Magenta操作系统内核

教你研发操作系统

http://elastos.org

同济大学电子与信息工程学院计算机科学与技术系

2016/9

**目录**

[1. 开发环境搭建 1](#_Toc462300977)

[1.1 先试试（Getting Started） 1](#_Toc462300978)

[1.2 在硬件上玩Magenta 1](#_Toc462300979)

[1.2.1 Raspberry Pi 3 1](#_Toc462300980)

[1.2.2 PC x86平台 2](#_Toc462300981)

[1.3 源码树目录结构 2](#_Toc462300982)

[1.4 开源许可证 3](#_Toc462300983)

[2. 基础概念 4](#_Toc462300984)

[2.1 内核对象（Kernel Objects） 4](#_Toc462300985)

[2.1.1 内核对象生命周期 4](#_Toc462300986)

[2.1.2 内核对象实现 5](#_Toc462300987)

[2.1.3 内核对象安全 5](#_Toc462300988)

[2.2 句柄（Capabilities） 5](#_Toc462300989)

[2.2.1 Magenta句柄 6](#_Toc462300990)

[2.2.2 Magenta句柄垃圾回收 8](#_Toc462300991)

[2.2.3 句柄的权限 9](#_Toc462300992)

[2.3 虚拟地址空间（Virtual Address Spaces） 9](#_Toc462300993)

[2.4 线程（Threads） 10](#_Toc462300994)

[2.5 进程间通信（Inter-Process Communication，IPC） 10](#_Toc462300995)

[2.6 设备驱动与中断（Device Drivers and IRQs） 11](#_Toc462300996)

[2.7 抢占（Preemption） 11](#_Toc462300997)

[3. 加电开始 12](#_Toc462300998)

[3.1 lk\_main() 12](#_Toc462300999)

[3.1.1 lk\_main 源码分析 13](#_Toc462301000)

[3.1.2 arch\_early\_init() 13](#_Toc462301001)

[3.1.3 platform\_early\_init() 14](#_Toc462301002)

[3.1.4 bootstrap2 14](#_Toc462301003)

[3.2 Boot程序中的trampoline(弹簧床) 15](#_Toc462301004)

[3.3 起动过程 16](#_Toc462301005)

[4. Magenta内核 18](#_Toc462301006)

[4.1 内核起动地址 18](#_Toc462301007)

[4.2 从内核回用户态 18](#_Toc462301008)

[4.3 内核对象 18](#_Toc462301009)

[4.3.1 Process 19](#_Toc462301010)

[4.3.2 Thread 19](#_Toc462301011)

[4.3.3 Event 20](#_Toc462301012)

[4.3.4 Message pipe 20](#_Toc462301013)

[4.3.5 Interrupt request 20](#_Toc462301014)

[4.3.6 VMObject 20](#_Toc462301015)

[4.3.7 Data pipe 20](#_Toc462301016)

[4.3.8 Job 21](#_Toc462301017)

[4.3.9 IOPort 21](#_Toc462301018)

[4.4 程序加载器Loader 21](#_Toc462301019)

[4.4.1 内核elf-loader 22](#_Toc462301020)

[4.4.2 应用程序加载器 22](#_Toc462301021)

[5. 系统调用 24](#_Toc462301022)

[5.1 svc中断向量 24](#_Toc462301023)

[5.2 内核栈svc stack 24](#_Toc462301024)

[5.3 系统调用在内核侧的实现 26](#_Toc462301025)

[5.4 3.4 系统调用在应用程序侧的实现 27](#_Toc462301026)

[5.4.1 系统调用定义 27](#_Toc462301027)

[5.4.2 用户态与内核态调用者 28](#_Toc462301028)

[5.4.3 动态库libmagenta.so 29](#_Toc462301029)

[5.4.4 应用程序系统调用头文件 30](#_Toc462301030)

[5.4.5 导出系统调用符号 30](#_Toc462301031)

[5.5 用户态与内核态间的参数传递 31](#_Toc462301032)

[6. 线程调度与时间管理 33](#_Toc462301033)

[6.1 当前线程 33](#_Toc462301034)

[6.2 调度器 33](#_Toc462301035)

[6.3 线程优先级管理 34](#_Toc462301036)

[6.4 context切换 35](#_Toc462301037)

[6.5 定时器 37](#_Toc462301038)

[6.6 线程抢先preempt的实现 37](#_Toc462301039)

[7. 内存管理 39](#_Toc462301040)

[7.1 ARM MMU基本原理 39](#_Toc462301041)

[7.2 地址空间布局 40](#_Toc462301042)

[7.2.1 虚拟地址规划 40](#_Toc462301043)

[7.2.2 物理内存管理 41](#_Toc462301044)

[7.3 MMU页表组织 42](#_Toc462301045)

[7.4 物理内存管理 43](#_Toc462301046)

[7.5 虚拟地址管理 43](#_Toc462301047)

[7.6 虚实映射 43](#_Toc462301048)

[8. 中断 45](#_Toc462301049)

[8.1 内核态中断编程 46](#_Toc462301050)

[8.2 用户态中断编程 47](#_Toc462301051)

[8.3 中断程序执行过程 47](#_Toc462301052)

[9. 文件系统 50](#_Toc462301053)

[9.1 内核虚拟文件系统MXIO 50](#_Toc462301054)

[9.1.1 内置文件系统 53](#_Toc462301055)

[10. 设备驱动与管理 55](#_Toc462301056)

[10.1 硬件IO 55](#_Toc462301057)

[10.2 驱动程序 55](#_Toc462301058)

[10.3 设备管理 57](#_Toc462301059)

[10.3.1 设备节点 57](#_Toc462301060)

[10.4 设备管理应用devmgr 58](#_Toc462301061)

[10.5 虚拟文件系统vfs 58](#_Toc462301062)

[10.6 设备树DeviceTree 58](#_Toc462301063)

[11. 编程概念 60](#_Toc462301064)

[11.1 Dispatcher 60](#_Toc462301065)

[11.2 信号Signal 62](#_Toc462301066)

[11.3 内核对象唯一标识值 63](#_Toc462301067)

[11.4 StateTracker/ StateObserver 63](#_Toc462301068)

[11.5 资源Resource 64](#_Toc462301069)

[11.6 异常处理ExceptionPort 64](#_Toc462301070)

[11.7 事件对（EventPair） 65](#_Toc462301071)

[11.8 状态信息status\_t 65](#_Toc462301072)

[11.8.1 Descriptions 66](#_Toc462301073)

[11.8.2 Categories 66](#_Toc462301074)

[12. 编程基础设施 69](#_Toc462301075)

[12.1 mxtl，c++模板 69](#_Toc462301076)

[12.1.1 智能指针 69](#_Toc462301077)

[12.1.2 数据类型支持type\_support 70](#_Toc462301078)

[12.1.3 资源获取即初始化RAII 70](#_Toc462301079)

[12.1.4 容器、链表等 71](#_Toc462301080)

[12.2 内核编程可用程序资源 72](#_Toc462301081)

[12.3 内核堆 73](#_Toc462301082)

[12.3.1 cmpctmalloc 73](#_Toc462301083)

[12.3.2 miniheap 74](#_Toc462301084)

[12.3.3 物理内存申请 74](#_Toc462301085)

[12.3.4 c++ new/delete支持及AllocChecker 74](#_Toc462301086)

[12.4 用户堆/c库 76](#_Toc462301087)

[12.5 互斥机制 76](#_Toc462301088)

[12.5.1 cond 79](#_Toc462301089)

[12.5.2 mutex 79](#_Toc462301090)

[12.5.3 semaphore 79](#_Toc462301091)

[12.5.4 spinlock 80](#_Toc462301092)

[12.5.5 Futexes 82](#_Toc462301093)

[12.6 进程间通信（IPC） 83](#_Toc462301094)

[12.6.1 网络套接字（socket） 83](#_Toc462301095)

[12.7 看门狗（watchdog） 84](#_Toc462301096)

[12.8 调试debug机制 84](#_Toc462301097)

[12.8.1 LTRACEF 84](#_Toc462301098)

