

# Lab 0: GDB & QEMU 调试 64 位 RISC-V LINUX

## 1 实验目的

- 使用交叉编译工具, 完成Linux内核代码编译
- 使用QEMU运行内核
- 熟悉GDB和QEMU联合调试

## 2 实验环境

Ubuntu 22.04.2 LTS Windows Subsystem for Linux 2

## 3 实验基础知识介绍

### 3.1 Linux 使用基础

在 Linux 环境下, 人们通常使用命令行接口来完成与计算机的交互。终端 (Terminal) 是用于处理该过程的一个应用程序, 通过终端你可以运行各种程序以及在自己的计算机上处理文件。在类 Unix 的操作系统上, 终端可以为你完成一切你所需要的操作。

### 3.2 QEMU 使用基础

#### 什么是QEMU

QEMU 是一个功能强大的模拟器, 可以在 x86 平台上执行不同架构下的程序。我们实验中采用 QEMU 来完成 RISC-V 架构的程序的模拟。

#### 如何使用 QEMU (常见参数介绍)

以以下命令为例, 我们简单介绍 QEMU 的参数所代表的含义

```
$ qemu-system-riscv64 \  
-nographic \  
-machine virt \  
-kernel path/to/linux/arch/riscv/boot/Image \  
-device virtio-blk-device,drive=hd0 \  
-append "root=/dev/vda ro console=ttys0" \  
-bios default \  
-drive file=rootfs.img,format=raw,id=hd0 \  
-S -s
```

- `-nographic`: 不使用图形窗口, 使用命令行
- `-machine`: 指定要 emulate 的机器, 可以通过命令 `qemu-system-riscv64 -machine help` 查看可选择的机器选项
- `-kernel`: 指定内核 image
- `-append cmdline`: 使用cmdline作为内核的命令行
- `-device`: 指定要模拟的设备, 可以通过命令 `qemu-system-riscv64 -device help` 查看可选择的设备, 通过命令 `qemu-system-riscv64 -device <具体的设备>,help` 查看某个设备的命令选项

- `-drive, file=<file_name>`: 使用 `file_name` 作为文件系统
- `-S`: 启动时暂停CPU执行
- `-s: -gdb tcp::1234` 的简写
- `-bios default`: 使用默认的 OpenSBI firmware 作为 bootloader

更多参数信息可以参考[这里](#)

## 3.3 GDB 使用基础

### 什么是 GDB

GNU 调试器（英语：GNU Debugger，缩写：gdb）是一个由 GNU 开源组织发布的、UNIX/LINUX 操作系统下的、基于命令行的、功能强大的程序调试工具。借助调试器，我们能够查看另一个程序在执行时实际在做什么（比如访问哪些内存、寄存器），在其他程序崩溃的时候可以比较快速地了解导致程序崩溃的原因。

被调试的程序可以和 GDB 运行在同一台机器上，并由 GDB 控制（本地调试 native debug）。也可以只和 `gdb-server` 运行在同一台机器上，由连接着 `gdb-server` 的 GDB 进行控制（远程调试 remote debug）。

GDB 的功能十分强大，我们经常在调试中用到的有：

- 启动程序，并指定可能影响其行为的所有内容
- 使程序在指定条件下停止
- 检查程序停止时发生了什么
- 更改程序中的内容，以便纠正一个bug的影响

### GDB 基本命令介绍

- `(gdb) layout asm`: 显示汇编代码
- `(gdb) start`: 单步执行，运行程序，停在第一执行语句
- `(gdb) continue`: 从断点后继续执行，简写 `c`
- `(gdb) next`: 单步调试（逐过程，函数直接执行），简写 `n`
- `(gdb) step instruction`: 执行单条指令，简写 `si`
- `(gdb) run`: 重新开始运行文件（`run-text`: 加载文本文件，`run-bin`: 加载二进制文件），简写 `r`
- `(gdb) backtrace`: 查看函数的调用的栈帧和层级关系，简写 `bt`
- `(gdb) break` 设置断点，简写 `b`
  - 断在 `foo` 函数: `b foo`
  - 断在某地址: `b * 0x80200000`
- `(gdb) finish`: 结束当前函数，返回到函数调用点
- `(gdb) frame`: 切换函数的栈帧，简写 `f`
- `(gdb) print`: 打印值及地址，简写 `p`
- `(gdb) info`: 查看函数内部局部变量的数值，简写 `i`
  - 查看寄存器 `ra` 的值: `i r ra`
- `(gdb) display`: 追踪查看具体变量值
- `(gdb) x/4x <addr>`: 以 16 进制打印 `<addr>` 处开始的 16 Bytes 内容

更多命令可以参考[100个gdb小技巧](#)

## 3.4 Linux 内核编译基础

### 交叉编译

交叉编译指的是在一个平台上编译可以在另一个架构运行的程序。例如在 x86 机器上编译可以在 RISC-V 架构运行的程序，交叉编译需要交叉编译工具链的支持，在我们的实验中所用的交叉编译工具链就是 `riscv-gnu-toolchain`。

### 内核配置

内核配置是用于配置是否启用内核的各项特性，内核会提供一个名为 `defconfig` (即default configuration) 的默认配置，该配置文件位于各个架构目录的 `configs` 文件夹下，例如对于RISC-V而言，其默认配置文件为 `arch/riscv/configs/defconfig`。使用 `make ARCH=riscv defconfig` 命令可以在内核根目录下生成一个名为 `.config` 的文件，包含了内核完整的配置，内核在编译时会根据 `.config` 进行编译。

配置之间存在相互的依赖关系，直接修改`defconfig`文件或者 `.config` 有时候并不能达到想要的效果，或是给进一步内核配置带来同步问题。因此如果需要修改配置一般采用 `make ARCH=riscv menuconfig` 的方式对内核进行配置。

### 编译工具

`make` 是用于程序构建的重要工具，它的行为由当前目录或 `make -C` 指定目录下的 `Makefile` 来决定。更多有关 `Makefile` 的内容可以参考 [Learn Makefiles With the tastiest examples](#)。下面用本次实验中可能用到的用于编译 Linux 内核的编译命令作为示例：

```
$ make help                # 查看make命令的各种参数解释

$ make <target-name>      # 编译名为 <target-name> 的目标文件或目标任务
$ make defconfig          # 使用当前平台的默认配置，在x86机器上会使用x86的默认配置
$ make clean              # 清除所有编译好的 object 文件
$ make mrproper           # 删除所有编译产物和配置文件

$ make -j<thread-count>   # 使用 <thread-count> 个物理线程来进行多线程编译
$ make -j4                # 编译当前平台的内核，-j4 为使用 4 线程进行多线程编译
$ make -j$(nproc)         # 编译当前平台的内核，-j$(nproc) 为以全部机器硬件线程数进行多线程编译

$ make <var-name>=<var-value> # 在编译过程中将 <var-name> 变量的值手动设置为 <var-value>
$ make ARCH=riscv defconfig # 使用 RISC-V 平台的默认配置
$ make ARCH=riscv CROSS_COMPILE=riscv64-linux-gnu- # 编译 RISC-V 平台内核
```

