 BogoMIPS (lpj=780288)
pid_max: default: 32768 minimum: 301
Mount-cache hash table entries: 256
bio: create slab <bio-0> at 0
Switching to clocksource uc64-ost-oscr-clocksource
Block layer SCSI generic (bsg) driver version 0.4 loaded (major
io scheduler noop registered
io scheduler deadline registered
io scheduler cfq registered (default)
serio: i8042 KBD port at 0xffffffffef100180,0xffffffffef100190 i
mousedev: PS/2 mouse device common for all mice
Freeing init memory: 1385 pages

Please press Enter to activate this console. input: AT Raw Set 2

vices/platform/i8042/serio0/input/input0

/ # /etc/helloworld
Hello world!
/ #
```

！：

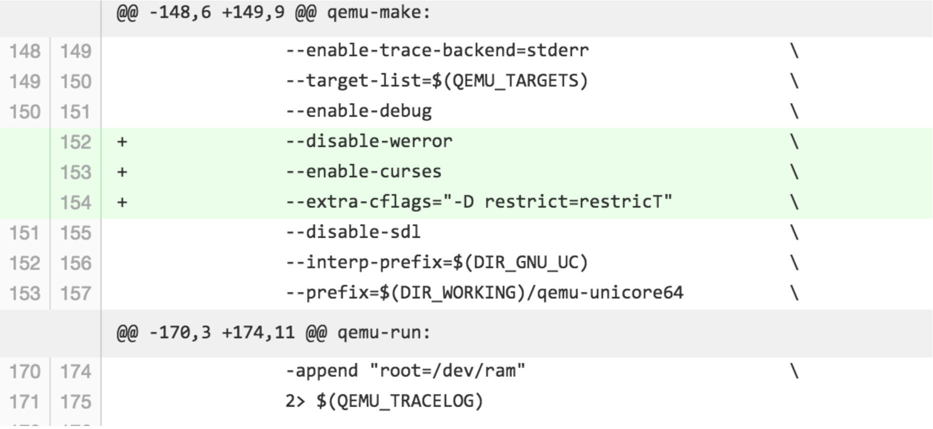
必须使用curses
来让qemu占有终端
执行halt命令后
用ESC+2来退出

System-mode



+1 -0 initramfs/initramfs_config.busybox

```
@@ -37,6 +37,7 @@ slink /dev/fb         /dev/fb0 777 0 0
 file /etc/fstab              ../../etc/fstab          755 0 0
 file /etc/inittab       ../../etc/inittab       755 0 0
 file /etc/passwd        ../../etc/passwd        755 0 0
+file /etc/helloworld    ../../working/helloworld         755 0 0
 #file /etc/sysinit      ../../etc/sysinit       755 0 0

 file /bin/busybox       ../busybox/_install/bin/busybox 755 0 0
```



```
@@ -148,6 +149,9 @@ qemu-make:
                  --enable-trace-backend=stderr                    \
                  --target-list=$(QEMU_TARGETS)                    \
                  --enable-debug                                   \
+                 --disable-werror                                 \
+                 --enable-curses                                  \
+                 --extra-cflags="-D restrict=restricT"            \
                  --disable-sdl                                    \
                  --interp-prefix=$(DIR_GNU_UC)                    \
                  --prefix=$(DIR_WORKING)/qemu-unicore64           \
@@ -170,3 +174,11 @@ qemu-run:
                  -append "root=/dev/ram"                          \
                  2> $(QEMU_TRACELOG)
```

！ ：
initramfs_config.busybox
会在编译内核的时候被引用
指导文件加入到ramfs中

如果需要strace，我们认为需要将strace编译到busybox中

System-mode

- Qemu加载kernel zImage
- Kernel完成init，执行第一个用户进程
- 第一个用户进程应该是busybox sh
- 此时可以执行各种命令
- 执行halt命令关机
- Qemu释放终端

Q&A

Thanks

胡越予	1400012817
高煜	1400012705
章嘉晨	1300012792