[12.8.2 DEBUG\_ASSERT 85](#_Toc462301099)

[12.8.3 DEBUGLOG 86](#_Toc462301100)

[12.8.4 系统控制台console 86](#_Toc462301101)

[12.9 调优profile机制 86](#_Toc462301102)

[12.9.1 THREAD\_STATS 86](#_Toc462301103)

[12.9.2 KTRACE 87](#_Toc462301104)

[12.9.3 KLOG 87](#_Toc462301105)

[12.9.4 内核事件EVLOG（kernel event log） 88](#_Toc462301106)

[12.10 监控运行log机制 89](#_Toc462301107)

[12.10.1 LogDispatcher 89](#_Toc462301108)

[12.10.2 内核诊断信息diagnostics 89](#_Toc462301109)

[13. 调试Magenta 90](#_Toc462301110)

[13.1 用QEMU+gdb调试Magenta 90](#_Toc462301111)

[13.1.1 通过QEMU跑起来Magenta。 90](#_Toc462301112)

[13.1.2 起调试器arm-none-eabi-gdb 90](#_Toc462301113)

[13.1.3 QEMU跑操作系统的第一条指令 91](#_Toc462301114)

[13.1.4 经验总结 92](#_Toc462301115)

[13.2 用 Python 拓展 GDB 92](#_Toc462301116)

[13.2.1 如何用Python 拓展 GDB 92](#_Toc462301117)

[13.2.2 Magenta中的python调试角本 93](#_Toc462301118)

[14. Magenta系统功能调用 95](#_Toc462301119)

[14.1 句柄Handles 95](#_Toc462301120)

[14.1.1 handle\_close 95](#_Toc462301121)

[14.1.2 handle\_duplicate 96](#_Toc462301122)

[14.1.3 handle\_replace 97](#_Toc462301123)

[14.1.4 handle\_wait\_many 98](#_Toc462301124)

[14.1.5 handle\_wait\_one 100](#_Toc462301125)

[14.2 消息管道（Message Pipes） 101](#_Toc462301126)

[14.2.1 msgpipe\_create 101](#_Toc462301127)

[14.2.2 msgpipe\_read 103](#_Toc462301128)

[14.2.3 msgpipe\_write 104](#_Toc462301129)

[14.3 数据管道（Data Pipe） 105](#_Toc462301130)

[14.3.1 datapipe\_create 106](#_Toc462301131)

[14.3.2 datapipe\_read 107](#_Toc462301132)

[14.3.3 datapipe\_begin\_read 109](#_Toc462301133)

[14.3.4 datapipe\_end\_read 111](#_Toc462301134)

[14.3.5 datapipe\_write 112](#_Toc462301135)

[14.3.6 datapipe\_begin\_write 114](#_Toc462301136)

[14.3.7 datapipe\_end\_write 116](#_Toc462301137)

[14.4 IO端口（IO Ports） 117](#_Toc462301138)

[14.4.1 port\_create 117](#_Toc462301139)

[14.4.2 port\_queue 118](#_Toc462301140)

[14.4.3 port\_wait 120](#_Toc462301141)

[14.4.4 port\_bind 121](#_Toc462301142)

[14.5 线程（Threads） 122](#_Toc462301143)

[14.5.1 nanosleep 123](#_Toc462301144)

[14.5.2 thread\_arch\_prctl 123](#_Toc462301145)

[14.5.3 thread\_create 124](#_Toc462301146)

[14.5.4 thread\_exit 125](#_Toc462301147)

[14.5.5 thread\_start 125](#_Toc462301148)

[14.6 进程（Processes） 126](#_Toc462301149)

[14.6.1 process\_create 127](#_Toc462301150)

[14.6.2 process\_start 128](#_Toc462301151)

[14.6.3 process\_map\_vm 130](#_Toc462301152)

[14.6.4 process\_protect\_vm 131](#_Toc462301153)

[14.6.5 process\_unmap\_vm 132](#_Toc462301154)

[14.7 Objects 132](#_Toc462301155)

[14.7.1 object\_signal 132](#_Toc462301156)

[14.8 等待集（Wait Sets） 133](#_Toc462301157)

[14.8.1 waitset\_create 133](#_Toc462301158)

[14.8.2 waitset\_add 134](#_Toc462301159)

[14.8.3 waitset\_remove 135](#_Toc462301160)

[14.8.4 waitset\_wait 136](#_Toc462301161)

[14.9 Events and Event Pairs 138](#_Toc462301162)

[14.9.1 event\_create 138](#_Toc462301163)

[14.9.2 eventpair\_create 139](#_Toc462301164)

[14.10 中断Interrupt 140](#_Toc462301165)

[14.10.1 interrupt\_create 141](#_Toc462301166)

[14.10.2 interrupt\_complete 141](#_Toc462301167)

[14.11 硬件IO（Device Memory） 142](#_Toc462301168)

[14.11.1 mmap\_device\_memory 142](#_Toc462301169)

[14.11.2 alloc\_device\_memory 142](#_Toc462301170)

[14.12 快速用户区互斥futex 142](#_Toc462301171)

[14.12.1 futex\_wait 142](#_Toc462301172)

[14.12.2 futex\_wake 143](#_Toc462301173)

[14.12.3 futex\_requeue 144](#_Toc462301174)

[14.13 Cryptographically Secure RNG 145](#_Toc462301175)

[14.13.1 cprng\_draw 145](#_Toc462301176)

[14.13.2 cprng\_add\_entropy 146](#_Toc462301177)

[14.14 系统运行log 147](#_Toc462301178)

[14.14.1 log\_create 148](#_Toc462301179)

[14.14.2 log\_write 148](#_Toc462301180)

[14.14.3 log\_read 148](#_Toc462301181)

[15. 开发工具链 149](#_Toc462301182)

[15.1 Make文件 149](#_Toc462301183)

[15.2 源代码管理 150](#_Toc462301184)

[16. Magenta深入开发 151](#_Toc462301185)

[17. 问答Q&A 152](#_Toc462301186)

[17.1 程序技术问题 152](#_Toc462301187)

[17.2 高阶逻辑在操作系统开发中的应用 155](#_Toc462301188)

[18. 结语 156](#_Toc462301189)

# 开发环境搭建

## 先试试（Getting Started）

文档：<https://github.com/fuchsia-mirror/magenta/blob/master/docs/getting_started.md>

源码位置：

<https://github.com/fuchsia-mirror/magenta.git>

Travis-Ci持续集成：

<https://travis-ci.org/fuchsia-mirror>

Google内部Gerrit：

<https://fuchsia-review.googlesource.com/#/q/status:open>

## 在硬件上玩Magenta

### Raspberry Pi 3

In order to boot on Raspberry Pi3 you will need an sd card with the following:

config.txt file containing the following:

enable\_uart=1 framebuffer\_depth=16

bootcode.bin and start.elf files. Can be obtainied from here

build armstub8.bin from source that can be found here and copy to sd card

copy the magenta.bin file from you build to the sd card as kernel8.img

serial console is available on the rpi3 header.