我们可以手动为 `make` 指定变量的值，本次实验中用到的如下：

- `ARCH` 指定架构，可选的值包括 `arch` 目录下的文件夹名，如 `x86`、`arm`、`arm64` 等，不同于 `arm` 和 `arm64`，32 位和 64 位的RISC-V共用 `arch/riscv` 目录，通过使用不同的 `config` 可以编译 32 位或 64 位的内核。
- `CROSS_COMPILE` 指定使用的交叉编译工具链，例如指定 `CROSS_COMPILE=riscv64-linux-gnu-`，则编译时会采用 `riscv64-linux-gnu-gcc` 作为编译器，编译在 RISC-V 64 位平台上运行的 Linux 内核。

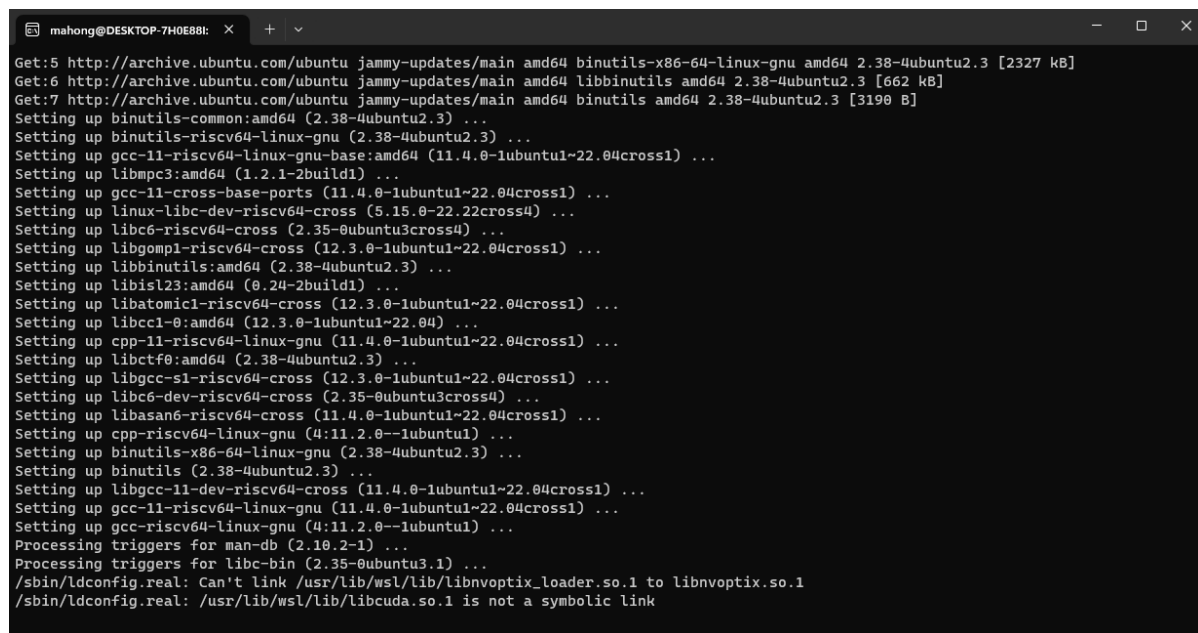
## 4 实验步骤

在执行每一条命令前，请你对将要进行的操作进行思考，给出的命令不需要全部执行，并且不是所有的命令都可以无条件执行，请不要直接复制粘贴命令去执行。

### 4.1 搭建实验环境

首先安装编译内核所需要的交叉编译工具链和用于构建程序的软件包

```
$ sudo apt install gcc-riscv64-linux-gnu
$ sudo apt install autoconf automake autotools-dev curl libmpc-dev libmpfr-dev
libgmp-dev \
                                gawk build-essential bison flex texinfo gperf libtool
patchutils bc \
                                zlib1g-dev libexpat-dev git
```



```
mahong@DESKTOP-7H0E88: ~
Get:5 http://archive.ubuntu.com/ubuntu jammy-updates/main amd64 binutils-x86-64-linux-gnu amd64 2.38-4ubuntu2.3 [2327 kB]
Get:6 http://archive.ubuntu.com/ubuntu jammy-updates/main amd64 libbinutils amd64 2.38-4ubuntu2.3 [662 kB]
Get:7 http://archive.ubuntu.com/ubuntu jammy-updates/main amd64 binutils amd64 2.38-4ubuntu2.3 [3190 B]
Setting up binutils-common:amd64 (2.38-4ubuntu2.3) ...
Setting up binutils-riscv64-linux-gnu (2.38-4ubuntu2.3) ...
Setting up gcc-11-riscv64-linux-gnu-base:amd64 (11.4.0-1ubuntu1~22.04cross1) ...
Setting up libmpc3:amd64 (1.2.1-2build1) ...
Setting up gcc-11-cross-base-ports (11.4.0-1ubuntu1~22.04cross1) ...
Setting up linux-libc-dev-riscv64-cross (5.15.0-22.22cross4) ...
Setting up libc6-riscv64-cross (2.35-0ubuntu3cross4) ...
Setting up libgomp1-riscv64-cross (12.3.0-1ubuntu1~22.04cross1) ...
Setting up libbinutils:amd64 (2.38-4ubuntu2.3) ...
Setting up libisl23:amd64 (0.24-2build1) ...
Setting up libatomic1-riscv64-cross (12.3.0-1ubuntu1~22.04cross1) ...
Setting up libcc1-0:amd64 (12.3.0-1ubuntu1~22.04) ...
Setting up cpp-11-riscv64-linux-gnu (11.4.0-1ubuntu1~22.04cross1) ...
Setting up libctf0:amd64 (2.38-4ubuntu2.3) ...
Setting up libgcc-s1-riscv64-cross (12.3.0-1ubuntu1~22.04cross1) ...
Setting up libc6-dev-riscv64-cross (2.35-0ubuntu3cross4) ...
Setting up libasan6-riscv64-cross (11.4.0-1ubuntu1~22.04cross1) ...
Setting up cpp-riscv64-linux-gnu (4:11.2.0--1ubuntu1) ...
Setting up binutils-x86-64-linux-gnu (2.38-4ubuntu2.3) ...
Setting up binutils (2.38-4ubuntu2.3) ...
Setting up libgcc-11-dev-riscv64-cross (11.4.0-1ubuntu1~22.04cross1) ...
Setting up gcc-11-riscv64-linux-gnu (11.4.0-1ubuntu1~22.04cross1) ...
Setting up gcc-riscv64-linux-gnu (4:11.2.0--1ubuntu1) ...
Processing triggers for man-db (2.10.2-1) ...
Processing triggers for libc-bin (2.35-0ubuntu3.1) ...
/sbin/ldconfig.real: Can't link /usr/lib/wsl/lib/libnvoptix_loader.so.1 to libnvoptix.so.1
/sbin/ldconfig.real: /usr/lib/wsl/lib/libcuda.so.1 is not a symbolic link
```

```

Setting up librt-dev:amd64 (2.0.4-8build2) ...
Setting up dpkg-dev (1.21.1ubuntu2.2) ...
Setting up libltdl-dev:amd64 (2.4.6-15build2) ...
Setting up libmpc-dev:amd64 (1.2.1-2build1) ...
Setting up libxml-libxml-perl (2.0207+dfsg+really+2.0134-1) ...
update-perl-sax-parsers: Registering Perl SAX parser XML::LibXML::SAX::Parser with priority 50...
update-perl-sax-parsers: Registering Perl SAX parser XML::LibXML::SAX with priority 50...
update-perl-sax-parsers: Updating overall Perl SAX parser modules info file...
Replacing config file /etc/perl/XML/SAX/ParserDetails.ini with new version
Setting up libwww-robotrules-perl (6.02-1) ...
Setting up libgcc-11-dev:amd64 (11.4.0-1ubuntu1~22.04) ...
Setting up gcc-11 (11.4.0-1ubuntu1~22.04) ...
Setting up cpp (4:11.2.0-1ubuntu1) ...
Setting up libhtml-parser-perl:amd64 (3.76-1build2) ...
Setting up libc6-dev:amd64 (2.35-0ubuntu3.4) ...
Setting up libtiff5:amd64 (4.3.0-6ubuntu0.5) ...
Setting up libfontconfig1:amd64 (2.13.1-4.2ubuntu5) ...
Setting up libio-socket-ssl-perl (2.074-2) ...
Setting up libhttp-message-perl (6.36-1) ...
Setting up libhtml-form-perl (6.07-1) ...
Setting up libhttp-negotiate-perl (6.01-1) ...
Setting up libhttp-cookies-perl (6.10-1) ...
Setting up libtool (2.4.6-15build2) ...
Setting up libhtml-tree-perl (5.07-2) ...
Setting up libhtml-format-perl (2.12-1.1) ...
Setting up gcc (4:11.2.0-1ubuntu1) ...
Setting up libexpat1-dev:amd64 (2.4.7-1ubuntu0.2) ...
Setting up libnet-smtp-ssl-perl (1.04-1) ...
Setting up libmailtools-perl (2.21-1) ...
Setting up libgd3:amd64 (2.3.0-2ubuntu2) ...
Setting up texinfo (6.8-4build1) ...
Setting up libstdc++-11-dev:amd64 (11.4.0-1ubuntu1~22.04) ...
Setting up zlib1g-dev:amd64 (1:1.2.11.dfsg-2ubuntu9.2) ...
Setting up libhttp-daemon-perl (6.13-1ubuntu0.1) ...
Setting up libc-devtools (2.35-0ubuntu3.4) ...
Setting up g++-11 (11.4.0-1ubuntu1~22.04) ...
Setting up g++ (4:11.2.0-1ubuntu1) ...
update-alternatives: using /usr/bin/g++ to provide /usr/bin/c++ (c++) in auto mode
Setting up build-essential (12.9ubuntu3) ...
Setting up liblwp-protocol-https-perl (6.10-1) ...
Setting up libwww-perl (6.61-1) ...
Setting up libxml-parser-perl:amd64 (2.46-3build1) ...
Setting up libxml-sax-expat-perl (0.51-1) ...
update-perl-sax-parsers: Registering Perl SAX parser XML::SAX::Expat with priority 50...
update-perl-sax-parsers: Updating overall Perl SAX parser modules info file...
Replacing config file /etc/perl/XML/SAX/ParserDetails.ini with new version
Processing triggers for install-info (6.8-4build1) ...
Processing triggers for libc-bin (2.35-0ubuntu3.1) ...
/sbin/ldconfig.real: Can't link /usr/lib/wsl/lib/libnvoptix_loader.so.1 to libnvoptix.so.1
/sbin/ldconfig.real: /usr/lib/wsl/lib/libcuda.so.1 is not a symbolic link

Processing triggers for man-db (2.10.2-1) ...
mahong@DESKTOP-7H0E88I:~$

