|  |  |
| --- | --- |
| 实验编号：**Lab1** | |
| 实验题目：Nachos实验环境准备、安装与源码分析 | |
| 实验学时：5 | 实验日期：2022.12.4 |
| 实验目的：  1. Nachos开发环境的安装测试(不含Linux系统本身及虚拟机软件的安装测试)。  2. Nachos实验代码框架(源码目录)的基本分析。  3. Nachos Makefile的基本分析。  4. 硬件机制模拟部分的实现原理分析，包括中断、时钟、CPU指令执行。 | |
| 硬件环境：  联想品牌 thinkbook14+ 型号笔记本  AMD Ryzen7-6800H CPU  32GB内存  512GB SSD | |
| 软件环境：  宿主机：Windows 10 22H2 64位  虚拟机软件：VMware Workstation Pro 16.1.2 build-17966106  Linux：Ubuntu 14.04.6 LTS Desktop i386 (Trusty Tahr)  gcc/g++：(Ubuntu 4.8.4-2ubuntu1~14.04.4) 4.8.4  MIPS交叉编译器：gcc-2.8.1-mips.tar.gz  Nachos：Nachos-3.4-UALR-2022 | |
| 实验步骤与内容：  目录  [一、Nachos环境安装 2](#_Toc121471248)  [*1.1更新Ubuntu的源* 2](#_Toc121471249)  [*1.2安装gcc，g++,make及一些gcc库* 3](#_Toc121471250)  [*1.3 安装用于MIPS的交叉编译器* 3](#_Toc121471251)  [*1.4 安装Nachos 3.4* 3](#_Toc121471252)  [*1.5 测试Nachos threads* 4](#_Toc121471253)  [二、 Make分析 5](#_Toc121471254)  [*2.1 make基本原理* 5](#_Toc121471255)  [*2.2 make中的变量与规则* 6](#_Toc121471256)  [*2.3 Nachos的Makefile结构* 7](#_Toc121471257)  [三、Nachos概述 11](#_Toc121471258)  [*3.1 Nachos概念及其特点* 11](#_Toc121471259)  [*3.2 Nachos目录结构* 12](#_Toc121471260)  [*3.3 Nachos各个部分的编译运行* 13](#_Toc121471261)  [*3.4 应用程序的编译* 13](#_Toc121471262)  [四、Nachos虚拟机 14](#_Toc121471263)  [*4.1 Machine分析* 16](#_Toc121471264)  [*4.2 Interrupt分析* 16](#_Toc121471265)  [*4.3 Timer分析* 23](#_Toc121471266)  [*4.4 Nachos控制台与统计信息* 25](#_Toc121471267)  [*4.5 Nachos Disk分析* 27](#_Toc121471268)  [五、Nachos启动分析 27](#_Toc121471269)  [六、Nachos Thread分析 32](#_Toc121471270)  [七、Nachos Schedule分析 38](#_Toc121471271)  [八、Nachos Semaphore分析 41](#_Toc121471272)  [*8.1 Nachos Semaphore* 41](#_Toc121471273)  [*8.2 ring分析* 44](#_Toc121471274)  [九、Nachos用户程序 46](#_Toc121471275)  [十、Nachos系统调用 49](#_Toc121471276) 一、Nachos环境安装1.1更新Ubuntu的源 对Ubuntu的源进行替换，防止一些站点网速过慢。替换为清华https://mirrors.tuna.tsinghua.edu.cn/help/ubuntu/的Ubuntu14.04镜像源  **（1）备份系统自带更新源配置文件**  切换到管理员，进入/etc/apt目录，输入：  cp sources.list sources.list.backup  **（2）在清华Ubuntu镜像源网站找到Ubuntu14.04的源进行复制**  **（3）打开sources.list文件**  gedit sources.list  **（4）将内容替换为刚刚复制的清华源并保存**  **（5）更新Ubuntu的源**  apt update 1.2安装gcc，g++,make及一些gcc库 (1)sudo apt install gcc  (2)sudo apt install g++  (3)sudo apt install make  (4)sudo apt install gcc-multilib g++-multilib 1.3 安装用于MIPS的交叉编译器 **（1）将压缩包 gcc-2.8.1-mips.tar.gz 复制到 ~ (Home，用户主目录)**  **（2）**cd /usr/local  **（3）将文件解压缩**  sudo tar -xzvf ~/gcc-2.8.1-mips.tar.gz 1.4 安装Nachos 3.4 **（1）**cd ~  **（2）**mkdir oscp  **（3）**cd oscp  **（4）将压缩包 nachos-3.4-ualr-2022.tar.gz 复制到 ~/oscp**  **（5）将文件解压缩**  tar -xzvf nachos-3.4-ualr-2022.tar.gz 1.5 测试Nachos threads **（1）**cd ~/oscp/nachos-3.4-ualr-2022/code/threads  **（2）**make clean  **（3）**make  **（4）**./nachos  测试结果   二、 Make分析2.1 make基本原理 make 是一种控制编译或重复编译软件的工具软件，make 可以自动管理软件的编译内容、 编译方式和编译时机。使用 make 需要你为你所编写的软件的开发过程和组织结构编写一个 Makefile 文件。make 将根据 Makefile 中的说明去自动管理你的软件的开 发过程。Makefile 是一个文本形式的数据库文件。可应包含以下目标软件的生成规则：  target: dependency […]   command1   command2   […]   * target：目标体（target），即 make 要建立的目标文件。 * dependency：目标的依赖体（dependency）列表，通常为要编译的源文件或要连接的浮动目标代码文件。 * command： 从目标依赖体创建目标体的命令（command）列表，通常为编译或连接命令。   例如我们编写了一个 C 程序存放在hello.c和一个hello.h文件中，为了使用 make 自动管理这个 C 程序的开发，可以编写以下 Makefile 文件：  hell.o: hello.c hello.h  gcc –c hello.c hello.h hello: hello.o  gcc hello.o –o hello clean:  rm –f \*.o  这样我们就可以在**命令行**中使用 make命令 按我们说明在 Makefile 中的编译规则编译我们的程序了：  make #生成可执行文件 hello make hello.o #生成浮动模块文件 hello.o make clean #清除所有.o 文件  **make 怎样知道什么时候需要重新编译或无需重新编译或编译部分文件呢？**   * 如果指定的目标体 make 找不到，make 就根据该目标体在 Makefile 中说明的生成规则**建立**它。 * 如果目标体存在，make 就对目标体和依赖体的**时间戳**进行比较，若有一个或 多个依赖体**比目标体新**，make 就根据生成命令**重新生成目标体**。这意味着每个 依赖体的改动都将使目标体重新生成。  2.2 make中的变量与规则 **make 中的宏变量：**  在 Makefile 中可以定义宏变量。**变量的定义格式为：变量名=字符串1 字符串2 ….**，变量的引用格式为：**$(变量名)**  如之前hello例可改写为：  obj=hello.o hello: $(obj)  gcc $(obj) –o hello  **make 中的自动变量：**  make 中提供了一组元字符用来表示自动变量，自动变量用来匹配某种规则，它们有：  $@ 规则的目标体所对应的文件名 $< 规则中第一个相关文件名 $^ 规则中所有相关文件名的列表 $? 规则中所有日期新于目标文件名的列表 $(@D) 目标文件的目录部分 $(@F) 目标文件的文件名部分  **make 中的预定义变量：**  AR 归档维护程序，默认值=ar AS 汇编程序，默认值=as CC C 编译程序，默认值=gcc CPP C++编译程序，默认值=cpp RM 删除程序，默认值=rm -f ARFIAGS 归档选项开关，默认值=rv ASFLAGE 汇编选项开关 CFLAGS C 编译选项开关 CPPFLAGS C++编译选项开关 LDFILAGS 链接选项开关  **make中隐式规则（静态规则）：**  编译过程中一些固定的规则可以省略说明，称为隐式规则。如上例中目标体 hello.o 的规则隐含在目标体 hello 的规则中，就属于隐式规则，可以省略为：  obj=hello.c hello: $(obj)  gcc $(obj) –o hello  **make 中的模式规则：**  % 用于匹配目标体和依赖体中任意非空字符串，例如：  %.o: %.c  $(cc) –c $^ -o $@  以上的模式规则表示，用 g++编译器编译依赖体中所有的.c 文件，生成.o 浮动目标模块，目标文件名采用目标体文件名。 2.3 Nachos的Makefile结构 在Nachos的 code 目录中有个子目录公用的 Makefile 文件： Makefile.common，在 code/下的每个子目录中各自都有两个 Makefile 文件： Makefile,Makefile.local，即 Nachos 系统的 Makefile 结构为：  ../code/Makefile.common,Makefile.dep |\_\_\_\_threads /Makefile,Makefile.local |\_\_\_\_userprog/ Makefile,Makefile.local . . . |\_\_\_\_filesys /Makefile,Makefile.local  在code/下的每个子目录中的Makefile都有以下两行代码，分别导入同级目录的Makefile.local与上一级目录公用的Makefile.common：  include Makefile.local include ../Makefile.common   * Makefile.local：Makefile.local 每个子目录中都不同，主要用于说明本目录中文件特有的依赖关系。 其中预定义变量的值为：   + CCFILE 构造本目录中 Nachos 系统所用到的 C++源文件的文件名串   + INCPATH 指示 g++编译器查找 C++源程序中括入的.h 文件的路径名串   + DEFINES 传递给 g++编译器的标号串 * 例如在threads/目录下的Makefile.local的定义为： * CCFILES = main.cc\  list.cc\  scheduler.cc\  synch.cc\  synchlist.cc\  system.cc\  thread.cc\  utility.cc\  threadtest.cc\  synchtest.cc\  interrupt.cc\  sysdep.cc\  stats.cc\  timer.cc INCPATH += -I../threads -I../machine DEFINES += -DTHREADS   Nachos允许你在code/下任建的一个新目录中利用原有的内核源代码扩充和修改后重新构造。在这个**新目录中可以仅有你想改变的源代码文件或增加一些你为内核源代码新增的文件。**   * 例如，我们要在空目录../lab2/目录中重新构造一个仅改变了调度算法的新版Nachos内核。 假设这需要改变Scheduler类，使用新的scheduler.h和scheduler.cc文件。而其他所有的文件仍然使用在../threads/，../machine/等目录中原有的文件。 * 为了这样做，首先你需要在../lab2/目录中重建或从../threads/目录中拷贝scheduler.h和scheduler.cc文件，从../threads/目录中递归的拷贝../arch/目录和Makefile, Makefile.local文件。接下来的工作是修改../lab2/中的Makefile.local文件，以便能在.. /lab2/中正确的构建新的Nachos * 在Makefile. local文件中定义了基本的CCFILE宏和重定义的INCPATH宏。**如果新增了.cc文件你需要在CCFILE中声明。**本例中CCFILE宏无需改变，因为你没有增加新的.cc文件，make会**沿着vpaths定义的路径顺序(vpath定义在Makefile.common中)**查找所有不在当前目录中.cc文件。