Pin 6 - GND

Pin 8 - TXD (output from Pi)

Pin 10 - RXD (input to pi)

Baudrate = 115200

### PC x86平台

## 源码树目录结构

源码：$Magenta/magenta

* kernel
  + app
  + arch：arm、arm64、x86
  + dev：平台内置设备：gpio、timer、intel\_rng
  + include

├── arch

├── dev

├── hw

├── kernel

│   └── vm

├── lib

├── lk

├── platform

└── sys

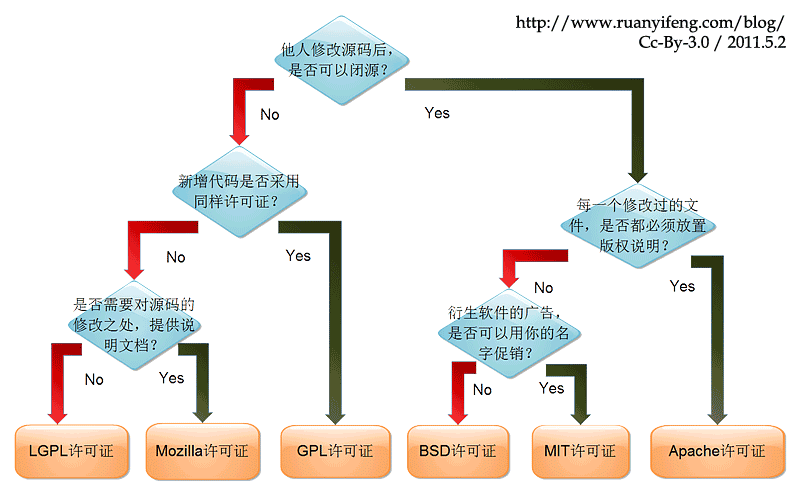
* + kernel：小内核，处理物理内存、线程、定时器，提供seamphore、mutex等。
  + lib：库
  + make：build makefile文件
  + platform：平台：bcm28xx、pc、qemu-virt等
  + project：针对目标板的makefile文件
  + target：目标板
  + top：lk\_init\_level、lk\_main，第0个进程init0程序入口。

总的makefile，包括：lk\_inc.mk、engine.mk

* prebuilt预编译内容
* scripts工作角本
* system
* third\_party第三方库

## 开源许可证

参考：<http://www.ruanyifeng.com/blog/2011/05/how_to_choose_free_software_licenses.html>



# Use of this source code is governed by a MIT-style

# license that can be found in the LICENSE file or at

# https://opensource.org/licenses/MIT

# 基础概念

## 内核对象（Kernel Objects）

操作系统内核提供的功能，很多并不是内核本身提供的，而是跑在内核态的程序提供的，象Linux这样的操作系统的内核，这类内核程序可能是驱动，或以伪驱动形式存在的内核程序。

Magenta中的内核对象是内核向用户程序提供的一组功能集，应用程序眼中的这些内核对象，与内核眼中的这些对象，在接口上是一样的，就是说，服务态程序中看到的这些对象，并没被单独包装过，只是需要通过句柄才能标识这些对象。

每个内核动态数据结构都表述为内核对象，内核并不为这些内核对象分配内存，Magenta一旦起动，内核就不再需要新的内存，所有内存都是在用户态申请的。用户态程序为了申请内存，需要提供原始内存（untyped memory），内存对象最终存储在这个原始内存中。

原始内存无法直接被应用程序访问（access）。

Magenta is a object-based kernel. User mode code almost exclusively interacts with OS resources via object handles which map kernel objects to processes.

Magenta内核对象有如下几种：

* Process
* Thread
* Event
* Message pipe
* Interrupt request
* VMObject
* Data pipe
* Job
* IOPort

### 内核对象生命周期

通过引用计数（ref-counted）方式管理内核对象

Kernel objects are ref-counted. Most kernel objects are born during a syscall and are held alive at refcount = 1 by the handle which binds the handle value given as the output of the syscall. The handle object is held alive as long it is attached to a handle table. Handles are detached from the handle table closing them (for example via sys\_close()) which decrements the refcount of the kernel object. Usually, when the last handle is closed the kernel object refcount will reach 0 which causes the destructor to be run.

The refcount increases both when new handles (referring to the object) are created and when a direct pointer reference (by some kernel code) is acquired; therefore a kernel object lifetime might be longer than the lifetime of the process that created it.

### 内核对象实现

内核对象都继承自分发器Dispatcher，每个具体的对象在基类的基础上，扩充实现自己的功能。

A kernel object is implemented as a C++ class that derives from Dispatcher and that overrides the methods it implements. Thus, for example, the code of the Thread object is found in ThreadDispatcher. There is plenty of code that only cares about kernel objects in the generic sense, in that case the name you'll see is mxtl::RefPtr<Dispatcher>.

### 内核对象安全

Kernel Object security

In principle, kernel objects do not have an intrinsic notion of security and do not do authorization checks; security rights are held by each handle. A single process can have two different handles to the same object with different rights.

## 句柄（Capabilities）

Magenta has a capability-based security model.

Capability概念上类似于句柄（Handle），在操作系统这样的系统软件设计中，有一个可靠性的设计原则，就是下层软件不信任上层软件，而上层软件要无条件信任下层软件。那么，下层软件如何把自己的实现细节隐藏，不让上层软件通过“简单”方法就可以直接操作下层软件的资源呢，句柄是一个常用的设计。

一个句柄指向一个内核对象，内核对象也只能通过与其绑定的句柄来操作它，无法直接访问。大多数的内核对象都有方法，用来操作这个对象的数据结构，就象是c++中的封装中的protect数据结构，方法自身可以访问数据结构中的数据，但是，使用这个对象的其它程序，只能通过API与这个对象打交道。

举例来说，用户来以通过调用一个原始内存untyped-memory 句柄的invoke方法，用来在这个原始内存上创建内核对象。

有些内核对象只有方法，但自身没有什么状态（state）信息，这类对象的目的是为了让应用程序与内核打交道，这类对象没有自身的存储实例。

下面泛义地讨论一下什么是句柄？为什么会有句柄？

句柄是一个概念，Handler是一个句柄，Magenta中的Capability也是一个句柄，打开文件，fopen得到的那个FILE \*，open得到的那个int都是句柄。

从广义上，能够从一个数值（或数据结构）拎起一大堆数据的东西都可以叫做句柄。句柄的英文是“Handle”，本义就是“柄”，只是在计算机科学中，被特别地翻译成“句柄”，其实还是个“柄”。从一个小东西拎起一大堆东西，这难道不像是个“柄”吗？

然后，指针其实也是一种“句柄”，只是由于指针同时拥有更特殊的含义——实实在在地对应内存里的一个地址——所以，通常不把指针说成是“句柄”。但指针也有着能从一个32位的值（在32位硬件平台上）引用到一大堆数据的作用，这不是句柄又是什么？

一个操作系统中，可能有许多内核对象（这里的对象不完全等价于“面向对象程序设计”一词中的“对象”，虽然实质上还真差不多），比如打开的文件，创建的线程，程序的窗口，等等。这些重要的对象肯定不是4个字节或者8个字节足以完全描述的，他们拥有大量的属性。为了保存这样一个“对象”的状态，往往需要上百甚至上千字节的内存空间，那么怎么在程序间或程序内部的子过程（函数）之间传递这些数据呢？拖着这成百上千的字节拷贝来拷贝去吗？显然会浪费效率。那么怎么办？当然传递这些对象的首地址是一个办法，但这至少有两个缺点：

* 暴露了内核对象本身，使得程序（而不是操作系统内核）也可以任意地修改对象的内部状态（首地址都知道了，还有什么不能改的？），这显然是操作系统内核所不允许的。上面不是已经介绍过操作系统的可靠性设计原则了吗？
* 操作系统有定期整理内存的责任，如果一些内存整理过一次后，对象被搬走了怎么办？

Magenta提供了基于句柄的访问控制（Capability-based Access Control）机制，访问控制掌控着所有对内核的访问。用户态程序，必须有足够的权限，通过访问它自己拥有的句柄来发出请求（invoke）。通过这个机制，系统使得软件构件间得以隔离，并且允许审计、控制构件间的通信，手段就是有选择地授权特定的通信句柄。这个机制使得软件构件在更高层面上得以检查，因为只有被明确授权过的操作才能以被调用。

一个句柄是一个不可伪造的令牌，它唯一地标识了一个内核对象（如线程控制块TCB），句柄的管理机构中，有这个句柄的访问权限信息，这些信息中包含哪些方法可以被访问。概念上，句柄存储于应用程序的特定存储区（capability space），这个存储区的存储单元你为slot，一个slot可以包含一个句柄，也可以啥也不包含。应用程序通过句柄（即存有这个句柄的那个slot的地址）来请求内核中的服务。这意味着Magenta的capability模型是一个被内核管理的隔离的（segregated）或分区的（partitioned) capability模型，也就是说这些句柄的内存虽然是存储在用户态中的，但是被内核管理。

句柄上的权限也可以被撤销，递归地撤销所有从原句柄中继承来的权限。句柄的繁殖控制模型被称为take-grant-based模型。

### Magenta句柄

句柄（Handle）由内核创建，供用户态的应用程序使用，应用程序通过句柄引用内核对象。

多个句柄可以对应一个内核对象，但是一个句柄只能对应一个对象。当一个句柄对应一个内核对象时，我们称它为在运输途中（in-transit）。

In user-mode a handle is simply a specific number returned by some syscall. Only handles that are not in-transit are visible to user-mode.