```

接着是用于启动 riscv64 平台上的内核的模拟器 `qemu`

```
$ sudo apt install qemu-system-misc
```

```

Setting up libglx0:amd64 (1.4.0-1) ...
Setting up dconf-gsettings-backend:amd64 (0.40.0-3) ...
Setting up libpulse0:amd64 (1:15.99.1+dfsg1-1ubuntu2.1) ...
Setting up libxcursor1:amd64 (1:1.2.0-2build4) ...
Setting up libspice-server1:amd64 (0.15.0-2ubuntu4) ...
Setting up libpango-1.0-0:amd64 (1.50.6+ds-2ubuntu1) ...
Setting up gstreamer1.0-plugins-base:amd64 (1.20.1-1ubuntu0.1) ...
Setting up libgl1:amd64 (1.4.0-1) ...
Setting up libshout3:amd64 (2.4.5-1build3) ...
Setting up librbdl (17.2.6-0ubuntu0.22.04.1) ...
Setting up libgfapi0:amd64 (10.1-1ubuntu0.1) ...
Setting up libcupss2:amd64 (2.4.10p1-1ubuntu4.7) ...
Setting up libpangoft2-1.0-0:amd64 (1.50.6+ds-2ubuntu1) ...
Setting up libiscsi7:amd64 (1.19.0-3build2) ...
Setting up libsd12-2.0-0:amd64 (2.0.20+dfsg-2ubuntu1.22.04.1) ...
Setting up qemu-block-extra (1:6.2+dfsg-2ubuntu6.14) ...
Setting up libgtk-3-common (3.24.33-1ubuntu2) ...
Setting up libpangocairo-1.0-0:amd64 (1.50.6+ds-2ubuntu1) ...
Setting up gsettings-desktop-schemas (42.0-1ubuntu1) ...
Setting up gstreamer1.0-x:amd64 (1.20.1-1ubuntu0.1) ...
Setting up qemu-system-common (1:6.2+dfsg-2ubuntu6.14) ...
Created symlink /etc/systemd/system/multi-user.target.wants/qemu-kvm.service → /lib/systemd/system/qemu-kvm.service.
Setting up qemu-system-misc (1:6.2+dfsg-2ubuntu6.14) ...
Setting up librsvg2-2:amd64 (2.52.5+dfsg-3ubuntu0.2) ...
Setting up libdecor-0-plugin-1-cairo:amd64 (0.1.0-3build1) ...
Setting up librsvg2-common:amd64 (2.52.5+dfsg-3ubuntu0.2) ...
Setting up adwaita-icon-theme (41.0-1ubuntu1) ...
update-alternatives: using /usr/share/icons/Adwaita/cursor.theme to provide /usr/share/icons/default/index.theme (x-cursor-theme) in auto mode
Setting up humanity-icon-theme (0.6.16) ...
Setting up ubuntu-mono (20.10-0ubuntu2) ...
Processing triggers for man-db (2.10.2-1) ...
Processing triggers for libgl1:amd64 (1.4.0-1) ...
Setting up libgtk-3-0:amd64 (3.24.33-1ubuntu2) ...
Processing triggers for libc-bin (2.35-0ubuntu3.1) ...
/sbin/ldconfig.real: Can't link /usr/lib/wsl/lib/libnvoptix_loader.so.1 to libnvoptix.so.1
/sbin/ldconfig.real: /usr/lib/wsl/lib/libcuda.so.1 is not a symbolic link

Setting up libgtk-3-bin (3.24.33-1ubuntu2) ...
Setting up libvte-2.91-0:amd64 (0.68.0-1) ...
Setting up at-spi2-core (2.44.0-3) ...
Setting up glib-networking:amd64 (2.72.0-1) ...
Setting up libsoup2.4-1:amd64 (2.74.2-3) ...
Setting up qemu-system-gui (1:6.2+dfsg-2ubuntu6.14) ...
Setting up gstreamer1.0-plugins-good:amd64 (1.20.3-0ubuntu1.1) ...
Processing triggers for libgd3:amd64 (2.3.0-2ubuntu2) ...
Processing triggers for libc-bin (2.35-0ubuntu3.1) ...
/sbin/ldconfig.real: Can't link /usr/lib/wsl/lib/libnvoptix_loader.so.1 to libnvoptix.so.1
/sbin/ldconfig.real: /usr/lib/wsl/lib/libcuda.so.1 is not a symbolic link