重定义的INCPATH需要修改。首先要把**当前新建的目录**添加到INCPATH中： * INCPATH += -I- -I../labe –I../threads –I../machine * -I-作用：编译开关。-I-开关禁止处理与.cc文件在同一个目 录中的.h文件，即关闭由g++ MM产生的依赖关系，让每个.cc文件按INCPATH定义 的路径查找.h文件。 * 不添加-I-的话会产生如下影响：INCPATH += -I../labe –I../threads –I../machine * 这样做仅是声明了.cc文件中直接扩入的.h文件的查找路径，但是一些.cc文件中间 接括入的.h文件的查找路径并不是按照INCPATH定义的路径查找的,它们是按照由g ++ MM产生的依赖关系来查找的。因此一些不在当前目录中而又间接括入了当前目录中.h文件的.cc文件不会随着当前目录中.h文件的修改而重新编译。 * 例如main.cc文件括入了system.h文件， 而system.h文件又括入了scheduler.h文件，现在的main.cc不会随着scheduler.h的 改变而重新编译。 * 解决这个问题的第一种方法是：查出不在本目录中所有与要修改的.h文件有间接关系的文件，将它们拷贝到当前目录中。但这种方法比较麻烦。**解决这个问题的第二种方法是：利用-I-编译开关。** * 现在不需要查找和拷贝不在本目录中所有与要修改的.h文件有间接关系的文件了， make会根据我们在当前目录中所作的修改正确的重构新的系统。 * Makefile.dep：在 code/目录中的 Makefile.dep 文件用于定义由 g++使用的系统依赖关系的宏。**它被括入在 code/Makefile.common 文件中。**当前发行的 Nachos 可以在 4 种不同的 unix/linux 系统中编译并生成可执行的二进制文件 nachos。可执行文件统一放在 arch 目录的特定目录下。例如在 i386 的 linux 系统中可执行的 nachos 程序应放在 arch/unknown-i386-linux/bin/目录中。 * 这些在 Makefile.dep 定义的依赖系统的宏有：   + HOST 主机系统架构   + arch 文档存放路径   + CPP C++编译器的名字   + CPPFLAGS C++编译开关   + GCCDIR g++安装路径   + LDFLAGS 程序链接开关   + ASFLAGS 汇编开关 * 例如：当前系统为 i386 架构，linux 操作系统，则以上的宏定义为： * HOST\_LINUX=-linux HOST = -DHOST\_i386 -DHOST\_LINUX CPP=/lib/cpp CPPFLAGS = $(INCDIR) -D HOST\_i386 -D HOST\_LINUX arch = unknown-i386-linux * 在这个文件中还定义了其他一些依赖系统的宏，它们是： * arch\_dir = arch/$(arch) #归档文件目录 obj\_dir = $(arch\_dir)/objects #存放目标文件的目录 bin\_dir = $(arch\_dir)/bin #存放可执行文件的目录 depends\_dir = $(arch\_dir)/depends #存放依赖关系文件的目录 * 例如在i386/linux系统中最后3个目录为： 、   + arch/unknown-i386-linux/objects   + arch/unknown-i386-linux/bin   + arch/unknown-i386-linux/depends * Makefile.common： * code/目录中的 Makefile.common 首先括入 Makefile.dep，然后用 vpath 定义各类 文件搜索路径。 * include ../Makefile.dep vpath %.cc ../network:../filesys:../vm:../userprog:../threads:../machine vpath %.h ../network:../filesys:../vm:../userprog:../threads:../machine vpath %.s ../network:../filesys:../vm:../userprog:../threads:../machine * **vpath 定义告诉 make 到哪儿去查找在当前目录中找不到的文件。这就是为什么我们在一个新的目录中构造一个新的 Nachos 系统时不必复制那些我们不作修改的文件的原因。** * 然后定义了根据.cc和.h、.c和.h、.s文件编译链接生成.o文件（Linux系统存储在unknown-i386-linux/bin中）的指令。以及根据所有的.o 文件构造二进制可执行文件 nachos的命令。具体内容可见Makefile.common  三、Nachos概述3.1 Nachos概念及其特点 Nachos 是美国加州大学伯克莱分校在操作系统课程中已多次使用的操作系统课程设计平台，在美国很多大学中得到了应用，它具有一下几个突出的特点：   1. 采用通用虚拟机   Nachos是建立在一个软件模拟的虚拟机之上的，模拟了MIPS R2/3000的指令集、主存、中断系统、网络以及磁盘系统等操作系统所必须的硬件系统。许多现代操作系统大多是先在用软件模拟的硬件上建立并调试，最后才在真正的硬件上运行。用软件模拟硬件的可靠性比真实硬件高得多，不会因为硬件故障而导致系统出错，便于调试。虚拟机可以在运行时报告详尽的出错信息，更重要的是采用虚拟机使Nachos的移植变得非常容易，在不同机器上移植Nachos，只需对虚拟机部分作移植即可。  采用R2/3000指令集的原因是该指令集为RISC指令集，其指令数目比较少。Nachos虚拟机模拟了其中的63条指令。由于R2/3000指令集是一个比较常用的指令集，许多现有的编译器如gc++能够直接将C或C++源程序编译成该指令集的目标代码，于是就不必编写编译器，读者就可以直接用C/C++语言编写应用程序，使得在Nachos上开发大型的应用程序也成为可能。   1. 使用并实现了操作系统中的一些新的概念   随着计算机技术和操作系统技术的不断发展，产生了很多新的概念。Nachos将这些新概念融入操作系统教学中，包括网络、线程和分布式应用。而且Nachos以线程作为一个基本概念讲述，取代了进程在以前操作系统教学中的地位。  Nachos的虚拟机使得网络的实现相当简单。与MINIX不同，Nachos只是一个在宿主机上运行的一个进程。在同一个宿主机上可以运行多个Nachos进程，各个进程可以相互通讯，作为一个全互连网络的一个节点；进程之间通过Socket进行通讯，模拟了一个全互连网络。   1. 确定性调试比较方便；随机因素使系统运行更加真实   因为操作系统的不确定性，所以在一个实际的系统中进行多线程调试是比较困难的。由于Nachos是在宿主机上运行的进程，它提供了确定性调试的手段。所谓确定性调试，就是在同样的输入顺序、输入参数的情况下，Nachos运行的结果是完全一样的。在多线程调试中，可以将注意力集中在某一个实际问题上，而不受操作系统不确定性的干扰。  另外，不确定性是操作系统所必须具有的特征，Nachos采用了随机因子模拟了真实操作系统的不确定性。   1. 简单而易于扩展   Nachos是一个教学用操作系统平台，它必须简单而且有一定的扩展余地。Nachos不是向读者展示一个成功的操作系统，而是让读者在一个框架下发挥自己的创造性进行扩展。例如一个完整的类似于UNIX的文件系统是很复杂的，但是对于文件系统来说，无非是需要实现文件的逻辑地址到物理地址的映射以及实现文件inode、打开文件结构、线程打开文件表等重要的数据结构以及维护它们之间的关系。Nachos中具有所有这些内容，但是在很多方面作了一定的限制，比如只有一级索引结构限制了系统中最大文件的大小。读者可以应用学到的各种知识对文件系统进行扩展，逐步消除这些限制。Nachos在每一部分给出很多课程作业，作为读者进行系统扩展的提示和检查对系统扩展的结果。   1. 面向对象性   Nachos的主体是用C++的一个子集来实现的。目前面向对象语言日渐流行，它能够清楚地描述操作系统各个部分的接口。Nachos没有用到面向对象语言的所有特征，如继承性、多态性等，所以它的代码就更容易阅读和理解。 3.2 Nachos目录结构 安装了Nachos后可以发现在工作目录下生成一个名为nachos-3.4的目录。该目录中含有：   |  |  |  | | --- | --- | --- | | copyright | 文件 | Nachos的版权信息 | | readme | 文件 | Nachos的readme信息 | | nachos.ps | 文件 | Nachos的介绍文档（Postscript格式） | | c++example | 目录 | 有关C++介绍和实例 | | doc | 目录 | Nachos各个部分介绍和原有的作业要求 | | code | 目录 | Nachos各个部分的源代码 |   最主要的部分是Nachos的源代码部分。它的目录结构是：   |  |  |  | | --- | --- | --- | | Makefile  Makefile.common  Makefile.dep | 文件  文件  文件 | Nachos的Makefile文件。当Nachos需要移植到其它系统时，可以修改Makefile.dep中的HOST参数 | | machine | 目录 | Nachos虚拟机模拟部分源代码 | | threads | 目录 | Nachos线程管理部分源代码 | | filesys | 目录 | Nachos文件系统管理部分源代码 | | userprog | 目录 | Nachos用户程序部分源代码 | | network | 目录 | Nachos网络管理部分源代码 | | vm | 目录 | Nachos虚拟内存管理部分源代码 | | test | 目录 | 一些测试用应用程序 | | bin | 目录 | 包含有用户程序目标码变换的程序 |  3.3 Nachos各个部分的编译运行 Nachos的各个部分都可以独立编译运行，也可以同时编译各个部分。  **全部编译**可以采用如下命令：  ~/nachos-3.4$ make  当需要**单独编译线程管理部分**时，先进入threads目录，然后采用如下命令：  ~/nachos-3.4/threads$ make depend  ~/nachos-3.4/threads$ make nachos  实际上，各部分目录下都有一个Makefile文件，内容大体相同，区别在于一些条件编译的参数。比如在单独编译线程管理部分时，文件管理部分就被屏蔽了，这样读者读者就可以专心于线程管理部分的调试。 3.4 应用程序的编译 由于Linux指令集和R2/3000指令集不同，用户编写的应用程序用Linux系统中标准gcc编译后，不能直接在Nachos虚拟机环境下运行。所以需要采用交叉编译技术。   * 将压缩包 gcc-2.8.1-mips.tar.gz 复制到 ~ (Home，用户主目录) * cd /usr/local * sudo tar -xzvf ~/gcc-2.8.1-mips.tar.gz * 这样就安装好了用于MIPS的交叉编译器   在编译用户程序时，用交叉编译器将源码编译成 R2/3000 指令集的目标代码，再经过一个简单的转换就可以在 Nachos 虚拟机上运行。 四、Nachos虚拟机 Nachos 是建立在**一个软件模拟的虚拟机**上的。该虚拟机包括计算机的基本部分：如 CPU、 主存、寄存器、中断系统，还包括一些外部设备，如终端设备、网络以及磁盘系统。  用软件来模拟硬件另一个优点是充分利用了宿主机操作系统的软件资源，避免了编写复杂的硬件控制程序。更重要的是提高了程序的可移植性，**只要在不同硬件上实现 Nachos 虚拟机就完成了 Nachos 的大部分移植工作。**我们将 Nachos 移植到 Linux 上的工作就受益于这种设计。下面先对Nachos的机器模拟部分做简单介绍：   * Machine类：模拟计算机主机。 * Interrupt类：用来模拟硬件中断系统。在这个中断系统中，定义了中断状态、中断类型、机器状态。中断系统提供的功能有开/关中断，读/写机器状态， 将一个即将发生中断放入中断队列，以及使机器时钟前进一步。 * 在Interrupt类中有一个记录即将发生中断的队列，称为**中断等待队列**。中断等待队列中每个等待处理的中断包含中断类型、中断处理程序的地址及参数、中断应当发生的时间等信息。 一般是由**硬件设备模拟程序**把将要发生的中断放入中断队列。 * 在这个中断系统基础上，Nachos 模拟了各种硬件设备，这些设备都是异步设备，依靠中断来与主机通信。   + Timer 类模拟定时器。定时器每隔 X 个时钟周期就向CPU发一个时钟中断。它是时间片管理必不可少的硬件基础。   + Console类模拟的是控制台设备。   + Disk类模拟了物理磁盘，它一次只能接受一个读写请求，当读写操作完成后向 CPU 发一个磁盘中断。   中断系统成为整个 Nachos 虚拟机的基础，其它的模拟硬件设备都是建立在中断系统之上的。在此之上，加上Machine 类模拟的指令解释器，可以实现 Nachos 的线程管理、文件系统管理、虚拟内存、用户程序和网络管理等所有操作系统功能。  image-20211130142735888  **Nachos与主机操作系统**的关系如图，可以看到Nachos建立在用户主机操作系统(Linux之上)：  image-20211130142955917 4.1 Machine分析 Machine类用来模拟计算机主机。