在用户程序中，句柄是一个整数，句柄是与进程相关的数据结构，在这个进程中的句柄，到另外一个进程中是无效的，同样的句柄值（就是那个整数值）完全可能对应完全不同的内核对象。

内核中，句柄是一个至少包含了下列成员的c++对象：

* A reference to a kernel object
* The rights to the kernel object
* The process it is bound to (or if its bound to kernel)

操作权限用来标识这个对象允许的操作，同一个内核对象，通过多个句柄引用它，这多个句柄，完全可能自己有自己的权限，也就是虽然指向的是同一个对象，但你通过这个句柄能实现的操作，通过另外一个句柄却不可以。

#### 句柄的使用

很多系统调用创建出句柄并且返回结果为句柄，如：

* mx\_event\_create
* mx\_process\_create
* mx\_thread\_create

These calls create both the kernel object and the first handle pointing to it. The handle is bound to the process that issued the syscall and the rights are the default rights for that type of kernel object.

#### 句柄的复制

只有一个系统调用实现句柄复制，它创建一个指向同一内核对象的句柄，并且与同一进程绑定：

mx\_handle\_duplicate

#### 句柄的替换

There is one syscall that creates an equivalent handle (possibly with fewer rights), invalidating the original handle:

mx\_handle\_replace

#### 句柄的销毁

There is one syscall that just destroys a handle:

mx\_handle\_close

#### 句柄的写

There is only one syscall that takes a handle bound to calling process and binds it into kernel (puts the handle in-transit):

mx\_message\_write

#### 句柄的写

There is only one syscall that takes an in-transit handle and binds it to the calling process:

mx\_message\_read

The pair of 'message' syscalls above are used to effectively transfer a handle from one process to another. The gist is that it is possible to connect two processes with a 'message pipe'. To transfer a handle the source process calls mx\_message\_write and then the destination process calls mx\_message\_read on the same pipe.

Finally, there is a single syscall that gives a new process its boostrapping handle, that is, the handle that it can use to request other handles:

mx\_process\_start

It is natural that the bootstrapping handle points to one end of a message pipe.

### Magenta句柄垃圾回收

当一个内核对象是有效的，则指向它的句柄都是有效的，因为内核对象是通过引用计数管理内存的，每个句柄持有内核对象的的一个引用计数。

The opposite does not hold. When a handle is destroyed it does not mean its object is destroyed. There could be other handles pointing to the object or the kernel itself could be holding a reference to the kernel object.

When there is but one handle referencing a kernel object and the handle is being closed, the kernel object is either destroyed then or the kernel marks the object for garbage collection; the object will be destroyed when the current set of operations on it are completed.

特殊情况

When a handle is in-transit and the message pipe it was written to is destroyed, the handle is closed.

Debugging sessions (and debuggers) might have special syscalls to get access to handles.

### 句柄的权限

Rights are associated with handles and convey privileges to perform actions on either the associated handle or the object associated with the handle.

|  |  |
| --- | --- |
| **Right** | **Conferred Privileges** |
| **MX\_RIGHT\_DUPLICATE** | Allows handle duplication via [mx\_handle\_duplicate](https://github.com/fuchsia-mirror/magenta/blob/master/docs/syscalls/handle_duplicate.md) |
| **MX\_RIGHT\_TRANSFER** | Allows handle transfer via [mx\_message\_write](https://github.com/fuchsia-mirror/magenta/blob/master/docs/syscalls/message_write.md) |
| **MX\_RIGHT\_READ** | Allows inspection of object state |
|  | Allows reading of data from containers (pipes, VM objects, etc) |
| **MX\_RIGHT\_WRITE** | Allows modification of object state |
|  | Allows writing of data to containers (pipes, VM objects, etc) |
| **MX\_RIGHT\_EXECUTE** |  |
| **MX\_RIGHT\_DEBUG** | Placeholder for debugger use, pending audit of all rights usage |

## 虚拟地址空间（Virtual Address Spaces）

传统上，象Linux这样的操作系统，虚拟地址空间是针对进程（Process）来说的，每个进程工作地独立的地址空间中，进程为其中的计算提供隔离的计算容器。Java虚拟机中的class-loader也提供了一个计算的隔离能力，Linux的cgroup也提供了一种计算隔离能力。因为不同的计算隔离能力，产生了很多的内存管理措施。

Magenta内核没有虚拟地址空间管理的能力，它也没有进程这样的概念，换句话说，你是自己想玩Windows CE slot那样的进程，还是Linux那样的完整的概念的进程，那是在Magenta上搭建的计算模型支持层的事。Magenta+Elastos中的Elastos就是样的一个计算模型支持层。

Windows CE只能管理512MB的物理内存和4GB大小的虚拟地址空间。在Windows CE 4GB的虚拟地址空间中，从0x00000000到Ox41FFFFFF由所有应用程序使用。这块地址空间分成33个槽(Slot)，每个槽占有32MB的地址空间。槽0由当前占有CPU的进程使用。槽1由XIP DLL使用。其它槽用于进程使用，每个进程占用一个槽，进程彼此不能够随意访问。因为槽0只有32MB，因此每个进程运行时只有32MB的虚拟地址空间。

Magenta没有对虚拟地址空间的定义，虚拟地址与物理地址的影射（map）是被用户态的程序自己管理的。例如，一个page fault中断触发的异常是被送到定义在用户态空间的处理线程用户态页机制（user-level pager），这个页处理机制决定这个缺页中断如何处理，你是映射到一块物理内存，还是做什么处理，Magenta是不管的。

用户态的桢（User-level frame）是唯一可以在用户态被直接访问的内存，它们通过原始内存（untyped memory）创建而来。在这些帧被访问之前，它们需要被映射到虚拟地址空间，地址空间通过创建、链接页表对象得到，地个地址空间是一个指向最上层页表的句柄可能（a capability to its top-level page table）标识的。

虚拟地址空间对象 Virtual Address Space Objects

用来创建虚拟地址空间（或VSpace），这些虚拟地址空间可以给一个线程或多个线程使用。这些对象管理着物理的存储设备，例如，页字典（page directory）管理着页表（page directory），页表就是让你的虚拟地址与物理地址对应起来的那个物理器件MMU，内核还包括ASID Pool和ASID Control对象，用来跟踪地址空间状态。

## 线程（Threads）

线程（Thread）是被内核调度的执行单位。线程被创建后，需要为其指定内存地址空间，它在运行的过程中，可以改变这个指定的内存地址空间。一段内存地址空间，可以被0个、一个或多个线程指定，这些线程没有主线程、原始线程之类的概念。

Magenta中，一个象Linux这样的传统的操作系统进程的概念被分解为：地址空间、虚实映射机制、程序及原始数据（装到内存里的那些用户自己写的逻辑）、执行线索等等。

Magenta的每个线程对应内存中的一个线程控制块（TCB，thread control block）对象，没有内核线程这样的说法，也就是说，没有一个线程是只工作在内核态中的，除非它是一个哑（idle）线程，所有系统调用都是工作在调用它的那个线程的用户态空间中的。

## 进程间通信（Inter-Process Communication，IPC）

IPC发生在端点（endpoint）间。一个端点是一个独立的内核对象，拥有端点的线程通过调用端点的句柄（endpoint capability）发送或接收IPC消息。当一个端点被调用（发送消息Send或接收消息Receive），IPC消息传输立即发生在这两个线程（发送者与接收者）之间。IPC只能发生在处理同一个端点的两个线程之间。

IPC在语义上并不要求发生请求与应答的双方在一个地址空间或不在一个地址空间。

IPC的端点有同步与异步的说法，当访问同步端点，当发出请求或接收请求，线程将被阻塞，直到消息发出（此时接收者需要要接收），或有消息传过来（当然是请求者把消息传过来，它发了请求）。