```

我们还需要用 `gdb` 来对在 `qemu` 上运行的 Linux 内核进行调试

```
$ sudo apt install gdb-multiarch
```

```
Selecting previously unselected package libdebuginfod-common.
(Reading database ... 50728 files and directories currently installed.)
Preparing to unpack .../0-libdebuginfod-common_0.186-1build1_all.deb ...
Unpacking libdebuginfod-common (0.186-1build1) ...
Selecting previously unselected package libbabeltrace1:amd64.
Preparing to unpack .../1-libbabeltrace1_1.5.8-2build1_amd64.deb ...
Unpacking libbabeltrace1:amd64 (1.5.8-2build1) ...
Selecting previously unselected package libdebuginfod1:amd64.
Preparing to unpack .../2-libdebuginfod1_0.186-1build1_amd64.deb ...
Unpacking libdebuginfod1:amd64 (0.186-1build1) ...
Selecting previously unselected package libipt2.
Preparing to unpack .../3-libipt2_2.0.5-1_amd64.deb ...
Unpacking libipt2 (2.0.5-1) ...
Selecting previously unselected package libsource-highlight-common.
Preparing to unpack .../4-libsource-highlight-common_3.1.9-4.1build2_all.deb ...
Unpacking libsource-highlight-common (3.1.9-4.1build2) ...
Selecting previously unselected package libboost-regex1.74.0:amd64.
Preparing to unpack .../5-libboost-regex1.74.0-1.74.0-14ubuntu3_amd64.deb ...
Unpacking libboost-regex1.74.0:amd64 (1.74.0-14ubuntu3) ...
Selecting previously unselected package libsource-highlight4v5.
Preparing to unpack .../6-libsource-highlight4v5_3.1.9-4.1build2_amd64.deb ...
Unpacking libsource-highlight4v5 (3.1.9-4.1build2) ...
Selecting previously unselected package gdb.
Preparing to unpack .../7-gdb_12.1-0ubuntu1-22.04_amd64.deb ...
Unpacking gdb (12.1-0ubuntu1-22.04) ...
Selecting previously unselected package gdb-multiarch.
Preparing to unpack .../8-gdb-multiarch_12.1-0ubuntu1-22.04_amd64.deb ...
Unpacking gdb-multiarch (12.1-0ubuntu1-22.04) ...
Selecting previously unselected package libc6-dbg:amd64.
Preparing to unpack .../9-libc6-dbg_2.35-0ubuntu3.4_amd64.deb ...
Unpacking libc6-dbg:amd64 (2.35-0ubuntu3.4) ...
Setting up libdebuginfod-common (0.186-1build1) ...

Creating config file /etc/profile.d/debuginfod.sh with new version

Creating config file /etc/profile.d/debuginfod.csh with new version
Setting up libdebuginfod1:amd64 (0.186-1build1) ...
Setting up libsource-highlight-common (3.1.9-4.1build2) ...
Setting up libc6-dbg:amd64 (2.35-0ubuntu3.4) ...
Setting up libboost-regex1.74.0:amd64 (1.74.0-14ubuntu3) ...
Setting up libipt2 (2.0.5-1) ...
Setting up libbabeltrace1:amd64 (1.5.8-2build1) ...
Setting up libsource-highlight4v5 (3.1.9-4.1build2) ...
Setting up gdb (12.1-0ubuntu1-22.04) ...
Setting up gdb-multiarch (12.1-0ubuntu1-22.04) ...
Processing triggers for man-db (2.10.2-1) ...
Processing triggers for libc-bin (2.35-0ubuntu3.1) ...
/sbin/ldconfig.real: Can't link /usr/lib/wsl/lib/libnvoptix_loader.so.1 to libnvoptix.so.1
/sbin/ldconfig.real: /usr/lib/wsl/lib/libcuda.so.1 is not a symbolic link
```

## 4.2 获取 Linux 源码和已经编译好的文件系统

从 <https://www.kernel.org> 下载最新的 Linux 源码。

截至写作时，最新的 Linux 内核版本是 6.6-rc1。

并且使用 git 工具 clone [本仓库](#)。其中已经准备好了根文件系统的镜像。

根文件系统为 Linux Kernel 提供了基础的文件服务，在启动 Linux Kernel 时是必要的。

```
$ git clone https://gitee.com/zju_xiayingjie/os23fall-stu.git
```

```
$ cd os23fall-stu/src/lab0
```

```
$ ls
```

```
rootfs.img # 已经构建完成的根文件系统的镜像
```

```
mahong@DESKTOP-7H0E881:/mnt/c/Users/MaHong/Desktop/OS_EX$ tar -xvf linux-6.5.5.tar
mahong@DESKTOP-7H0E881:/mnt/c/Users/MaHong/Desktop/OS_EX$ git clone https://gitee.com/zju_xiayingjie/os23fall-stu.git
Cloning into 'os23fall-stu'...
remote: Enumerating objects: 147, done.
remote: Counting objects: 100% (147/147), done.
remote: Compressing objects: 100% (121/121), done.
remote: Total 147 (delta 33), reused 97 (delta 6), pack-reused 0
Receiving objects: 100% (147/147), 1.94 MiB | 1.07 MiB/s, done.
Resolving deltas: 100% (33/33), done.
mahong@DESKTOP-7H0E881:/mnt/c/Users/MaHong/Desktop/OS_EX$ cd os23fall-stu/src/lab0
mahong@DESKTOP-7H0E881:/mnt/c/Users/MaHong/Desktop/OS_EX/os23fall-stu/src/lab0$ ls
rootfs.img
mahong@DESKTOP-7H0E881:/mnt/c/Users/MaHong/Desktop/OS_EX/os23fall-stu/src/lab0$ |
```



## 4.3 编译 linux 内核

```
$ cd path/to/linux
$ make ARCH=riscv CROSS_COMPILE=riscv64-linux-gnu- defconfig # 使用默认配置
$ make ARCH=riscv CROSS_COMPILE=riscv64-linux-gnu- -j$(nproc) # 编译
```

```
mahong@DESKTOP-7H0E88I:/mnt/c/Users/MaHong/Desktop/OS_EX/os23fall-stu/src/lab0$ cd ../../linux-6.5.5
mahong@DESKTOP-7H0E88I:/mnt/c/Users/MaHong/Desktop/OS_EX/linux-6.5.5$ make ARCH=riscv CROSS_COMPILE=riscv64-linux-gnu- defconfig
HOSTCC scripts/basic/fixdep
HOSTCC scripts/kconfig/conf.o
HOSTCC scripts/kconfig/confdata.o
HOSTCC scripts/kconfig/expr.o
LEX scripts/kconfig/lexer.lex.c
YACC scripts/kconfig/parser.tab.[ch]
HOSTCC scripts/kconfig/lexer.lex.o
HOSTCC scripts/kconfig/menu.o
HOSTCC scripts/kconfig/parser.tab.o
HOSTCC scripts/kconfig/preprocess.o
HOSTCC scripts/kconfig/symbol.o
HOSTCC scripts/kconfig/util.o
HOSTLD scripts/kconfig/conf
*** Default configuration is based on 'defconfig'
#
# configuration written to .config
#
```

```
LD [M] net/xfrm/xfrm_user.ko
LD [M] net/ipv6/netfilter/ip6_tables.ko
LD [M] net/ipv6/netfilter/ip6table_filter.ko
LD [M] net/ipv6/netfilter/ip6table_mangle.ko
LD [M] net/ipv6/netfilter/nf_defrag_ipv6.ko
LD [M] net/ipv6/netfilter/nf_reject_ipv6.ko
LD [M] net/ipv6/ip6_udp_tunnel.ko
LD [M] net/ipv6/netfilter/ip6t_ipv6header.ko
LD [M] net/ipv6/netfilter/ip6t_REJECT.ko
LD [M] net/8021q/8021q.ko
LD [M] net/llc/llc.ko
LD [M] net/bridge/br_netfilter.ko
LD [M] net/bridge/bridge.ko
NM .tmp_vmlinux.kallsyms1.syms
KSYMS .tmp_vmlinux.kallsyms1.S
AS .tmp_vmlinux.kallsyms1.S
LD .tmp_vmlinux.kallsyms2
NM .tmp_vmlinux.kallsyms2.syms
KSYMS .tmp_vmlinux.kallsyms2.S
AS .tmp_vmlinux.kallsyms2.S
LD vmlinux
NM System.map
SORTTAB vmlinux
OBJCOPY arch/riscv/boot/Image
GZIP arch/riscv/boot/Image.gz
Kernel: arch/riscv/boot/Image.gz is ready
```

```
ahong@DESKTOP-7H0E88I:/mnt/c/Users/MaHong/Desktop/OS_EX/linux-6.5.5$ |
```