它提供的功能有：读写寄存器。读写主存、运行一条用户程序的汇编指令、运行用户程序、单步调试用户程序、显示主存和寄存器状态、将虚拟内存地址转换为物理内存地址、陷入 Nachos 内核等等。  Machine 类实现方法是在宿主机上分配两块内存分别作为虚拟机的寄存器和物理内存。运行用户程序时，先将用户程序从 Nachos 文件系统中读出，写入模拟的物理内存中，然后调用 指令模拟模块对每一条用户指令解释执行。将用户程序的读写内存要求，转变为对物理内存地址的读写。  Machine类提供了单步调试用户程序的功能，执行一条指令后会自动停下来， 让用户查看系统状态，不过这里的单步调试是汇编指令级的，需要读者对 R2/3000 指令比较 熟悉。如果用户程序想使用操作系统提供的功能或者发出异常信号时，Machine 调用系统异常陷入功能，进入 Nachos 的核心部分。 4.2 Interrupt分析 中断模块的主要作用是**模拟计算机底层的中断机制**。可以通过该模拟机制来启动和禁止中断 (SetLevel)；该中断机制模拟了 Nachos 系统需要处理的所有的中断，包括时钟中断、磁盘中断、终端读/终端写中断以及网络接收/网络发送中断。中断模块定义在machine/interrupt.cc与machine/interrupt.h中  中断的发生总是有一定的时间。比如当向硬盘发出读请求，硬盘处理请求完毕后会发生中断； 在**请求和处理完毕之间需要经过一定的时间**。所以在该模块中，模拟了时钟的前进。为了实现简单和便于统计各种活动所占用的时间起见，Nachos 规定**系统时间**在以下三种情况下前进：   * **执行用户态指令**：执行用户态指令，时钟前进是显而易见的。我们认为，Nachos 执行每条指令所需时间是固定的，为一个时钟单位Tick。 * **重新打开中断**：一般系统态在进行中断处理程序时，**需要关中断**。但是中断处理程序本身也需要消耗时 间，而在关闭中断到重新打开中断之间无法非常准确地计算时间，所以当中断重新打开的时候，加上一个中断处理所需时间的平均值。 * **就绪队列中没有进程**：当系统中没有就绪进程时（进程全部处于等待状态），系统处于Idle状态。这种状态可能是系统中所有的进程都在**等待**各自的某种操作完成。也就是说，系统将在未来某个时间发生中断，到中断发生的时候中断处理程序将进行中断处理。在系统模拟中，有一个**中断等待队列**，专门存放将来发生的中断。 * 在这种情况下，可以将系统时间直接跳到中断等待队列第一项所对应的时间，（将来一定会发生第一项所对应的中断）以免不必要的等待。   当**前面两种情况**需要时钟前进时，调用 OneTick方法。OneTick方法将系统态和用户态的时间分开进行处理：  void Interrupt::OneTick() {  MachineStatus old = status;   // advance simulated time  if (status == SystemMode) {// 系统态  stats->totalTicks += SystemTick;  stats->systemTicks += SystemTick;  } else {// 用户态  stats->totalTicks += UserTick;  stats->userTicks += UserTick;  }  ......  ......  }  **中断等待队列**是 Nachos 虚拟机最重要的数据结构之一，它记录了当前虚拟机可以预测的将在未来发生的所有中断。当系统进行了某种操作可能引起未来发生的中断时，如磁盘的写入、 向网络写入数据等都会将中断插入到中断等待队列中.  对于一些定期需要发生的中断，如时钟中断、终端读取中断等，系统会在中断处理后将下一次要发生的中断插入到中断等待队列中。中断的插入过程是一个优先队列的插入过程，其**优先级是中断发生的时间**，也就是说， 先发生的中断将优先得到处理。  中断处理程序是在某种特定的中断发生时被调用。  Interrupt.h中首先声明了一些预定义枚举变量：   * 包括是否开中断： * // Interrupts can be disabled (IntOff) or enabled (IntOn) enum IntStatus { IntOff, IntOn }; * Nachos 操作系统运行的三种状态： * // Nachos can be running kernel code (SystemMode), user code (UserMode), // or there can be no runnable thread, because the ready list is empty (IdleMode). enum MachineStatus {IdleMode, SystemMode, UserMode};   + IdleMode： **系统 CPU 处于空闲状态，没有就绪线程可以运行。**如果中断等待队列中有需要处理的除了时钟中断以外的中断，说明系统还没有结束，将时钟调整到发生中断的时间，进行中断处理；否则认为系统结束所有的工作，**退出关机**。   image-20211130152119814   * + SystemMode ：Nachos 执行系统程序。Nachos 虽然模拟了虚拟机的内存，**但是 Nachos 系统程序本身的运行不是在该模拟内存中，而是利用宿主机的存储资源。**这是 Nachos 操作系统同真正操作系统的重要区别。   + UserMode ：系统执行用户程序。当执行用户程序时，每条指令占用空间是 Nachos 的模拟内存。 * Nachos需要处理的中断种类： * // IntType records which hardware device generated an interrupt. // 时钟中断、 磁盘（读/写）中断、终端写中断、终端读终端、网络发送中断、网络接收中断 enum IntType { TimerInt, DiskInt, ConsoleWriteInt, ConsoleReadInt,   NetworkSendInt, NetworkRecvInt};  （1）PendingInterrupt类 class PendingInterrupt {  public:  PendingInterrupt(VoidFunctionPtr func, \_int param, int time, IntType kind);  // initialize an interrupt that will occur in the future  VoidFunctionPtr handler; // 中断发生时对应的中断处理程序函数  \_int arg; // 中断处理函数的参数  int when; // 中断发生的时机  IntType type; // for debugging 中断类型 };  这个类定义了一个**中断等待队列中**需要处理的中断的数据结构。为了方便起见，所有类的数据和成员函数都设置为 public 的，不需要其它的 Get 和 Set 等存取内部数据的函数。初始化函数就是为 对应的参数赋值。 （2）Interrupt类 Interrupt类定义了模拟的硬件中断，在 Nachpos 中只存在一个Interrupt类对象。 它记录中断是启用还是禁用IntStatus level，中断等待队列List \*pending，系统状态MachineStatus status...  class Interrupt {  private:  IntStatus level; // 中断的开关状态  List \*pending; // 当前系统中等待中断队列  bool inHandler; // 是否正在进行中断处理标志  bool yieldOnReturn; // 中断处理后是否需要正文切换标志  MachineStatus status; // 当前虚拟机运行状态  bool CheckIfDue(bool advanceClock);// 检查当前时刻是否有要处理的中断  void ChangeLevel(IntStatus old, IntStatus now);// 改变当前中断的开关状态，但是不前进模拟时钟    public:  Interrupt();  ~Interrupt();  IntStatus SetLevel(IntStatus level);// 开关中断，并且返回之前的状态  void Enable(); // 开中断  IntStatus getLevel() {return level;}// 取回当前中断的开关状态  void Idle(); // 当进程就绪队列为空时，执行该函数  void Halt(); // 退出系统，并打印状态  void YieldOnReturn(); // 设置中断结束后要进行进程切换的标志  MachineStatus getStatus() { return status; }// 返回系统当前的状态  void setStatus(MachineStatus st) { status = st; }// 设置系统当前的状态  void DumpState(); // 调试当前中断队列状态用  void Schedule(VoidFunctionPtr handler, int arg, int when, IntType type);// 在中断等待队列中，增加一个等待中断  void OneTick(); // 模拟时钟前进 };  其中，Schedule 和 OneTick两个方法虽然标明是 public 的，但是除了虚拟机模拟部分以外的其它类方法是不能调用这两个方法的。将它们设置成 public 的原因是因为虚拟机模拟的其它类方法需要直接调用这两个方法。  void Interrupt::Schedule(VoidFunctionPtr handler, \_int arg, int fromNow, IntType type) {  int when = stats->totalTicks + fromNow;  PendingInterrupt \*toOccur = new PendingInterrupt(handler, arg, when, type);   DEBUG('i', "Scheduling interrupt handler the %s at time = %d\n",   intTypeNames[type], when);  ASSERT(fromNow > 0);  pending->SortedInsert(toOccur, when); }  重点分析CheckIfDue与Idle两个后面经常用到的方法  **CheckIfDue(bool advanceClock)**测试当前等待中断队列中是否要有中断发生，并根据不同情况作出不同处理（执行中断），具体过程：   1. 如果有中断，在等待处理的中断队列中取出第一项（最早会发生的中断）  * PendingInterrupt \*toOccur =   (PendingInterrupt \*)pending->SortedRemove(&when);  1. 如果不存在任何中断，返回 **FALSE**。  * if (toOccur == NULL) // no pending interrupts  return FALSE;  1. 如果该中断的发生时机没有到：    * 如果 advanceClock=TRUE，**系统时间 totalTicks 跳到中断将要发生的时间。** 说明中断马上就要发生。    * 如果 advanceClock=FALSE，将取出的中断放回原处，等待将来处理，返回**FALSE**  * if (advanceClock && when > stats->totalTicks) { // advance the clock  stats->idleTicks += (when - stats->totalTicks);  stats->totalTicks = when;  } else if (when > stats->totalTicks) { // not time yet, put it back  pending->SortedInsert(toOccur, when);  return FALSE; }  1. 如果当前的状态是 Idle态（就绪队列里没有线程），**而且取出的中断是时钟中断，同时等待中断队列中没有其它的中断，意味着系统将退出。**但是系统的退出不在这里处理，而是将该中断放回原处，等待以后处理；并返回 **FALSE**。  * if ((status == IdleMode) && (toOccur->type == TimerInt)   && pending->IsEmpty()) {  pending->SortedInsert(toOccur, when);  return FALSE; }  1. **中断发生！**  * inHandler = TRUE; status = SystemMode; // whatever we were doing,  // we are now going to be running in the kernel (\*(toOccur->handler))(toOccur->arg); // 执行中断处理程序 status = old; // restore the machine status inHandler = FALSE; delete toOccur; return TRUE;   Idle()：当就绪队列中没有任何东西时调用的函数。