消息（Message）最大480字节（120个消息字，每个消息字32比特）。

发送一个异步消息从来不被阻塞，异步消息只能是一个消息字，即32比特，4个字节。这个消息被存储在这个端点，端点上不能存储多个消息，如果多个消息被发送，这些消息将被通过位或（bitwase OR operation）运算为新的异步消息。

## 设备驱动与中断（Device Drivers and IRQs）

微内核操作系统的驱动通常不在内核中实现，为了让用户态中的程序可以访问设备寄存器，内核向用户态程序提供了设备桢（device frame），这些设备桢覆盖了设备的寄存器端口地址空间（memory-mapped registers）。

中断被异步递送到侦听这个中断的驱动程序端点。Magenta内核允许设置哪些端点侦听哪些中断，这些端点也被用来设置中断的使能与告知（enable、disable、acknowledge）。

## 抢占（Preemption）

在处理一个事件时，Magenta不能直接被打断，在内核执行时，不允许发生中断。为了防止高优先级的中心被延迟，Magenta在需要长时间操作的事务（long-running operation）中，设置是抢占点（preemption point）。在内核执行到抢占点时，将检查被挂起的中断，如果检查到有挂起的中断，触发一个抢点异常（preemption exception），这个异常被传给内核入口函数（the main kernel entry function），在那里，中断被触发，然后我们再次进入内核处理这个中断。处理完这个中断后，内核返回到用户态，原来的系统调用被重新执行，然后这个长事务被继续执行。

# 加电开始

对于ARM系统：系统复位或开机时马上进入到SVC模式，即管理模式（Supervisor，SVC）。

万物之始。加电后CPU执行的第一条外部指令（在CPU执行FLASH中的指令前，SOC内部可能有一些初始化程序的）。

源码：$Magenta/magenta/kernel/arch/arm/arm/start.S

.section ".text.boot"

.globl \_start

\_start:

b platform\_reset

b arm\_undefined

b arm\_syscall

b arm\_prefetch\_abort

b arm\_data\_abort

b arm\_reserved

b arm\_irq

b arm\_fiq

#if WITH\_SMP

b arm\_reset

#endif

.weak platform\_reset

platform\_reset:

/\* Fall through for the weak symbol \*/

## lk\_main()

lk\_main 主要做两件事：

1、本身 lk 这个系统模块的初始化；

2、boot 的启动初始化动作。

### lk\_main 源码分析

源码：Magenta/magenta/kernel/top/main.c

/\* called from arch code \*/

void lk\_main(ulong arg0, ulong arg1, ulong arg2, ulong arg3)

void lk\_main（）

{

1. 初始化进程（lk 中的简单进程）相关结构体。

thread\_init\_early();

1. 做一些如 关闭 cache，使能 mmu 的 arm 相关工作。

arch\_early\_init();

1. 相关平台的早期初始化

platform\_early\_init();

1. 现在就一个函数跳转，初始化UART（板子相关）

target\_early\_init();

1. 构造函数相关初始化

call\_constructors();

1. lk系统相关的堆栈初始化

heap\_init();

}

以上与boot启动初始化相关函数是arch\_early\_init、platform\_early\_init、bootstrap2。

### arch\_early\_init()

体系架构相关的初始化我们一般用的 ARM 体系

1. 关闭cache

arch\_disable\_cache(UCACHE);

1. 设置向量基地址（中断相关）

set\_vector\_base(MEMBASE);

1. 初始化MMU

arm\_mmu\_init();

1. 初始化MMU映射\_\_平台相关

platform\_init\_mmu\_mappings();

1. 开启cache

arch\_enable\_cache(UCACHE)

1. 使能 cp10 和 cp11

\_\_asm\_\_ volatile("mrc p15, 0, %0, c1, c0, 2" : "=r" (val));

val |= (3<<22)|(3<<20);

\_\_asm\_\_ volatile("mcr p15, 0, %0, c1, c0, 2" :: "r" (val));

1. 设置使能 fpexc 位 （中断相关）

\_\_asm\_\_ volatile("mrc p10, 7, %0, c8, c0, 0" : "=r" (val));

val |= (1<<30);

\_\_asm\_\_ volatile("mcr p10, 7, %0, c8, c0, 0" :: "r" (val));

1. 使能循环计数寄存器

\_\_asm\_\_ volatile("mrc p15, 0, %0, c9, c12, 0" : "=r" (en));

en &= ~(1<<3); /\*循环计算每个周期\*/

en |= 1;

\_\_asm\_\_ volatile("mcr p15, 0, %0, c9, c12, 0" :: "r" (en));

1. 使能循环计数器

en = (1<<31);

\_\_asm\_\_ volatile("mcr p15, 0, %0, c9, c12, 1" :: "r" (en));

### platform\_early\_init()

平台相关初始化不同平台不同的初始化。

1. 初始化中断

platform\_init\_interrupts();

1. 初始化定时器

platform\_init\_timer();

### bootstrap2

bootstrap2 在lk\_main的末尾以线程方式开启。主要分三步：platform\_init、target\_init、apps\_init。

1. platform\_init

platform\_init 中主要是函数 acpu\_clock\_init。

在 acpu\_clock\_init 对 arm11 进行系统时钟设置，超频

1. target\_init

针对硬件平台进行设置。主要对 arm9 和 arm11 的分区表进行整合，初始化flash和读取FLASH信息

1. apps\_init

apps\_init 是关键，对 LK 中所谓 app 初始化并运行起来。

源码：$Magenta/magenta/kernel/app/app.c

/\* one time setup \*/

void apps\_init(void)

{

const struct app\_descriptor \*app;

/\* call all the init routines \*/

for (app = \_\_start\_apps; app != \_\_stop\_apps; app++) {

if (app->init)

app->init(app);

}

/\* start any that want to start on boot \*/

for (app = \_\_start\_apps; app != \_\_stop\_apps; app++) {

if (app->entry && (app->flags & APP\_FLAG\_DONT\_START\_ON\_BOOT) == 0) {

start\_app(app);

}

}

}

## Boot程序中的trampoline(弹簧床)

Boot Loader 的 stage2 <https://www.ibm.com/developerworks/cn/linux/l-btloader/>

stage2 的代码通常用 C 语言来实现，以便于实现更复杂的功能和取得更好的代码可读性和可移植性。但是与普通 C 语言应用程序不同的是，在编译和链接 boot loader 这样的程序时，我们不能使用 glibc 库中的任何支持函数。其原因是显而易见的。这就给我们带来一个问题，那就是从那里跳转进 main() 函数呢？直接把 main() 函数的起始地址作为整个 stage2 执行映像的入口点或许是最直接的想法。但是这样做有两个缺点：1)无法通过main() 函数传递函数参数；2)无法处理 main() 函数返回的情况。一种更为巧妙的方法是利用 trampoline(弹簧床)的概念。也即，用汇编语言写一段trampoline 小程序，并将这段 trampoline 小程序来作为 stage2 可执行映象的执行入口点。然后我们可以在 trampoline 汇编小程序中用 CPU 跳转指令跳入 main() 函数中去执行；而当 main() 函数返回时，CPU 执行路径显然再次回到我们的 trampoline 程序。简而言之，这种方法的思想就是：用这段 trampoline 小程序来作为 main() 函数的外部包裹(external wrapper)。

下面给出一个简单的 trampoline 程序示例(来自blob)：

.text

.globl \_trampoline

\_trampoline:

bl main

/\* if main ever returns we just call it again \*/

b \_trampoline

可以看出，当 main() 函数返回后，我们又用一条跳转指令重新执行 trampoline 程序――当然也就重新执行 main() 函数，这也就是 trampoline(弹簧床)一词的意思所在。

如果你的main()函数不是call进去的，从main()返回时，就不知道返回到哪里去，通过trampoline(弹簧床)这个机制，相当于是造了一个栈，好让main()函数能够正确进入与退出。