编译完成之后的文件结构：

```
Kernel: arch/riscv/boot/Image.gz is ready
mahong@DESKTOP-7H0E88I:/mnt/c/Users/MaHong/Desktop/OS_EX/linux-6.5.5$ ls
COPYING      Kconfig      Module.symvers  .config      .modules.order  modules.builtin  modules.builtin.modinfo  modules.order
CREDITS      MAINTAINERS  README          built-in.a    .config.gz      .modules.order  modules.builtin.modinfo  modules.order
Documentation  Makefile     System.map      .config.gz    .modules.order  modules.order    modules.builtin.modinfo  modules.order
Kbuild       Makefile     System.map      .config.gz    .modules.order  modules.order    modules.builtin.modinfo  modules.order
mahong@DESKTOP-7H0E88I:/mnt/c/Users/MaHong/Desktop/OS_EX/linux-6.5.5$ |
```

## 4.4 使用QEMU运行内核

```
$ qemu-system-riscv64 -nographic -machine virt -kernel arch/riscv/boot/Image \
    -device virtio-blk-device,drive=hd0 -append "root=/dev/vda ro console=ttyS0" \
    -bios default -drive file=./os23fall-stu/src/lab0/rootfs.img,format=raw,id=hd0
```

退出 QEMU 的方法为：使用 Ctrl+A，**松开**后再按下 X 键即可退出 QEMU。

```
mahong@DESKTOP-7H0E88L: ~
[ 0.100772] io scheduler mq-deadline registered
[ 0.100803] io scheduler kyber registered
[ 0.100856] io scheduler bfq registered
[ 0.102456] pci-host-generic 30000000.pci: host bridge /soc/pci@30000000 ranges:
[ 0.102965] pci-host-generic 30000000.pci: IO 0x0003000000..0x000300ffff -> 0x0000000000
[ 0.103206] pci-host-generic 30000000.pci: MEM 0x0040000000..0x007fffffff -> 0x0040000000
[ 0.103242] pci-host-generic 30000000.pci: MEM 0x0400000000..0x07fffffff -> 0x0400000000
[ 0.104039] pci-host-generic 30000000.pci: Memory resource size exceeds max for 32 bits
[ 0.104277] pci-host-generic 30000000.pci: ECAM at [mem 0x30000000-0x3fffffff] for [bus 00-ff]
[ 0.105245] pci-host-generic 30000000.pci: PCI host bridge to bus 0000:00
[ 0.105388] pci_bus 0000:00: root bus resource [bus 00-ff]
[ 0.105434] pci_bus 0000:00: root bus resource [io 0x0000-0xffff]
[ 0.105467] pci_bus 0000:00: root bus resource [mem 0x40000000-0x7fffffff]
[ 0.105472] pci_bus 0000:00: root bus resource [mem 0x400000000-0x7fffffff]
[ 0.106152] pci 0000:00:00.0: [1b36:0008] type 00 class 0x060000
[ 0.157619] Serial: 8250/16550 driver, 4 ports, IRQ sharing disabled
[ 0.163634] printk: console [ttyS0] disabled
[ 0.165296] 10000000.uart: ttyS0 at MMIO 0x10000000 (irq = 12, base_baud = 230400) is a 16550A
[ 0.166022] printk: console [ttyS0] enabled
[ 0.194907] SuperH (H)SCI(F) driver initialized
[ 0.203205] loop: module loaded
[ 0.203885] virtio_blk virtio0: 1/0/0 default/read/poll queues
[ 0.205626] virtio_blk virtio0: [vda] 32768 512-byte logical blocks (16.8 MB/16.0 MiB)
[ 0.217934] e1000e: Intel(R) PRO/1000 Network Driver
[ 0.218072] e1000e: Copyright(c) 1999 - 2015 Intel Corporation.
[ 0.219752] usbcore: registered new interface driver uas
[ 0.219931] usbcore: registered new interface driver usb-storage
[ 0.220627] moudev: PS/2 mouse device common for all mice
[ 0.222255] goldfish_rtc 101000.rtc: registered as rtc0
[ 0.222808] goldfish_rtc 101000.rtc: setting system clock to 2023-10-05T21:28:08 UTC (1696541288)
[ 0.224685] cpuidle-riscv-sbi: HSM suspend not available
[ 0.224974] sdhci: Secure Digital Host Controller Interface driver
[ 0.225273] sdhci: Copyright(c) Pierre Ossman
[ 0.225691] sdhci-pltfm: SDHCI platform and OF driver helper
[ 0.226328] usbcore: registered new interface driver usbhid
[ 0.226405] usbhid: USB HID core driver
[ 0.227538] NET: Registered PF_INET6 protocol family
[ 0.233686] Segment Routing with IPv6
[ 0.234050] In-situ OAM (IOAM) with IPv6
[ 0.234485] sit: IPv6, IPv4 and MPLS over IPv4 tunneling driver
[ 0.236318] NET: Registered PF_PACKET protocol family
[ 0.237274] 9pnet: Installing 9P2000 support
[ 0.237531] Key type dns_resolver registered
[ 0.253896] debug_vm_pgtable: [debug_vm_pgtable] : Validating architecture page table helpers
[ 0.258000] Legacy PMU implementation is available
[ 0.258910] clk: Disabling unused clocks
[ 0.282383] EXT4-fs (vda): mounted filesystem c3e9bbca-ec22-47f9-a368-187b21172fc1 ro with ordered data mode. Quota
ode: disabled.
[ 0.282834] VFS: Mounted root (ext4 filesystem) readonly on device 254:0.
[ 0.284833] devtmpfs: mounted
[ 0.302671] Freeing unused kernel image (initmem) memory: 2200K
[ 0.303170] Run /sbin/init as init process

Please press Enter to activate this console. █
```