由于为了将一个线程放到就绪队列上，必须运行一些东西，所以唯一要做的就是**将模拟时间提前到下一个预定的硬件中断**（CheckIfDue函数实现），处理在**新的时刻其它需要发生的中断**。如果没有中断，停机退出Nachos。  void Interrupt::Idle() {  DEBUG('i', "Machine idling; checking for interrupts.\n");  status = IdleMode; // 将系统状态调为Idle态  if (CheckIfDue(TRUE)) { // 中断队列上有中断，模拟时间提前到下一个预定的硬件中断,中断处理完后会自动进行上下文切换，将阻塞的线程放到就绪对列中  while (CheckIfDue(FALSE)); // check for any other pending interrupts  yieldOnReturn = FALSE; // since there's nothing in the  // ready queue, the yield is automatic  status = SystemMode;  return; // 返回到调用Sleep()的进程  }    // 没有中断程序，也没有就绪线程，停机  DEBUG('i', "Machine idle. No interrupts to do.\n");  printf("No threads ready or runnable, and no pending interrupts.\n");  printf("Assuming the program completed.\n");  Halt();// 停机函数 } 4.3 Timer分析 该模块的作用是**模拟时钟中断**。Nachos 虚拟机可以如同实际的硬件一样，每隔一定的时间会发生一次时钟中断。时钟中断间隔由 TimerTicks宏决定（100 倍 Tick 的时间）。  这是一个可选项，原始的 Nachos 还没有充分发挥时钟中断的作用，只有在Nachos **指定线程随机切换时（Nachos -rs 参数**，见线程管理部分Nachos 主控模块分析） 启动时钟中断，**在每次的时钟中断处理的最后，加入了线程的切换**。实际上，时钟中断的作用远不止如此，但Nachos还未实现以下方法：   * 线程管理中的时间片轮转法的时钟控制，（详见线程管理系统中的实现实例中，对线程调度的改进部分）不一定每次时钟中断都会引起线程的切换，而是由该线程是否的时间 片是否已经用完来决定。 * 分时系统线程优先级的计算（详见线程管理系统中的实现实例中，对线程调度的改进部分） * 线程进入睡眠状态时的时间计算 可以通过时钟中断机制来实现 sleep 系统调用，在时钟中断处理程序中，每隔一定的时 间对定时睡眠线程的时间进行一次评估，判断是否需要唤醒它们。   timer.h 类定义如下所示：  class Timer {  private:  bool randomize; // 是否需要随机时钟中断标志  VoidFunctionPtr handler; //时钟中断处理函数  \_int arg; // 处理函数参数  public:  Timer(VoidFunctionPtr timerHandler, \_int callArg, bool doRandom);// 初始化时钟，每个时间片调用timerHandler时钟中断处理函数  ~Timer() {}    // 内部调用函数，除Nachos模拟程序其他不调用  void TimerExpired(); //当时钟中断发生时调用  int TimeOfNextInterrupt(); // 计算下一次时钟中断发生的时机 };  timer.cc：  static void TimerHandler(\_int arg) { Timer \*p = (Timer \*)arg; p->TimerExpired(); }  Timer::Timer(VoidFunctionPtr timerHandler, \_int callArg, bool doRandom){  randomize = doRandom;  handler = timerHandler;  arg = callArg;   // 添加第一个时钟中断到等待队列中  interrupt->Schedule(TimerHandler, (\_int) this, TimeOfNextInterrupt(), TimerInt);  }  void Timer::TimerExpired() {  // 添加新的时钟中断到中断等待队列中  interrupt->Schedule(TimerHandler, (\_int) this, TimeOfNextInterrupt(), TimerInt);  // 调用timerHandker中断处理程序  (\*handler)(arg); }  int Timer::TimeOfNextInterrupt() {  if (randomize)  return 1 + (Random() % (TimerTicks \* 2));  else  return TimerTicks; }  Timer类的实现很简单，当生成出一个Timer类的实例时，就设计了一个模拟的时钟中断。 这里考虑的问题是：怎样实现定期发生时钟中断？  在 Timer 的初始化函数中，该时钟中断函数是TimerHandler内部函数（见第 1 行）。为什么不直接用初始化函数中的timerHandler **中断处理函数指针**参数作为中断处理函数呢？  因为我们**不仅要执行该时钟中断的中断函数，还要将新的时钟中断插入到中断等待队列中**，这样 Nachos 就可以定时的收到时钟中断。因此真正的时钟中断处理函数不只是timerHandler函数，我们编写TimerExpired()函数表示这个过程，**但C++不允许指针指向类成员函数**，因此借用TimerHandler内部函数调用TimerExpired()方法。  TimeOfextInterrupt()方法的作用是**计算下一次时钟中断发生的时机**，如果需要时钟中断发生的时机是随机的，可以在 Nachos 命令行中设置 –rs 选项。这样，Nachos 的线程切换的时机将会是随机的。但是此时时钟中断则不能作为系统计时的标准了。 4.4 Nachos控制台与统计信息 Console 类模拟的是控制台设备。该模块的作用是模拟实现终端的输入和输出。包括两个部分，即键盘的输入和显示输出。终端输入输出的模拟是异步的，也就是说当发出终端的输入输出请求后系统即返回，需要等待中断发生后才是真正完成了整个过程。  class Console {  public:  Console(char \*readFile, char \*writeFile, VoidFunctionPtr readAvail,   VoidFunctionPtr writeDone, int callArg);// 初始化方法  // readAvail: 键盘读入中断处理函数  // WriteDonel: 显示输出中断处理函数  ~Console(); // 析构方法  void PutChar(char ch); // 将字符 ch 向终端上输出  char GetChar(); // 从终端上读取一个字符  void WriteDone(); // 写终端中断时调用  void CheckCharAvail(); // 读终端中断时调用  private:  int readFileNo; // 模拟键盘输入的文件标识符  int writeFileNo; // 模拟显示器的文件标识符  VoidFunctionPtr writeHandler; // 写中断处理函数  VoidFunctionPtr readHandler; // 读中断处理函数  int handlerArg; // 中断处理函数参数  bool putBusy; // 正在写终端标志  char incoming; // 读取终端字符的暂存空间 };  Nachos 的终端模拟借助了两个文件，即在生成函数Console()中的 readFile 和 writeFile。这两个文件分 别模拟键盘输入和屏幕显示。  对 Nachos 运行情况进行统计的类 stats。这并不属于机器模拟的一部分，但是为了了解自己设计的操作系统的各种运行情况。 stats 类中包含的各种统计项是非常有价值的。Statistics 类的定义和实现如下：  class Statistics {  public:  int totalTicks; // Nachos 运行的时间  int idleTicks; // Nachos 在 Idle 态的时间  int systemTicks; // Nachos 在系统态运行的时间  int userTicks; // Nachos 在用户态运行的时间  int numDiskReads; // Nachos 发出的读磁盘请求次数  int numDiskWrites; // Nachos 发出的写磁盘请求次数  int numConsoleCharsRead; // Nachos 读取的终端字符数  int numConsoleCharsWritten; // Nachos 输出的字符数  int numPageFaults; // 页转换出错陷入次数  int numPacketsSent; // 向网络发送的数据包数  int numPacketsRecvd; // 从网络接收的数据包数  Statistics(); // 初始化方法，将所有的统计信息值都置 0  void Print(); // 系统结束时，打印统计信息 };   Statistics::Statistics() {  totalTicks = idleTicks = systemTicks = userTicks = 0;  numDiskReads = numDiskWrites = 0;  numConsoleCharsRead = numConsoleCharsWritten = 0;  numPageFaults = numPacketsSent = numPacketsRecvd = 0; }  //---------------------------------------------------------------------- // Statistics::Print // Print performance metrics, when we've finished everything // at system shutdown. //----------------------------------------------------------------------  void Statistics::Print() {  printf("Ticks: total %d, idle %d, system %d, user %d\n", totalTicks,   idleTicks, systemTicks, userTicks);  printf("Disk I/O: reads %d, writes %d\n", numDiskReads, numDiskWrites);  printf("Console I/O: reads %d, writes %d\n", numConsoleCharsRead,   numConsoleCharsWritten);  printf("Paging: faults %d\n", numPageFaults);  printf("Network I/O: packets received %d, sent %d\n", numPacketsRecvd,   numPacketsSent); } 4.5 Nachos Disk分析 将会放在文件系统的分析中 五、Nachos启动分析 Nachos的主控模块是整个Nachos系统的入口，包括main.cc,system.cc,system.h等，如其他操作系统一样，Nachos 内核也是操作系统的一部分。最小的 Nachos 内核仅包含 Nachos 线程管理，可以在 threads 目录中编译生成。  Nachos 内核组成包括：   * 一个CPU调度器 * 一个中断模拟器 * 一个时钟模拟器 * 统计信息模块 * 至少一个内核线程(main线程)   system.h中定义了Nachos这些内核组件的**全局变量**，并且导出到整个项目中：  extern void Initialize(int argc, char \*\*argv); // Initialization,  // called before anything else extern void Cleanup(); // Cleanup, called when  // Nachos is done.  extern Thread \*currentThread; // 当前CPU中运行的线程 extern Thread \*threadToBeDestroyed; // 刚调用finish()的线程 extern Scheduler \*scheduler; // 线程调度器 extern Interrupt \*interrupt; // 中断模拟 extern Statistics \*stats; // 统计性能信息 extern Timer \*timer; // 时钟中断硬件模拟  //根据定义不同的宏，声明一些特殊的全局变量： #ifdef USER\_PROGRAM #include "machine.h" extern Machine\* machine; // user program memory and registers #endif  #ifdef FILESYS\_NEEDED // FILESYS or FILESYS\_STUB  #include "filesys.h" extern FileSystem \*fileSystem; #endif  #ifdef FILESYS #include "synchdisk.h" extern SynchDisk \*synchDisk; #endif  #ifdef NETWORK #include "post.h" extern PostOffice\* postOffice; #endif  system.cc中实现了Initialize(argc,argv)函数，该函数在main.cc中被调用。  