## 起动过程

起动过程中的这些信息，是哪个程序出来的？

[00000.070] K initializing platform

[00000.070] K INIT: cpu 0, calling hook 0xffff00000001f008 (pcie\_early\_init) at level 0x8ffff, flags 0x1

[00000.083] K initializing target

[00000.083] K calling apps\_init()

[00000.083] K INIT: cpu 0, calling hook 0xffff000000026368 (ktrace) at level 0xaffff, flags 0x1

[00000.328] K ktrace: buffer at 0xffff0007811c0000 (33554432 bytes)

[00000.328] K INIT: cpu 0, calling hook 0xffff000000035140 (userboot) at level 0xaffff, flags 0x1

[00000.328] K userboot: console init

[00000.330] K userboot: bootfs 3268608 @ 0xffff00000007c000

[00000.346] K userboot: userboot-rodata 0 @ [0x1000000,0x1001000)

[00000.347] K userboot: userboot-code 0x1000 @ [0x1001000,0x1003000)

[00000.348] K userboot: vdso-rodata 0 @ [0x1003000,0x1007000)

[00000.349] K userboot: vdso-code 0x4000 @ [0x1007000,0x1008000)

[00000.357] K userboot: entry point @ 0x1001840

[00000.364] U userboot: searching bootfs for "bin/devmgr"

[00000.369] U userboot: bin/devmgr has PT\_INTERP "lib/ld.so.1"

[00000.370] U userboot: searching bootfs for "lib/ld.so.1"

[00000.384] U userboot: bin/devmgr started. userboot exiting.

[00000.394] U Loaded at [0x10de000,0x1111000): <application>

[00000.394] U Loaded at [0x1099000,0x109e000): <vDSO> (libmagenta.so)

[00000.395] U Loaded at [0x1000000,0x1099000): libc.so

[00000.397] U devmgr: main()

[00000.401] U devmgr: vfs init

[00000.405] U devmgr: bootfs #0 contains 84 files

[00000.418] U devmgr: launch /boot/bin/crashlogger (crashlogger)

[00000.507] U devmgr: launch acpisvc

[00000.581] U crashlogger service ready

[00000.688] U devmgr: load drivers

[00000.689] U console\_init()

[00000.695] U debug\_reader()

[00000.700] U console\_init()

[00000.702] U devmgr: shell startup

[00000.741] U devmgr: launch /boot/bin/mxsh (mxsh:console)

[00000.783] U devmgr: launch /boot/bin/netsvc (netsvc)

[00000.878] U devmgr: launch /boot/bin/mxsh (mxsh:autorun)

源码：$Magenta/magenta/kernel/lib/debuglog/debuglog.c

static int debuglog\_reader(void\* arg) {

n = snprintf(tmp, sizeof(tmp), "[%05d.%03d] %c %s\n",

(int) (rec->timestamp / 1000000000ULL),

(int) ((rec->timestamp / 1000000ULL) % 1000ULL),

(rec->flags & DLOG\_FLAG\_KERNEL) ? 'K' : 'U',

rec->data);

# Magenta内核

## 内核起动地址

ARM平台

源码：$Magenta/magenta/kernel/arch/arm/arm/start.S

中断向量

.section ".text.boot"

.globl \_start

\_start:

b platform\_reset

b arm\_undefined

b arm\_syscall

b arm\_prefetch\_abort

b arm\_data\_abort

b arm\_reserved

b arm\_irq

b arm\_fiq

#if WITH\_SMP

b arm\_reset

#endif

## 从内核回用户态

源码：$Magenta/magenta/kernel/arch/arm/arm/arch.c

/\* switch to user mode, set the user stack pointer to user\_stack\_top, put the svc stack pointer to the top of the kernel stack \*/

void arch\_enter\_uspace(uintptr\_t pc, uintptr\_t sp,

uintptr\_t arg1, uintptr\_t arg2)

## 内核对象

内核对象，如VmObject，如果不只是被内核编程使用，用户态程序还会与这个对象直接打交道，则它会被包装为分发器Dispatcher。

|  |  |
| --- | --- |
| 内核对象 | 分发器Dispatcher |
|  | ProcessDispatcher |
| VmObject | VmObjectDispatcher |
| UserThread | ThreadDispatcher |
|  | EventDispatcher  EventPairDispatcher |
|  | DataPipeConsumerDispatcher  DataPipeProducerDispatcher |
|  | InterruptDispatcher  InterruptEventDispatcher |
|  | ResourceDispatcher |
|  | WaitSetDispatcher |
|  | IOPortDispatcher  IoMappingDispatcher |

### Process

#### 取当前进程

ProcessDispatcher::GetCurrent

auto up = ProcessDispatcher::GetCurrent();

### Thread

The thread object is the construct that represents a time-shared CPU execution context. Thread objects live associated to a particular Process Object which provides the memory and the handles to other objects necessary for I/O and computation.

Lifetime

A thread can be created implicitly by calling sys\_process\_start(), in which case the new thread is the "main thread" and the thread entrypoint is defined by the previously loaded binary. Or it can be created by calling sys\_thread\_create() which takes the entrypoint as a parameter.

A thread terminates when it returns from executing the routine specified as the entrypoint or by calling sys\_thread\_exit().

### Event

### Message pipe

### Interrupt request

### VMObject

A Virtual Memory Object (VMO) represents a contiguous region of virtual memory that may be mapped into multiple address spaces.

源码：$Magenta/magenta/kernel/include/kernel/vm/vm\_object.h

源码：$Magenta/magenta/kernel/kernel/vm/vm\_object.cpp

// The base vm object that holds a range of bytes of data

//

// Can be created without mapping and used as a container of data, or mappable

// into an address space via VmAspace::MapObject

class VmObject : public mxtl::RefCounted<VmObject> {

源码：$Magenta/magenta/kernel/lib/magenta/include/magenta/vm\_object\_dispatcher.h

class VmObjectDispatcher : public Dispatcher {

### Data pipe

### Job

### IOPort

## 程序加载器Loader

链接角本

源码：$Magenta/magenta/scripts/tmpl-rodso.ld

/\*

\* This is a linker script for producing a DSO (shared library) image

\* that is entirely read-only and trivial to map in without using a

\* proper ELF loader. It has two segments: read-only starting at the

\* beginning of the file, and executable code page-aligned and marked

\* by the (hidden) symbols CODE\_START and CODE\_END.

\*

\* Ideally this could be accomplished without an explicit linker

\* script. The linker would need an option to make the .dynamic

\* section (aka PT\_DYNAMIC segment) read-only rather than read-write;

\* in fact that could be the default for Magenta/Fuchsia or for

\* anything using a dynamic linker like musl's that doesn't try to

\* write into the .dynamic section at runtime (for -shared that is;

\* for -pie and dynamically-linked executables there is the DT\_DEBUG

\* question). The linker would need a second option to entirely

\* segregate code from rodata (and from non-loaded parts of the file),

\* and page-align the code segment (and pad the end to a page

\* boundary); in fact that could be the default for any system that

\* wants to minimize what can go into pages mapped with execute

\* permission, which is a worthwhile trade-off of security mitigation

\* over tiny amounts of wasted space in the ELF file. Beyond that,

\* the linker should not generate the .got\* or .plt\* sections at all

\* when there are no relocs being generated, but today's linkers still

\* do; since some of those sections are writable, they cause the

\* creation of a writable PT\_LOAD segment by normal linker logic.

\*/

### 内核elf-loader

Magenta所有程序都是ELF格式的。

bootstrap()是系统起动过程中的加载应用程序的函数。

load\_child\_process()会调用elf\_load\_bootfs(),elf\_load\_bootfs()会调用elf\_load\_prepare()

源码：$Magenta/magenta/system/uapp/userboot/start.c

// This is the main logic:

// 1. Read the kernel's bootstrap message.

// 2. Load up the child process from ELF file(s) on the bootfs.

// 3. Create the initial thread and allocate a stack for it.

// 4. Load up a message pipe with the mx\_proc\_args\_t message for the child.

// 5. Start the child process running.