## 4.5 使用 GDB 对内核进行调试

```
# Terminal 1
$ qemu-system-riscv64 -nographic -machine virt -kernel arch/riscv/boot/Image \
  -device virtio-blk-device,drive=hd0 -append "root=/dev/vda ro console=ttyS0" \
  -bios default -drive file=./os23fall-stu/src/lab0/rootfs.img,format=raw,id=hd0 -S -s

# Terminal 2
$ gdb-multiarch /mnt/c/users/mahong/desktop/OS_EX/linux-6.5.5
(gdb) target remote :1234 # 连接 qemu
(gdb) b start_kernel # 设置断点
(gdb) continue # 继续执行
(gdb) quit # 退出 gdb
```

左侧为terminal 1, 右侧为terminal 2



```
0.218972] e1000e: Copyright(c) 1999 - 2015 Intel Corporation.
0.218972] usbcore: registered new interface driver us
0.219311] usbcore: registered new interface driver usb-storage
0.220277] mousedev: PS/2 mouse device common for all sice
0.222253] goldfish_rtc 101800.rtc: registered as rtc0
0.222880] goldfish_rtc 101800.rtc: setting system clock to 2023-10-05T21:28:00 UTC (1696541280)
0.224652] cpuidle-riscv-ss: HPM suspend not available
0.224974] sdhci: Secure Digital Host Controller Interface driver
0.225273] sdhci: Copyright(c) Pierre Ossman
0.225691] sdhci-pltfm: SDHCI platform and OF driver helper
0.226328] usbcore: registered new interface driver usbhid
0.226469] usbhid: USB HID core driver
0.227538] NET: Registered PF_INET6 protocol family
0.233460] Segment Routing with IPv6
0.234058] In-situ OAM (IOAM) with IPv6
0.234855] sit: IPv6, IPv4 and MPLS over IPv4 tunneling driver
0.236131] NET: Registered PF_PACKET protocol family
0.237274] 9pnet: Installing 9P2000 support
0.237331] key type dns_resolver registered
0.238386] debug_vm_ptable: (debug_vm_ptable)
0.258800] Legacy PMU implementation is available
0.258910] clk: Disabling unused clocks
0.282383] EXT4-fs (vda): mounted filesystem c3e9bcca-c22-47f9-a368-187b21172fc1 ro with ordered data mode. Quota =
ode: disabled.
0.282383] VFS: Mounted root (ext4 filesystem) readonly on device 254:0.
0.284833] devtmpfs: mounted
0.286712] Freezing unused kernel image (initmem) memory: 2200K
0.289077] Run /sbin/init as init process

Please press Enter to activate this console. *ZEMU: Terminated
mahong@DESKTOP-7H8E8B1: /mnt/c/users/mahong/desktop/05_EX/linux-6.5.5 $ qemu-system-riscv64 -nographic -machine virt -kern
el arch/riscv/boot/image \
-device virtio-blk-device,drive=h0 -append "root=/dev/vda ro console=ttyS0 \
-bios default -drive file=../os23fall-stu/src/lab8/rootfs.img,format=raw,id=h0 -S -s

OpenSBI v0.9

Platform Name      : riscv-virtio,qemu
Platform Features  : timer,efideleg
Platform HART Count :
Firmware Base     : 0x00000000
Firmware Size     : 100 KB
Runtime SBI Version : 0.2

Domain Name       : root
Domain Boot HART  : 0
Domain HARTs      : 4
Domain Region00   : 0x0000000000000000-0x0000000000001ffff ()
Domain Region01   : 0x0000000000000000-0xffffffffffffff (R,W,X)
Domain Next Address : 0x000000000000200000
Domain Next Arg1   : 0x00000000007000000
Domain Next Arg0   : S-mode
Domain SysReset    : yes

Boot HART ID      : 0
Boot HART Domain  : root
Boot HART ISA     : rv64imafdcus
Boot HART Features : scounteren,acounteren,time
Boot HART PMP Count : 16
Boot HART PMP Granularity : 4
Boot HART PMP Address Bits: 54
Boot HART PMPW Count : 0
Boot HART PMPW Size : 0
Boot HART MIDDLEC : 0x00000000000000222
Boot HART MIDDLEC : 0x00000000000000109
0.000000] Linux version 6.5.5 (mahong@DESKTOP-7H8E8B1) (riscv64-linux-gnu-gcc (Ubuntu 11.4.0-1ubuntu1-22.04) 11.4.0
GNU ld (GNU Binutils for Ubuntu) 2.38) #1 SMP Fri Oct 6 05:03:11 CST 2023
0.000000] Machine model: riscv-virtio,qemu
0.000000] SBI specification v0.2 detected
0.000000] SBI implementation ID:0x1 Version:0x9
0.000000] SBI TIME extension detected
0.000000] SBI IPI extension detected
0.000000] SBI HFENCE extension detected
0.000000] efi: UEFI not found.
0.000000] OF reserved mem: 0x00000000000000000-0x0000000000001ffff (128 MiB) map non-reusable mmode_resv0000000000
0.000000] Zone ranges:
0.000000] DMA32 [mem 0x0000000000000000-0x00000000007ffffff]
0.000000] Normal empty
0.000000] Movable zone start for each node
```

```
0.000000] OpenSBI v0.9
Platform Name      : riscv-virtio,qemu
Platform Features  : timer,efideleg
Platform HART Count :
Firmware Base     : 0x00000000
Firmware Size     : 100 KB
Runtime SBI Version : 0.2

Domain Name       : root
Domain Boot HART  : 0
Domain HARTs      : 4
Domain Region00   : 0x0000000000000000-0x0000000000001ffff ()
Domain Region01   : 0x0000000000000000-0xffffffffffffff (R,W,X)
Domain Next Address : 0x000000000000200000
Domain Next Arg1   : 0x00000000007000000
Domain Next Arg0   : S-mode
Domain SysReset    : yes

Boot HART ID      : 0
Boot HART Domain  : root
Boot HART ISA     : rv64imafdcus
Boot HART Features : scounteren,acounteren,time
Boot HART PMP Count : 16
Boot HART PMP Granularity : 4
Boot HART PMP Address Bits: 54
Boot HART PMPW Count : 0
Boot HART PMPW Size : 0
Boot HART MIDDLEC : 0x00000000000000222
Boot HART MIDDLEC : 0x00000000000000109
0.000000] Linux version 6.5.5 (mahong@DESKTOP-7H8E8B1) (riscv64-linux-gnu-gcc (Ubuntu 11.4.0-1ubuntu1-22.04) 11.4.0
GNU ld (GNU Binutils for Ubuntu) 2.38) #1 SMP Fri Oct 6 05:03:11 CST 2023
0.000000] Machine model: riscv-virtio,qemu
0.000000] SBI specification v0.2 detected
0.000000] SBI implementation ID:0x1 Version:0x9
0.000000] SBI TIME extension detected
0.000000] SBI IPI extension detected
0.000000] SBI HFENCE extension detected
0.000000] efi: UEFI not found.
0.000000] OF reserved mem: 0x00000000000000000-0x0000000000001ffff (128 MiB) map non-reusable mmode_resv0000000000