主要作用：**初始化Nachos全局数据结构。解释处理Nachos启动命令行参数，以确定初始化的标志**：   * argc："argc"是命令行参数的数量(包括命令的名称)——例如："nachos -d +" -> argc = 3 * argv："arqv"是一个字符串数组，每个字符串对应一个命令行参数，例如："nachos -d +" -> argv = {"nachos"， "-d"， "4"}   ./nachos xx(参数) 一般选项： -d: 显示特定的调试信息 -rs: 使得线程可以随机切换 -z: 打印版权信息 和用户进程有关的选项： -s: 使用户进程进入单步调试模式 -x: 执行一个用户程序 -c: 测试终端输入输出 和文件系统有关的选项： -f: 格式化模拟磁盘 -cp: 将一个文件从宿主机拷贝到 Nachos 模拟磁盘上 -p: 将 Nachos 磁盘上的文件显示出来 -r: 将一个文件从 Nachos 模拟磁盘上删除 -l: 列出 Nachos 模拟磁盘上的文件 -D: 打印出 Nachos 文件系统的内容 -t: 测试 Nachos 文件系统的效率 和网络有关的选项： -n: 设置网络的可靠度（在 0-1 之间的一个小数） -m: 设置自己的 HostID -o: 执行网络测试程序  Initialize(argc,argv)代码如下：  void Initialize(int argc, char \*\*argv) {  int argCount;  char\* debugArgs = (char\*)"";  bool randomYield = FALSE;   //定义不同的宏执行不同的局部变量初始化操作  // 例如 #ifdef USER\_PROGRAM  bool debugUserProg = FALSE; // single step user program #endif  // ...    for (argc--, argv++; argc > 0; argc -= argCount, argv += argCount) {  argCount = 1;  if (!strcmp(\*argv, "-d")) {  if (argc == 1)  debugArgs = (char\*)"+"; // turn on all debug flags  else {  debugArgs = \*(argv + 1);  argCount = 2;  }  } else if (!strcmp(\*argv, "-rs")) {  ASSERT(argc > 1);  RandomInit(atoi(\*(argv + 1))); // initialize pseudo-random  // number generator  randomYield = TRUE;  argCount = 2;  }  //定义不同的宏执行不同的命令行解释操作  //例如： #ifdef USER\_PROGRAM  if (!strcmp(\*argv, "-s"))  debugUserProg = TRUE; #endif  // ...   }   DebugInit(debugArgs); // initialize DEBUG messages  stats = new Statistics(); // collect statistics  interrupt = new Interrupt; // start up interrupt handling  scheduler = new Scheduler(); // initialize the ready queue  if (randomYield) // start the timer (if needed)  timer = new Timer(TimerInterruptHandler, 0, randomYield);   threadToBeDestroyed = NULL;   //在内核创建新线程之前，当前运行的线程  currentThread = new Thread("main");  currentThread->setStatus(RUNNING);   interrupt->Enable();  CallOnUserAbort(Cleanup); // if user hits ctl-C    //定义不同的宏执行不同的全局变量初始化操作  //例如： #ifdef USER\_PROGRAM  machine = new Machine(debugUserProg); // this must come first #endif  //... }  在内核创建新线程之前，当前运行的线程就是Initialize()中创建的main线程，他有以下特点：   * 它是由内核模块中的main.cc的main()函数启动的线程。 * 它是作为第一个“运行”线程诞生的。 * 它不是以Fork(func, arg)开始的。因此不遵循ThreadRoot定义的三个阶段。 * 它确实需要一个线程控制块来进行上下文切换。 * 它通过直接调用Finish()来终止自身。   转到main.cc，Nachos 内核main()函数是内核程序的启动入口。可以在threads/main.cc中看到：  int main (int argc, char \*\*argv) {  (void) Initialize(argc, argv);// 初始化内核组件与第一个线程,定义在system.cc中  //一系列预编译指令 main.cc编译在不同的文件夹下执行不同的功能  currentThread -> Finish ();  return (0); // 此行执行不到。 }  **在**main**函数的最后，是**currentThread->Finish()**语句。为什么不直接退出呢？**  这是因为 Nachos 是在宿主机上运行的一个普通的进程，当 main 函数退出时，整个占用的空间要释放，进程也相应的结束。但是实际上在 Nachos 中，**main 函数的结束并不能代表系统的结束**，因为可能还有其它的就绪线程。所以在这里我们只是将 main 函数作为 Nachos 中一个**特殊线程**进行处理，该线程结束只是作为一个线程的结束，系统并不会退出。这个特殊的线程将在上下文切换之后被下一线程删除。当所有线程都终止之后，Nachos 内核将从 Unix/Linux 系统中退出。 六、Nachos Thread分析 **什么是线程，什么是线程和进程之间的不同?**  线程包含于进程中，线程实际上是一个抽象的并发程序执行顺序.属于同一进程的多个线程共享着进程的正文和数据部分、标识以及进程资源。但是每个线程具有各自的寄存器和栈空间。  **为什么我们需要把线程的栈和寄存器分开呢？**  因为栈和寄存器集决定了程序执行中动态上下文的内容。栈保存了函数调用的返回点和传递的参数，而寄存器组保存了当前指令执行后的结果、状态和下条要执行指令的地址。 现在我们就有了一个分级的程序执行的结构：一个系统中可以具有多个进程而且每个进程可以具有多个线程，它们共享着进程的代码、数据、堆、标识和资源。 但进程和线程共享许多相同的概念：   * 状态转换 * 控制块 * 上下文切换   以下我们主要通过 NACHOS 来讨论线程的实现和控制。NACHOS 中的线程是由类Thread定义的。线程控制块是作为线程类中的一部分数据成员来说明的。Thread.h文件定义了Thread结构  #ifndef THREAD\_H #define THREAD\_H  #include "copyright.h" #include "utility.h"  #ifdef USER\_PROGRAM #include "machine.h" #include "addrspace.h" #endif   #define MachineStateSize 18 //存放寄存器指针的最大长度 #define StackSize (sizeof(\_int) \* 1024) // in words // 线程状态 enum ThreadStatus { JUST\_CREATED, RUNNING, READY, BLOCKED }; //外部函数, dummy routine whose sole job is to call Thread::Print extern void ThreadPrint(\_int arg);   class Thread {  private:  int\* stackTop; // 指向整数的指针变量 stackTop 是当前栈顶指针 SP。  \_int machineState[MachineStateSize]; //其他的寄存器包括PC都被存储在数组元素类型为宿主机机器字长的数组中。 machineState[MachineStateSize]数组中  int\* stack; // 指向整数的指针变量 stack 用于存储栈底(对栈溢出做检查)  // NULL if this is the main thread(If NULL, don't deallocate stack)  ThreadStatus status; // 保存了线程的状态：ready, running or blocked  char\* name;  void StackAllocate(VoidFunctionPtr func, \_int arg);  // Allocate a stack for thread Used internally by Fork()   public:  Thread(const char\* debugName); //线程对象的构造函数。仅仅是建立对象的数据结构和将对象状态设置为 JUST\_CREATED。  ~Thread(); // deallocate a Thread  // NOTE -- thread being deleted  // must not be running when delete is called   // basic thread operations 线程状态转换控制原语  void Fork(VoidFunctionPtr func, \_int arg); // Make thread run (\*func)(arg)  void Yield(); // Relinquish the CPU if any other thread is runnable  void Sleep(); // Put the thread to sleep and relinquish the processor  void Finish(); // The thread is done executing    void CheckOverflow(); // 检查该进程的栈是否溢出  void setStatus(ThreadStatus st) { status = st; }  char\* getName() { return (name); }  void Print() { printf("%s, ", name); } };  下面是定义在Theard.h中的线程状态转换控制原语，这些函数的具体实现在Thread.cc中。  需要说明的是，很多函数执行部分都用IntStatus oldLevel = interrupt->SetLevel(IntOff)与(void) interrupt->SetLevel(oldLevel)包裹起来，这两条语句的作用分别是关闭中断，保存原中断状态与恢复中断状态。interrupt是保存在system.h中的一个全局指针变量，这样做的原因是Nachos是**单线程操作系统**，保证函数执行的部分能是**原子操作**（所谓原子操作是指不会被线程调度机制打断的操作；这种操作一旦开始，就一直运行到结束，中间不会有任何 context switch （切换到另一个线程））   * Thread()是线程对象的构造函数。它仅仅是建立对象的数据结构和将对象状态设置为JUST\_CREATED。 * Thread::Thread(const char\* threadName) {  name = (char\*)threadName;  stackTop = NULL;  stack = NULL;  status = JUST\_CREATED; } * Fork()用于产生线程状态从JUST\_CREATE到READY 的状态转换，并生成线程实例可运行的环境。 * void Thread::Fork(VoidFunctionPtr func, \_int arg) {  StackAllocate(func, arg);   IntStatus oldLevel = interrupt->SetLevel(IntOff);//关闭中断  scheduler->ReadyToRun(this); //调用线程调度器的ReadyToRun,assumes that interrupts are disabled!  (void) interrupt->SetLevel(oldLevel);//恢复中断状态 } * Fork中调用了StackAllcate(func, arg)方法，用于分配栈空间同时初始化machineState[]数组 * void Thread::StackAllocate (VoidFunctionPtr func, \_int arg) {  stack = (int \*) AllocBoundedArray(StackSize \* sizeof(int));  stackTop = stack + StackSize - 4; // -4 to be on the safe side!   machineState[PCState] = (\_int) ThreadRoot;//设置PC指针，使得每个线程从ThreadRoot开始运行  machineState[StartupPCState] = (\_int) InterruptEnable;  machineState[InitialPCState] = (\_int) func;  machineState[InitialArgState] = arg;  machineState[WhenDonePCState] = (\_int) ThreadFinish; } * ThreadRoot 是一个定义在switch.s中的汇编语言函数，它是**每个线程首次执行时调用的过程**。 * 当新线程被调上 CPU 时，要用 SWITCH 函数切换线程，SWITCH 函数返回时，会从栈顶取出返回地址，**于是将 ThreadRoot 放在栈顶，在 SWITCH 结束后就会立即执行 ThreadRoot 函数。**ThreadRoot 是所有线程的入口，它会调用 Fork 的两个参数，运行用户指定的函数； * InterruptEnable和ThreadFinish是 定 义 在thread.cc中 的 两 个 静 态 函 数 ， InterruptEnable用 于 打 开 中 断 ，ThreadFinish用于终止线程的执行。func 是**传入的线程执行函数入口地址（类比simpleThread函数）**， arg 是 func 所携带的参数，它俩都是由 Fork 函数的参数传递过来的。 * Yield()：**用于本线程放弃CPU转到就绪队列。**当就绪队列非空时将**当前调用的线程**状态从RUNNING转换为READY。它将当前进程（即调用 Yield 的线程）放入就绪队列尾部并且通过上下文切换将就绪队列中的一个线程变为运行状态。如果就绪队列为空，它没有任何作用并且继续运行当前线程。 * image-20211206144147470 * void Thread::Yield () {  Thread \*nextThread;  IntStatus oldLevel = interrupt->SetLevel(IntOff);//关中断    ASSERT(this == currentThread);//其他线程不能调用另一个线程的yield()，只能自己放弃执行    DEBUG('t', "Yielding thread \"%s\"\n", getName());  //先寻找下一个线程再将自己推到ready队列中，保证不会切换到自己  nextThread = scheduler->FindNextToRun();//利用线程调度器寻找下一个要执行的线程  if (nextThread != NULL) {  scheduler->ReadyToRun(this);// 将原线程放在等待队列中  scheduler->Run(nextThread);// 调用run方法切换到nextThread线程  }  (void) interrupt->SetLevel(oldLevel);//恢复中断优先级 } * Sleep()：。Sleep 方法可以使当前线程转入阻塞态，并放弃 CPU，直到被另一个线程唤醒，把它放回就绪线程队列。在没有就绪线程时，就把时钟前进到一个中断发生的时刻，让中断发生并处理此中断，这是因为在没有线程占用 CPU 时，只有中断处理程序可能唤醒一个线程，并把它放入就绪线程队列。线程要等到本线程被唤醒后，并且又被线程调度模块调上 CPU 时，才会从 Sleep 函数返回。 * 具体来说就是将调用者线程从RUNNING转变为BLOCKED，并从就绪队列中切换一个线程为运行。如果就绪队列为空，CPU 状态将变为空闲，直到有一个就绪线程要运行。 * Sleep()通常用于当线程开始 I/O 请求或要等待某个事件，它不能继续向前推进需要等待 I/O 完成或事件发生。**在调用这个函数之前，线程通常将自己放入对应的I/O等待或事件有关的队列中**。 * image-20211206144206906 * void Thread::Sleep () {  Thread \*nextThread;    ASSERT(this == currentThread);//保证自己调用Sleep  ASSERT(interrupt->getLevel() == IntOff);    DEBUG('t', "Sleeping thread \"%s\"\n", getName());   status = BLOCKED;  while ((nextThread = scheduler->FindNextToRun()) == NULL)  interrupt->Idle(); // no one to run, wait for an interrupt    scheduler->Run(nextThread); // returns when we've been signalled } * Finish()用于终止一个线程，实际上线程调用后会**不会删除自身(C++无法delete this)**，而是进入睡眠状态，直到下一个线程在**上下文切换**后负责销毁该线程。 * void Thread::Finish () {  (void) interrupt->SetLevel(IntOff);   ASSERT(this == currentThread);    DEBUG('t', "Finishing thread \"%s\"\n", getName());    threadToBeDestroyed = currentThread;//将当前运行的线程的指针保存在一个全局变量中，下一个线程负责Destory该线程  Sleep(); // invokes SWITCH  // not reached } * 全局变量threadToDestoryed保存在system.h中 * extern Thread \*threadToBeDestroyed; // the thread that just finished * 要删除的线程声明它应该被删除，通过设置全局变量threadToBeDestroyed来指向自己。接下来，这个线程将控制权转移给另一个线程。新线程在Run方法中删除要删除的控件。  七、Nachos Schedule分析 一个线程或进程在他们的生命期间将通过许多次状态切换。在所有这些状态中**就绪队列**用于放置所有就绪状态的线程或进程。 其他队列对应的放置在因为申请不同 I/O 设备而处于阻塞状态的进程或线程，它们等待响应 I/O 请求的完成。线程或进程由**作业调度者**在队列中按调度策略移动。  在**Nachos**中，线程调度是由定义在scheduler.h和scheduler.cc的Scheduler类的一个全局对象来完成的。这个类的方法提供了线程和进程的所有调度功能。当 Nachos 首次启动时，首先在system.h建立一个Scheduler类的全局实例对象的引用\*scheduler,由它负责完成线程或进程的调度任务。这个类的定义见 scheduler.h文件。  extern Scheduler \*scheduler; // the ready list  下面是对Scheduler类的分析：  class Scheduler {  public:  Scheduler(); // Initialize list of ready threads   ~Scheduler(); // De-allocate ready list   void ReadyToRun(Thread\* thread); // Thread can be dispatched.  Thread\* FindNextToRun(); // Dequeue first thread on the ready   // list, if any, and return thread.  void Run(Thread\* nextThread); // Cause nextThread to start running  void Print(); // Print contents of ready list    private:  List \*readyList; // queue of threads that are ready to run,  // but not running };  Scheduler类仅有一个私有对象它就是指向list对象的一个指针（见 list.h 和 list.cc）。readyList存放着所有status = READY的线程，可以将其理解为一个就绪队列。   * ReadyToRun(Thread\* thread)：将一个线程推入该队列尾 * void Scheduler::ReadyToRun (Thread \*thread) {  DEBUG('t', "Putting thread %s on ready list.\n", thread->getName());   thread->setStatus(READY);  readyList->Append((void \*)thread);// nachos默认实现先来先服务的调度 } * FindNextToRun()：从队列返回出队线程的**指针**（或 NULL,如果队列为空）。 * Thread\* Scheduler::FindNextToRun () {  return (Thread \*)readyList->Remove(); } * run(Thread\* thread)：这个函数调用汇编语言函数SWITCH(Thread\*,Thread\*)将当前线程切换到由第二参数指向的另一线程。 * 函数Scheduler::Run(Thread \*nextThread)首先将currentThread保存到变量oldThread中并将currentThread指向nextThread所指向的线程对象。然后**调用汇编函数**SWITCH(oldThread, nextThread)**真正实现当前运行线程的切换。** * void Scheduler::Run (Thread \*nextThread) {  Thread \*oldThread = currentThread;  oldThread->CheckOverflow(); // check if the old thread  // had an undetected stack overflow  currentThread = nextThread; // currentThread切换到下一个线程  currentThread->setStatus(RUNNING); // 设置新线程的状态为RUNNING    DEBUG('t', "Switching from thread \"%s\" to thread \"%s\"\n",  oldThread->getName(), nextThread->getName());   SWITCH(oldThread, nextThread); // oldThread会进入等待状态，已经切换到nextThread  // 线程中执行，oldThread需要等待其他线程的SWITCH   DEBUG('t', "Now in thread \"%s\"\n", currentThread->getName());  if (threadToBeDestroyed != NULL) {//由新的线程销毁记录在threadToBeDestroyed的线程  delete threadToBeDestroyed;  threadToBeDestroyed = NULL;  } }   **整个**Run**函数运行于内核，因为它属于**Nachos**内核进程。**  注意调用Run函数的oldThread线程它不会立即返回，实际上它将**不会自动返回**，而是进入等到状态，**此时系统已经开始执行**nextThread**新线程，直到有系统调度事件发生其他线程调用**run(oldThread)**后才可能被切换回来再次成为当前线程继续运行。** 八、Nachos Semaphore分析8.1 Nachos Semaphore 一个 Nachos 中的信号量是作为Semaphore 类的对象实现的。Semaphore 类的定义可 以在 threads/synch.h 中找到。