// 6. Optionally, wait for it to exit and then shut down.

static noreturn void bootstrap(mx\_handle\_t log, mx\_handle\_t bootstrap\_pipe) {

load\_child\_process(log,proc\_self,&o,bootfs\_vmo, vdso\_vmo, proc, to\_child,

&entry, &vdso\_base, &stack\_size);

源码：$Magenta/magenta/system/uapp/userboot/userboot-elf.c

mx\_vaddr\_t elf\_load\_bootfs(mx\_handle\_t log, mx\_handle\_t proc\_self,

struct bootfs \*fs, mx\_handle\_t proc,

const char\* filename, mx\_handle\_t to\_child,

size\_t\* stack\_size) {

源码：$Magenta/magenta/system/ulib/elfload/elf-load.c

mx\_status\_t elf\_load\_prepare(mx\_handle\_t vmo, elf\_load\_header\_t\* header,

uintptr\_t\* phoff) {

### 应用程序加载器

源码：$Magenta/magenta/system/ulib/launchpad/launchpad.c

struct launchpad {

uint32\_t argc;

uint32\_t envc;

char\* args;

size\_t args\_len;

char\* env;

size\_t env\_len;

mx\_handle\_t\* handles;

uint32\_t\* handles\_info;

size\_t handle\_count;

size\_t handle\_alloc;

mx\_vaddr\_t entry;

mx\_vaddr\_t vdso\_base;

size\_t stack\_size;

mx\_handle\_t special\_handles[HND\_SPECIAL\_COUNT];

bool loader\_message;

};

# 系统调用

操作系统的系统，分内核侧和应用程序侧，工作在用户态的程序（UserLand）通过svc指令调用内核侧的代码arm\_syscall。

## svc中断向量

#ifndef WITH\_LIB\_SYSCALL

FUNCTION(arm\_syscall)

saveall

/\* r0 now holds pointer to iframe \*/

bl arm\_syscall\_handler

restoreall

#endif

## 内核栈svc stack

源码：$Magenta/magenta/kernel/arch/arm/arm/arch.c

/\* initial and abort stacks \*/

uint8\_t abort\_stack[ARCH\_DEFAULT\_STACK\_SIZE \*SMP\_MAX\_CPUS] \_\_CPU\_ALIGN;

在ARM平台上，通常ARCH\_DEFAULT\_STACK\_SIZE=4096。系统起动时，初始化CPU时会设置内核栈。

源码：$Magenta/magenta/kernel/arch/arm/arm/start.S

/\* set up the stack for irq, fiq, abort, undefined, system/user, and lastly supervisor mode \*/

mov r1, #0

cpsid i,#0x12 /\* irq \*/

mov sp, r1

cpsid i,#0x11 /\* fiq \*/

mov sp, r1

cpsid i,#0x17 /\* abort \*/

mov sp, r1

cpsid i,#0x1b /\* undefined \*/

mov sp, r1

cpsid i,#0x1f /\* system \*/

mov sp, r1

cpsid i,#0x13 /\* supervisor \*/

ldr r1, =abort\_stack

mov r2, #ARCH\_DEFAULT\_STACK\_SIZE

add r0, #1

mul r2, r2, r0

add r1, r2

mov sp, r1

通过下面两段源码：system-onesegment.ld、qemu-virt/rules.mk，能看出内核在内存中的布局，在QEMU-VIRT仿真器上，内核留了64KB内存，就是为了摆这些stack的。

源码：$Magenta/magenta/kernel/arch/arm/system-onesegment.ld

ENTRY(\_start)

SECTIONS

{

. = %KERNEL\_BASE% + %KERNEL\_LOAD\_OFFSET%;

\_start = .;

源码：$Magenta/magenta/kernel/platform/qemu-virt/rules.mk

MEMBASE := 0x40000000

MEMSIZE ?= 0x08000000 # 512MB

KERNEL\_LOAD\_OFFSET := 0x10000 # 64k

有些操作系统内核，当程序从用户态跑到内核里来，就把请求的栈及当前的线程等信息保存起来，归内核的调度体使用，有些内核则直接利用用户态的栈，直接干活。Magenta属于后者，而且一上来不管什么情况，把通用寄存器都保存了起来。

源码：$Magenta/magenta/kernel/arch/arm/arm/exceptions.S

FUNCTION(arm\_syscall)

saveall

/\* r0 now holds pointer to iframe \*/

bl arm\_syscall\_handler

restoreall

/\* Save all registers.

\* At exit r0 contains a pointer to the register frame.

\*/

.macro saveall

/\* save spsr and r14 onto the svc stack \*/

srsdb #0x13!

/\* switch to svc mode, interrupts disabled \*/

cpsid i,#0x13

/\* save all regs \*/

push { r0-r12, lr }

/\* save user space sp/lr \*/

sub sp, #8

stmia sp, { r13, r14 }^

#if ARM\_WITH\_VFP

/\* save and disable the vfp unit \*/

vfp\_save r0

#endif

/\* make sure the stack is 8 byte aligned \*/

stack\_align r0

/\* r0 now holds the pointer to the original iframe (before alignment) \*/

.endm

## 系统调用在内核侧的实现

源码：$Magenta/magenta/kernel/lib/syscalls/syscalls.cpp

/\* build a function pointer to call the routine.

\* the args are jammed into the function independent of if the function

\* uses them or not, which is safe for simple arg passing.

\*/

syscall\_func sfunc;

switch (syscall\_num) {

#define MAGENTA\_SYSCALL\_DEF(nargs64, nargs32, n, ret, name, args...) \

case n: \

sfunc = reinterpret\_cast<syscall\_func>(sys\_##name); \

break;

#include <magenta/syscalls.inc>

default:

sfunc = reinterpret\_cast<syscall\_func>(sys\_invalid\_syscall);

}

真正的系统调用都是通过宏MAGENTA\_SYSCALL\_DEF定义的。

源码：$Magenta/magenta/system/ulib/magenta/include/magenta/syscalls.inc

// Threads

MAGENTA\_SYSCALL\_DEF(4, 4, 50, mx\_handle\_t, thread\_create, int (\*entry)(void\*), USER\_PTR(void) arg,

USER\_PTR(const char) name, uint32\_t name\_len)

MAGENTA\_SYSCALL\_DEF\_WITH\_ATTRS(0, 0, 51, void, thread\_exit, (noreturn), void)

MAGENTA\_SYSCALL\_DEF(3, 3, 52, mx\_status\_t, thread\_arch\_prctl, mx\_handle\_t handle, uint32\_t op,

USER\_PTR(uintptr\_t) value\_ptr)

## 3.4 系统调用在应用程序侧的实现

### 系统调用定义

源码：$Magenta/magenta/system/ulib/magenta/include/magenta/syscalls.h

// define all of the syscalls from the syscall list header.

// user space syscall vaneer routines are all prefixed with mx\_

#define MAGENTA\_DDKCALL\_DEF(a...)

#define MAGENTA\_SYSCALL\_DEF(nargs64, nargs32, n, ret, name, args...) extern ret mx\_##name(args);

#define MAGENTA\_SYSCALL\_DEF\_WITH\_ATTRS(nargs64, nargs32, n, ret, name, attrs, args...) extern ret mx\_##name(args) \_\_attribute\_\_(attrs);

#include <magenta/syscalls.inc>

In userspace the syscall dispatch layer (libmagenta) exposes the result values as variables of type mx\_status\_t that currently use the same spelling and values as the kernel for errors, but which will transition to using 0 for success and positive values for errors.

### 用户态与内核态调用者

工作在用户态的应用程序通过这些程序进入内核态，实现对系统功能的调用。用户态程序中关于系统调用的符号（如：mx\_handle\_duplicate），也就是通过这个程序提供的链接符号。

源码：

$Magenta/magenta/system/ulib/magenta/syscalls-arm32.S

$Magenta/magenta/system/ulib/magenta/syscalls-arm64.S

$Magenta/magenta/system/ulib/magenta/syscalls-x86-64.S

如ARM64的源码：

/\* define and implement the magenta syscall wrappers for arm64 \*/

.text

.cfi\_sections .eh\_frame, .debug\_frame

.macro syscall name, n

.globl \name

.type \name,STT\_FUNC

\name:

.cfi\_startproc

mov x16, #\n

svc #0xf0f /\* magic value to differentiate magenta syscalls \*/

ret

.cfi\_endproc

.size \name, . - \name

.endm

#if LIBDDK

#define MAGENTA\_SYSCALL\_DEF(a...)