0.000000] Zone ranges:
0.000000] DMA32 [mem 0x0000000000000000-0x00000000007ffffff]
0.000000] Normal empty
0.000000] Movable zone start for each node

mahong@DESKTOP-7H8E8B1: /mnt/c/users/mahong/desktop/05_EX/linux-6.5.5 $ qemu-system-riscv64 -nographic -machine virt -kern
el arch/riscv/boot/image \
-device virtio-blk-device,drive=h0 -append "root=/dev/vda ro console=ttyS0 \
-bios default -drive file=../os23fall-stu/src/lab8/rootfs.img,format=raw,id=h0 -S -s

OpenSBI v0.9

Platform Name      : riscv-virtio,qemu
Platform Features  : timer,efideleg
Platform HART Count :
Firmware Base     : 0x00000000
Firmware Size     : 100 KB
Runtime SBI Version : 0.2

Domain Name       : root
Domain Boot HART  : 0
Domain HARTs      : 4
Domain Region00   : 0x0000000000000000-0x0000000000001ffff ()
Domain Region01   : 0x0000000000000000-0xffffffffffffff (R,W,X)
Domain Next Address : 0x000000000000200000
Domain Next Arg1   : 0x00000000007000000
Domain Next Arg0   : S-mode
Domain SysReset    : yes

Boot HART ID      : 0
Boot HART Domain  : root
Boot HART ISA     : rv64imafdcus
Boot HART Features : scounteren,acounteren,time
Boot HART PMP Count : 16
Boot HART PMP Granularity : 4
Boot HART PMP Address Bits: 54
Boot HART PMPW Count : 0
Boot HART PMPW Size : 0
Boot HART MIDDLEC : 0x00000000000000222
Boot HART MIDDLEC : 0x00000000000000109
0.000000] Linux version 6.5.5 (mahong@DESKTOP-7H8E8B1) (riscv64-linux-gnu-gcc (Ubuntu 11.4.0-1ubuntu1-22.04) 11.4.0
GNU ld (GNU Binutils for Ubuntu) 2.38) #1 SMP Fri Oct 6 05:03:11 CST 2023
0.000000] Machine model: riscv-virtio,qemu
0.000000] SBI specification v0.2 detected
0.000000] SBI implementation ID:0x1 Version:0x9
0.000000] SBI TIME extension detected
0.000000] SBI IPI extension detected
0.000000] SBI HFENCE extension detected
0.000000] efi: UEFI not found.
0.000000] OF reserved mem: 0x00000000000000000-0x0000000000001ffff (128 MiB) map non-reusable mmode_resv0000000000
0.000000] Zone ranges:
0.000000] DMA32 [mem 0x0000000000000000-0x00000000007ffffff]
0.000000] Normal empty
0.000000] Movable zone start for each node
```

```
0.101395] 9p: Installing v9fs 9P2000 file system support
0.102373] NET: Registered PF_AGP protocol family
0.102576] Block layer SCSI generic (sgp) driver version 0.4 loaded (major 246)
0.102654] io scheduler mq-deadline registered
0.102687] io scheduler kyber registered
0.102765] io scheduler bfq registered
0.104220] pci-host-generic 38000000.pci: host bridge /soc/pci0380000000 ranges:
0.185214] pci-host-generic 38000000.pci: IO 0x0003800000-0x0003800000 -> 0x000000000000
0.185441] pci-host-generic 38000000.pci: MEM 0x0000000000-0x0000000000 -> 0x000000000000
0.185471] pci-host-generic 38000000.pci: MEM 0x0000000000-0x0000000000 -> 0x000000000000
0.185717] pci-host-generic 38000000.pci: Memory resource size exceeds max for 32 bits
0.185934] pci-host-generic 38000000.pci: ECAM at [mem 0x380000000-0x380000000] for [bus 00-ff]
0.186080] pci-host-generic 38000000.pci: PCI host bridge to bus 0000:00
0.186084] pci bus 0000:00: root bus resource [bus 00-ff]
0.186084] pci bus 0000:00: root bus resource [io 0x0000-0xffff]
0.186079] pci bus 0000:00: root bus resource [mem 0x00000000-0xffffffff]
0.186084] pci bus 0000:00: root bus resource [mem 0x00000000-0xffffffff]
0.187584] pci 0000:00:00.0: [1036:0000] type 00 class 0x068000
0.197081] Serial: 0x00000000 driver, 4 ports, IRQ sharing disabled
0.163082] printk: console [ttyS0] disabled
0.164792] 100000000 uart1 ttyS0 at MMIO 0x100000000 (irq = 12, base_baud = 230400) is a 16550A
0.165014] printk: console [ttyS0] enabled
0.193862] SuperH (HSCIT) driver initialized
0.201754] loop: module loaded
0.202363] virtio_blk virtio0: 1/0/0 default/read/poll queues
0.202607] virtio_blk virtio0: (vda) 32768 32-byte logical blocks (16.8 MiB/16.8 MiB)
0.217521] e1000e: Intel(r) PRO/1000 Network Driver
0.217640] e1000e: Copyright(c) 1999 - 2015 Intel Corporation.
0.218972] usbcore: registered new interface driver us
0.219104] usbcore: registered new interface driver usb-storage
0.219597] mousedev: PS/2 mouse device common for all mice
0.221580] goldfish_rtc 101800.rtc: registered as rtc0
0.222024] goldfish_rtc 101800.rtc: setting system clock to 2023-10-05T21:36:52 UTC (1696541812)
0.222970] cpuidle-riscv-ss: HPM suspend not available
0.224258] sdhci: Secure Digital Host Controller Interface driver
0.224716] sdhci: Copyright(c) Pierre Ossman
0.225131] sdhci-pltfm: SDHCI platform and OF driver helper
0.225587] usbcore: registered new interface driver usbhid
0.225669] usbhid: USB HID core driver
0.226481] NET: Registered PF_INET6 protocol family
0.231479] Segment Routing with IPv6
0.231673] In-situ OAM (IOAM) with IPv6
0.232802] sit: IPv6, IPv4 and MPLS over IPv4 tunneling driver
0.233803] NET: Registered PF_PACKET protocol family
0.234613] 9pnet: Installing 9P2000 support
0.234893] key type dns_resolver registered
0.235656] debug_vm_ptable: (debug_vm_ptable)
0.254744] Legacy PMU implementation is available
0.254853] clk: Disabling unused clocks
0.305807] EXT4-fs (vda): mounted filesystem c3e9bcca-c22-47f9-a368-187b21172fc1 ro with ordered data mode. Quota =
ode: disabled.
0.306231] VFS: Mounted root (ext4 filesystem) readonly on device 254:0.
0.309183] devtmpfs: mounted
0.320261] Freezing unused kernel image (initmem) memory: 2200K
0.320907] Run /sbin/init as init process

Please press Enter to activate this console.
```