其算法可以描述为：  P(){  While(信号量的值 V=0)  将调用者线程推入阻塞队列 B，调用者线程阻塞；  V = V-1 } V(){  If (阻塞队列B非空){  从阻塞队列B中取出一个线程；  把它推入系统就绪队列R；  }  V = V+1; }  Semaphore 类的定义如下：  class Semaphore {  public:  Semaphore(const char\* debugName, int initialValue); // set initial value  ~Semaphore(); // de-allocate semaphore  char\* getName() { return name;} // debugging assist    void P(); // these are the only operations on a semaphore  void V(); // they are both \*atomic\*    private:  char\* name; // useful for debugging  int value; // 资源可利用量, always >= 0  List \*queue; // threads waiting in P() for the value to be > 0 queue  };  Semaphore::Semaphore(const char\* debugName, int initialValue) {  name = (char\*)debugName;  value = initialValue;  queue = new List; } Semaphore::~Semaphore() {  delete queue; }  void Semaphore::P() {  IntStatus oldLevel = interrupt->SetLevel(IntOff); // disable interrupts    while (value == 0) { // semaphore not available  queue->Append((void \*)currentThread); // 将当前线程加入阻塞队列  currentThread->Sleep();  }   value--; // semaphore available, consume its value    (void) interrupt->SetLevel(oldLevel); // re-enable interrupts }  void Semaphore::V() {  Thread \*thread;  IntStatus oldLevel = interrupt->SetLevel(IntOff);   thread = (Thread \*)queue->Remove();  if (thread != NULL) // make thread ready, consuming the V immediately  scheduler->ReadyToRun(thread);  value++;  (void) interrupt->SetLevel(oldLevel); }  每个信号量维护一个队列queue用于指向所有在该信号量上阻塞的线程。name表示当前信号量的名称，value表示当前信号量的信号值。  **PV操作都要保证为原子操作。**因此都需要开关中断。Nachos 中的 P()、V()操作关键的概念是保持信号量的信号值始终大于等于 0。即信号量的值代表了资源可利用量，当资源量等于 0 时说明线程无资源可用必需等待可用资源的释放。  如果在使用 while 语句的地方使用了 if 语句，一些条件可能引起信号量的值小于 0，从而发生错误。   1. 线程 A 因请求该资源，引用 P()操作而阻塞； 2. 线程 B 释放该资源，引用 V()操作唤醒了线程 A，将 A 推入了就绪队列，使 V=1； 3. 线程 C 首先从就绪队列中被选中执行，C 也请求该资源，引用 P()操作，使 V=0；开始访问该资源； 4. 线程 A 从就绪队列中被选中执行，如果这里使用 if 语句，线程 A 不会再去判断 V 是否等于 0,而是使 V=-1，也开始访问该资源，从而发生了与线程 C 非互斥 的使用同一资源的错误。而如果这里使用 while 语句，线程 A 会发现 V 再次等于 0,而再次进入阻塞队列，保证了 V 的值始终大于等于 0，从而避免了与线程 C 同时使用同一资源的错误。 5. **由此可见，那些由 V()操作唤醒刚进入就绪队列的线程仍然被当作阻塞态线程，他们还需要进行一次判断信号量的操作，因为它们还未完成它们调用 P()操作中递减 V 值的工作。**  8.2 ring分析 环形缓冲类定义在ring.h中，包括环形缓冲区的内元素slot——插槽的定义。  class slot {  public:  slot(int id, int number);  slot() { thread\_id = 0; value = 0;};    int thread\_id;  int value; };  slot::slot(int id, int number) {  thread\_id = id;  value = number; }  一个先进先出的环形的缓冲区分别有两个指针in,out：   * in：新的slot放入缓冲区的位置 * out：当前最旧的slot的下标   当缓冲区的已被填满时，第一个插入缓冲区的slot将被下一个新的slot覆盖，达到一个环形的效果，因此缓冲区实时大小为(in-out)%size-1(数组下标从0开始)：   * 判断缓冲区为空：in-out=0 * 判断缓冲区已满：(in+1)%size=out，即out指针在in指针的后一位。   假设siez=12，当in=9，out=10时表示缓冲区已被填满了。  class Ring {  public:  Ring(int sz); // Constructor: sz表示插槽的数量  ~Ring(); // Destructor:   void Put(slot \*message); // Put a message the next empty slot.    void Get(slot \*message); // Get a message from the next full slot.    int Full(); // Returns non-0 if the ring is full, 0 otherwise.  int Empty(); // Returns non-0 if the ring is empty, 0 otherwise.    private:  int size; // 缓冲区内插槽的数量.  int in, out; // Index of   slot \*buffer; // 缓冲区数组，保存插槽  };  Ring::Ring(int sz) {  if (sz < 1) {  fprintf(stderr, "Error: Ring: size %d too small\n", sz);  exit(1);  }   // Initialize the data members of the ring object.  size = sz;  in = 0;  out = 0;  buffer = new slot[size]; //allocate an array of slots. }  Ring::~Ring() {  // Some compilers and books tell you to write this as:  // delete [size] stack;  // but apparently G++ doesn't like that.  delete [] buffer; }   // 将一个新的插槽放入缓冲区的in处 void Ring::Put(slot \*message) {  buffer[in].thread\_id = message->thread\_id;  buffer[in].value = message->value;  in = (in + 1) % size; }  void Ring::Get(slot \*message) {  message->thread\_id = buffer[out].thread\_id;  message->value = buffer[out].value;  out = (out + 1) % size; } int Ring::Empty() {  return in == out; } int Ring::Full() {  return ((in + 1) % size) == out; } 九、Nachos用户程序 重点关注如何实现**从内核线程到用户进程的转化。**  Nachos 用户进程是构建在 Nachos 的线程之上的。回顾一下 Thread 类中有关用户进程的定义：  #ifdef USER\_PROGRAM  int userRegisters[NumTotalRegs]; // user-level CPU register state   public:  void SaveUserState(); // save user-level register state  void RestoreUserState(); // restore user-level register state   AddrSpace \*space; // User code this thread is running. #endif  显示了内核线程有**用于保存用户寄存器的数组和一个内核线程的用户地址空间指针**。重新理解系统线程与用户线程的结构如图：  image-20211213162005351  当你在 userprog 目录中编译时，其中 Makefile 文件定义了 USER\_PROGRAM 标 志。此时以上 124-132 行的代码将会被编译进内核中去。 定义在../userprog/progtest.cc 文件中的函数 StartProcess() 说明了**如何由一个内核线程构造并启动一个用户进程**的过程：  //该参数是在 Nachos 系统启动时由命令行参数传入的 Noff 格式的用户可执行文件名字符串。 void StartProcess(char \*filename) {  //文件系统调用函数Open根据可执行文件名打开要装入的文件  OpenFile \*executable = fileSystem->Open(filename);    AddrSpace \*space;   if (executable == NULL) {  printf("Unable to open file %s\n", filename);  return;  }  //使用这个打开的文件建立和初始化好一个用户进程空间并且返回一个指向该进程空间的指针。  space = new AddrSpace(executable);   currentThread->space = space;   delete executable; // close file   space->InitRegisters(); // set the initial register values  space->RestoreState(); // 保存页表到machine中   // 跳转到用户进程  machine->Run(); // jump to the user progam  ASSERT(FALSE); // machine->Run never returns;  // the address space exits  // by doing the syscall "exit" }  当调用machine->Run()后**当前线程就变成了运行在 MIPS 模拟机上的用户进程**，当然之后的机器工作状态就由系统的核心态转变为用户态。而当用户进程结束时不会返回到Run()函数处，而是依赖于**系统调用exit()**切换回系统态。  **Nachos用户程序的编译：**  实际这些 C 语言编写的用户程序在由gcc MIPS交叉编译后都在前面连接上一个由 MIPS 汇编程序 start.s 生成的叫 start. o 的目标模块。实际上 start 是用户程序真正的启动入口，由它来调用 C 程序的 main 函数。所以不要求用户编程时一定要把 main 函数作为第一个函数。  例如 C 程序 halt.c 被编译为 halt.o，同时 start.s 也被汇编为 start.o。之后两个目标模块被连接成可执行的 Coff 格式的可执行文件，最后这个 Coff 文件又被转换为 Nof f 格式的 Nachos 可执行文件。image-20211213163924269 十、Nachos系统调用 系统调用是用户程序和操作系统内核的接口。用户程序**从系统调用函数取得系统服务**。   * 当 CPU 控制从用户程序切换到系统态时，CPU 的工作方式由用户态改变为系统态。 * 而当内核完成系统调用功能时，CPU 工作状态又从系统态改变回用户态并且将控制再次返回给用户程序。   两种不同的 CPU 工作状态提供了操作系统基本的保护方式。  所有 Nachos 系统调用的接口原型都定义在文件 userprog/syscall.h 中。当编译用户程序时编译器会括入这个文件并取得这些系统调用接口原型的信息  /\* syscalls.h   \* Nachos system call interface. These are Nachos kernel operations  \* that can be invoked from user programs, by trapping to the kernel  \* via the "syscall" instruction.  \*  \* This file is included by user programs and by the Nachos kernel.   \*  \* Copyright (c) 1992-1993 The Regents of the University of California.  \* All rights reserved. See copyright.h for copyright notice and limitation   \* of liability and disclaimer of warranty provisions.  \*/  #ifndef SYSCALLS\_H #define SYSCALLS\_H  #include "copyright.h"  /\* system call codes -- used by the stubs to tell the kernel which system call  \* is being asked for  \*/ #define SC\_Halt 0 #define SC\_Exit 1 #define SC\_Exec 2 #define SC\_Join 3 #define SC\_Create 4 #define SC\_Open 5 #define SC\_Read 6 #define SC\_Write 7 #define SC\_Close 8 #define SC\_Fork 9 #define SC\_Yield 10  #ifndef IN\_ASM  /\* The system call interface. These are the operations the Nachos  \* kernel needs to support, to be able to run user programs.  \*  \* Each of these is invoked by a user program by simply calling the   \* procedure; an assembly language stub stuffs the system call code  \* into a register, and traps to the kernel. The kernel procedures  \* are then invoked in the Nachos kernel, after appropriate error checking,   \* from the system call entry point in exception.cc.  \*/  /\* Stop Nachos, and print out performance stats \*/ void Halt();    /\* Address space control operations: Exit, Exec, and Join \*/  /\* This user program is done (status = 0 means exited normally). \*/ void Exit(int status);   /\* A unique identifier for an executing user program (address space) \*/ typedef int SpaceId;    /\* Run the executable, stored in the Nachos file "name", and return the   \* address space identifier  \*/ SpaceId Exec(char \*name);   /\* Only return once the the user program "id" has finished.   \* Return the exit status.  \*/ int Join(SpaceId id);    /\* File system operations: Create, Open, Read, Write, Close  \* These functions are patterned after UNIX -- files represent  \* both files \*and\* hardware I/O devices.  \*  \* If this assignment is done before doing the file system assignment,  \* note that the Nachos file system has a stub implementation, which  \* will work for the purposes of testing out these routines.  \*/   /\* A unique identifier for an open Nachos file. \*/ typedef int OpenFileId;   /\* when an address space starts up, it has two open files, representing   \* keyboard input and display output (in UNIX terms, stdin and stdout).  \* Read and Write can be used directly on these, without first opening  \* the console device.  \*/  #define ConsoleInput 0  #define ConsoleOutput 1    /\* Create a Nachos file, with "name" \*/ void Create(char \*name);  /\* Open the Nachos file "name", and return an "OpenFileId" that can   \* be used to read and write to the file.  \*/ OpenFileId Open(char \*name);  /\* Write "size" bytes from "buffer" to the open file. \*/ void Write(char \*buffer, int size, OpenFileId id);  /\* Read "size" bytes from the open file into "buffer".   \* Return the number of bytes actually read -- if the open file isn't  \* long enough, or if it is an I/O device, and there aren't enough   \* characters to read, return whatever is available (for I/O devices,   \* you should always wait until you can return at least one character).  \*/ int Read(char \*buffer, int size, OpenFileId id);  /\* Close the file, we're done reading and writing to it. \*/ void Close(OpenFileId id);  /\* User-level thread operations: Fork and Yield. To allow multiple  \* threads to run within a user program.   \*/  /\* Fork a thread to run a procedure ("func") in the \*same\* address space   \* as the current thread.  \*/ void Fork(void (\*func)());  /\* Yield the CPU to another runnable thread, whether in this address space   \* or not.   \*/ void Yield();   #endif /\* IN\_ASM \*/  #endif /\* SYSCALL\_H \*/  对应的系统调用的汇编语言存根在 test/start.s 文件中的 45-131 行。**如果你要添加你自己的系统调用，就应当首先在** syscall.h **和** start.s **中声明你的系统调用原型和存根**  当一个系统调用由一个用户进程发出时，由汇编语言编写的对应于存根的程序就被执行。然后，这个存根程序会由执行一个系统调用指令而引发一个**异常或自陷**处理该系统调用。 在 start.s 中的这些系统调用的接口程序代码都是一样的。即：   * 将对应的系统调用的编码送$2寄存器 * 执行系统调用指令 SYSCALL * 返回到用户程序   Halt:  addiu $2,$0,SC\_Halt  syscall  j $31  .end Halt   .globl Exit  .ent Exit  Nachos中的异常与自陷  模拟 MIPS 计算机的**异常和自陷管理**的是 Machine 类中的函数 RaiseException(ExceptionType which, int badVAddr)。其中的第一个参数 which 是 一个 ExceptionType 枚举类型的变量。ExceptionType 类型的定义也在 machine/machine.h 文件中：  系统调用是SyscallException类型，MIPS 计算机的”SYSCALL”指令在 Nachos 中是由 machine/mipssim.cc 中 534-536 行上的通过触发系统调用异常模拟的：  case OP\_SYSCALL:  RaiseException(SyscallException, 0);  return;  函 数 RaiseException(ExceptionType which, int badVAddr)的代码在 machine/machine.cc 文件中：  void Machine::RaiseException(ExceptionType which, int badVAddr) {  DEBUG('m', "Exception: %s\n", exceptionNames[which]);  // ASSERT(interrupt->getStatus() == UserMode);  registers[BadVAddrReg] = badVAddr;  DelayedLoad(0, 0); // finish anything in progress  interrupt->setStatus(SystemMode);  ExceptionHandler(which); // interrupts are enabled at this point  interrupt->setStatus(UserMode); }  这个函数模拟硬件的动作，切换到系统态并且在异常处理完成后返回到用户态。 **9行上的** ExceptionHandler(which)**函数调用模拟硬件的动作发一个异常中断到对应的异常处理程序**。这个函数定在 userprog/execution.cc 中：  void ExceptionHandler(ExceptionType which) {  int type = machine->ReadRegister(2);// 寄存器$2存储着系统调用类型   if ((which == SyscallException) && (type == SC\_Halt)) {// 实现系统调用Halt  DEBUG('a', "Shutdown, initiated by user program.\n");  interrupt->Halt();  } else {  printf("Unexpected user mode exception %d %d\n", which, type);  ASSERT(FALSE);  } }  对于系统调用 Halt 的异常处理只是简单的模拟了 Interrupt 类指向的中断函数 Halt()。 | |
| 结论分析与体会：  在本次实验中，首先根据教程安装了nachos开发环境与一些辅助实验的工具，接着对make命令的使用以及makefile的结构进行学习，结合指导教程，学会了在nachos中如何使用make工具对程序代码进行编译。  之后通过阅读nachos的文件结构，对nachos的总体架构有了初步的了解，认识了nachos各部分的功能模块。并对各模块下的源码进行了阅读与分析，重点对timer、interrupt、thread类的源码进行分析，通过阅读代码注释与查阅指导教程的方式，对类中的方法等进行了深入的理解，从而逐步建立了对nachos的中断机制、时钟中断模块、线程切换过程等知识模块的认识，了解了nachos在运行时，各模块的作用以及联系，为后续实验问题的解决提供了一些基础知识。  在进行了部分源码的阅读与分析工作之后，对nachos下CPU指令的执行方式与过程进行了学习，结合上学期操作系统课程中所学习的相关知识，深入了解了线程的各种状态及其切换过程，并对使用gdb进行程序调试的方法进行了熟悉与实践，加强了gdb使用的熟练程度。为整个课设的完成奠定知识基础，便于后续实验的推进。 | |