## 5 实验任务与要求

编译内核，使用QEMU启动后，远程连接GDB进行调试，并尝试使用GDB的各项命令（如backtrace, finish, frame, info, break, display, next, layout等）。

info	<pre>(gdb) info List of info subcommands:  info address -- Describe where symbol SVM is stored. info all-registers -- List of all registers and their contents, for selected stack frame. info args -- All argument variables of current stack frame or those matching REGEXPs. info auto-load -- Print current status of auto-loaded files. info auxv -- Display the inferior's auxiliary vector. info bookmarks -- Status of user-settable bookmarks. info breakpoints, info b -- Status of specified breakpoints (all user-settable breakpoints if no argument). info checkpoints -- IDs of currently known checkpoints. info classes -- All Objective-C classes, or those matching REGEXP. info common -- Print out the values contained in a Fortran COMMON block. info connections -- Target connections in use. info copying -- Conditions for redistributing copies of GDB. info dcache -- Print information on the dcache performance. info display -- Expressions to display when program stops, with code numbers. info exceptions -- List all Ada exception names. info extensions -- All filename extensions associated with a source language. info files -- Names of targets and files being debugged. info float -- Print the status of the floating point unit. info frame, info f -- All about the selected stack frame. info frame-filter -- List all registered Python frame-filters. info functions -- All function names or those matching REGEXPs. info guile, info gu -- Prefix command for Guile info displays. info inferiors -- Print a list of inferiors being managed. info line -- Core addresses of the code for a source line. info locals -- All local variables of current stack frame or those matching REGEXPs. info macro -- Show the definition of MACRO, and it's source location. info macros -- Show the definitions of all macros at LINESPEC, or the current source location. info mem -- Memory region attributes. info module -- Print information about modules. info modules -- All module names, or those matching REGEXP. info os -- Show OS data ARG. info pretty-printer -- GDB command to list all registered pretty-printers. info probes -- Show available static probes. info proc -- Show additional information about a process. info program -- Execution status of the program. info record, info rec -- Info record options. info registers, info r -- List of integer registers and their contents, for selected stack frame. info scope -- List the variables local to a scope. info selectors -- All Objective-C selectors, or those matching REGEXP. info sharedlibrary, info dll -- Status of loaded shared object libraries. info signals, info handle -- What debugger does when program gets various signals. info skip -- Display the status of skips. info source -- Information about the current source file. info sources -- All source files in the program or those matching REGEXP. info stack, info s -- Backtrace of the stack, or innermost COUNT frames. info static-tracepoint-markers -- List target static tracepoints markers. info symbol -- Describe what symbol is at location ADDR. info target -- Names of targets and files being debugged. info tasks -- Provide information about all known Ada tasks. info terminal -- Print inferior's saved terminal status. info threads -- Display currently known threads. info tracepoints, info tp -- Status of specified tracepoints (all tracepoints if no argument). info tvariables -- Status of trace state variables and their values. info type-printers -- GDB command to list all registered type-printers. info types -- All type names, or those matching REGEXP. info unwinder -- GDB command to list unwinders. info variables -- All global and static variable names or those matching REGEXPs. info vector -- Print the status of the vector unit. info vtbl -- Show the virtual function table for a C++ object. info warranty -- Various kinds of warranty you do not have. info watchpoints -- Status of specified watchpoints (all watchpoints if no argument). --Type &lt;RET&gt; for more, q to quit, c to continue without paging--</pre>
backtrace	<pre>(gdb) backtrace #0  0x0000000000000100 in ?? ()</pre>
layout asm	<pre>b&gt; 0x1000 auipc    t0,0x0 0x1004 addi      a2,t0,40 0x1008 csrr      a0,mhartid 0x100c ld        a1,32(t0) 0x1010 ld        t0,24(t0) 0x1014 jr        t0 0x1018 unimp 0x101a .2byte    0x8000 0x101c unimp 0x101e unimp 0x1020 unimp 0x1022 .2byte    0x8700 0x1024 unimp 0x1026 unimp 0x1028 fnmadd.s    ft6,ft4,fs4,fs1,unknown 0x102c unimp 0x102e unimp 0x1030 c.slli64    zero 0x1032 unimp 0x1034 unimp 0x1036 unimp 0x1038 unimp 0x103a .2byte    0x8020 0x103c unimp 0x103e unimp 0x1040 nop 0x1042 unimp 0x1044 unimp 0x1046 unimp 0x1048 unimp 0x104a unimp 0x104c unimp 0x104e unimp 0x1050 unimp 0x1052 unimp 0x1054 unimp 0x1056 unimp 0x1058 unimp 0x105a unimp 0x105c unimp 0x105e unimp 0x1060 unimp  remote Thread 1.1 In:                                     L??  PC: 0x1000 (gdb)</pre>
frame	<pre>(gdb) frame #0  0x0000000000000100 in ?? ()</pre>

break	(gdb) break Note: breakpoint 3 also set at pc 0x1000. Breakpoint 4 at 0x1000
next	(gdb) next Cannot find bounds of current function

## 6 思考题

1. 使用 `riscv64-unknown-elf-gcc` 编译单个 `.c` 文件

```
mahong@DESKTOP-7H0E88I:/mnt/c/Users/MaHong/Desktop/OS_EX/test$ ls
makefile test test.c
mahong@DESKTOP-7H0E88I:/mnt/c/Users/MaHong/Desktop/OS_EX/test$ make ARCH=riscv CROSS_COMPILE=riscv64-linux-gnu- -j$(nproc)
gcc -Wall -Wextra -o test test.c
gcc -c test.c
mahong@DESKTOP-7H0E88I:/mnt/c/Users/MaHong/Desktop/OS_EX/test$ ./test
hello world!
mahong@DESKTOP-7H0E88I:/mnt/c/Users/MaHong/Desktop/OS_EX/test$
```

2. 使用 `riscv64-unknown-elf-objdump` 反汇编 1 中得到的编译产物

```
mahong@DESKTOP-7H0E88I:/mnt/c/Users/MaHong/Desktop/OS_EX/test$ riscv64-linux-gnu-objdump -d test
test:      file format elf64-little

riscv64-linux-gnu-objdump: can't disassemble for architecture UNKNOWN!
```

3. 调试 Linux 时:

下断点并查看断点

```
(gdb) break *0x80000000
Breakpoint 1 at 0x80000000
(gdb) break *0x80200000
Breakpoint 2 at 0x80200000
(gdb) info breakpoint
Num      Type             Disp Enb Address      What
1        breakpoint        keep y   0x80000000
2        breakpoint        keep y   0x80200000
```

运行到断点/清除断点/单步调试/退出QEMU

```
(gdb) continue
Continuing.

Breakpoint 1, 0x0000000080000000 in ?? ()
(gdb) delete 1
(gdb) step
Cannot find bounds of current function
(gdb) monitor quit
(gdb)
```

4. 使用 `make` 工具清除 Linux 的构建产物

```
mahong@DESKTOP-7H0E88I: /mnt/c/Users/MaHong/Desktop/OS_EX/linux-6.5.5$ make clean
CLEAN drivers/firmware/efi/libstub
CLEAN drivers/gpu/drm/radeon
CLEAN drivers/scsi
CLEAN drivers/tty/vt
CLEAN init
CLEAN kernel
CLEAN lib/raid6
CLEAN lib
CLEAN security/apparmor
CLEAN security/selinux
CLEAN usr
CLEAN .
make[2]: *** Documentation/Kbuild: Is a directory. Stop.
make[1]: *** [/mnt/c/Users/MaHong/Desktop/OS_EX/linux-6.5.5/Makefile:2039: _clean_Documentation] Error 2
make: *** [Makefile:234: __sub-make] Error 2
mahong@DESKTOP-7H0E88I: /mnt/c/Users/MaHong/Desktop/OS_EX/linux-6.5.5$
```

5. `vmlinux` 和 `Image` 的关系和区别是什么？

`vmlinux` 和 `Image` 是Linux内核构建过程中生成的两个不同的文件。

`vmlinux`: Linux内核编译出来的原始的内核文件，elf格式，未做压缩处理。该映像可用于定位内核问题，但不能直接引导Linux系统启动。

`Image`: Linux内核编译时，使用objcopy处理vmlinux后生成的二进制内核映像。该映像未压缩，可直接引导Linux系统启动。

## 7 心得体会

在这次实验中，我成功地使用了交叉编译工具来完成Linux内核代码编译，并学习了如何使用QEMU运行内核，熟悉了GDB和QEMU联合调试的具体操作。