#define MAGENTA\_DDKCALL\_DEF(nargs64, nargs32, n, ret, name, args...) syscall mx\_##name, n

#else

#define MAGENTA\_DDKCALL\_DEF(a...)

#define MAGENTA\_SYSCALL\_DEF(nargs64, nargs32, n, ret, name, args...) syscall mx\_##name, n

#endif

#include <magenta/syscalls.inc>

### 动态库libmagenta.so

源码：$Magenta/magenta/kernel/lib/userboot/vdso.S

// The whole thing can't be just an assembler macro because a macro

// operand cannot be a string like .incbin needs for the filename.

#define FILE\_IMAGE(name, NAME) \

image\_section name, NAME##\_CODE\_END; \

DATA(name##\_image) \

.incbin NAME##\_FILENAME, 0, NAME##\_CODE\_END; \

END(name##\_image)

// The vDSO image, aka libmagenta.so.

FILE\_IMAGE(vdso, VDSO)

// The earliest user-mode process runs this image, aka userboot.

FILE\_IMAGE(userboot, USERBOOT)

**make文件相关：**

源码：$Magenta/magenta/system/ulib/magenta/rules.mk

MODULE\_TYPE := userlib

# This library should not depend on libc.

MODULE\_COMPILEFLAGS := -ffreestanding

# Both kernel and userspace code needs magenta headers.

GLOBAL\_INCLUDES += $(LOCAL\_DIR)/include

ifeq ($(ARCH),arm)

MODULE\_SRCS += $(LOCAL\_DIR)/syscalls-arm32.S

else ifeq ($(ARCH),arm64)

MODULE\_SRCS += $(LOCAL\_DIR)/syscalls-arm64.S

else ifeq ($(ARCH),x86)

ifeq ($(SUBARCH),x86-64)

MODULE\_SRCS += $(LOCAL\_DIR)/syscalls-x86-64.S

else

MODULE\_SRCS += $(LOCAL\_DIR)/syscalls-x86.S

endif

endif

# This gets an ABI stub installed in sysroots, but the DSO never gets

# installed on disk because it's delivered magically by the kernel.

MODULE\_SO\_NAME := magenta

MODULE\_SO\_INSTALL\_NAME := -

# All the code this DSO is pure read-only/reentrant code that

# does not need any writable data (except its caller's stack).

# Make it use a simplified, hardened memory layout.

MODULE\_LDFLAGS := -T $(BUILDDIR)/rodso.ld

MODULE\_EXTRA\_OBJS := $(BUILDDIR)/rodso-stamp

### 应用程序系统调用头文件

源码：$Magenta/magenta/system/ulib/magenta/include/magenta/syscalls.h

// define all of the syscalls from the syscall list header.

// user space syscall vaneer routines are all prefixed with mx\_

#define MAGENTA\_DDKCALL\_DEF(a...)

#define MAGENTA\_SYSCALL\_DEF(nargs64, nargs32, n, ret, name, args...) extern ret mx\_##name(args);

#define MAGENTA\_SYSCALL\_DEF\_WITH\_ATTRS(nargs64, nargs32, n, ret, name, attrs, args...) extern ret mx\_##name(args) \_\_attribute\_\_(attrs);

#include <magenta/syscalls.inc>

### 导出系统调用符号

Mangeta设有userboot机制，就是一个用户态应用起来时，你要加载的有些符号是系统向你提供的，就象是Linux动态链接库(.so)一样，只是这些库是预先装入的。

我再科普一下什么是系统调用。操作系统的系统调用大部分是实现在内核里的，应用程序通过一个类似ARM中的svc指令，调用内核的功能。但这些系统调用，需要完善、包装，才能被应用程序使用，比如堆heap，是c/c++库提供的功能，内核提供的内存管理API很简单，不易用。这个包装后的程序，被通俗称为系统调用。

#### make角本

# This generated linker script defines symbols for each vDSO entry point

# giving the relative address where it will be found at runtime. With

# this hack, the userboot code doesn't need to do any special work to

# find the vDSO and its entry points, keeping the code far simpler.

$(BUILDDIR)/$(LOCAL\_DIR)/vdso-syms.ld: \

$(LOCAL\_DIR)/vdso-syms.ld.h $(BUILDDIR)/$(LOCAL\_DIR)/vdso-syms.h

@$(MKDIR)

@echo generating $@

$(NOECHO)$(CC) -E -P -include $^ > $@

GENERATED += $(BUILDDIR)/$(LOCAL\_DIR)/vdso-syms.ld.h

源码：$Magenta/magenta/system/uapp/userboot/vdso-syms.ld.h

// For each function in the vDSO ABI, define a symbol in the linker script

// pointing to its address. The vDSO is loaded immediately after the

// userboot DSO image's last page, which is marked by the CODE\_END symbol.

// So these symbols tell the linker where each vDSO function will be found

// at runtime. The userboot code uses normal calls to these, declared as

// have hidden visibility so they won't generate PLT entries. This results

// in the userboot binary having simple PC-relative calls to addresses

// outside its own image, to where the vDSO will be found at runtime.

#define FUNCTION(name, address, size) \

PROVIDE\_HIDDEN(name = CODE\_END + address);

#### GCC链接参数

-E

Stop after the preprocessing stage; do not run the compiler proper. The output is in the form of preprocessed source code, which is sent to the standard output.

Input files which don't require preprocessing are ignored.

-P

Inhibit generation of linemarkers in the output from the preprocessor. This might be useful when running the preprocessor on something that is not C code, and will be sent to a program which might be confused by the linemarkers.

## 用户态与内核态间的参数传递

源码：$Magenta/magenta/kernel/arch/arm/arm/user\_copy.c

status\_t arch\_copy\_from\_user(void \*dst, const void \*src, size\_t len)

{

thread\_t \*thr = get\_current\_thread();

return \_arm\_copy\_from\_user(dst,src,len, &thr->arch.data\_fault\_resume);

}

status\_t arch\_copy\_to\_user(void \*dst, const void \*src, size\_t len)

{

thread\_t \*thr = get\_current\_thread();

return \_arm\_copy\_to\_user(dst,src, len, &thr->arch.data\_fault\_resume);

}

源码：$Magenta/magenta/kernel/lib/user\_copy/include/lib/user\_copy.h

inline status\_t copy\_to\_user\_unsafe(void\* dst, const void\* src, size\_t len) {

return arch\_copy\_to\_user(dst, src, len);

}

inline status\_t copy\_from\_user\_unsafe(void\* dst, const void\* src, size\_t len) {

return arch\_copy\_from\_user(dst, src, len);

}

源码：$Magenta/magenta/kernel/lib/user\_copy/user\_copy.c

// Default implementations of arch\_copy\* functions, almost certainly

// want to override with arch-specific versions that check access permissions

\_\_WEAK status\_t arch\_copy\_from\_user(void \*dst, const void \*src, size\_t len) {

memcpy(dst, src, len);

return NO\_ERROR;

}

\_\_WEAK status\_t arch\_copy\_to\_user(void \*dst, const void \*src, size\_t len) {

memcpy(dst, src, len);

return NO\_ERROR;

}

# 线程调度与时间管理

## 当前线程

## 调度器

调度器是一个操作系统整体调度的策略，不只是某一块具体的程序。

源码：$Magenta/magenta/kernel/kernel/thread.c

void thread\_resched(void) {

timer\_set\_periodic(&preempt\_timer[cpu],10,(timer\_callback)thread\_timer\_tick, NULL);

Magenta/magenta/kernel/kernel/timer.c

/\* let the scheduler have a shot to do quantum expiration, etc \*/

/\* in case of dynamic timer, the scheduler will set up a periodic timer \*/

if (thread\_timer\_tick() == INT\_RESCHEDULE)

ret = INT\_RESCHEDULE;

系统时钟初始化

源码：$Magenta/magenta/kernel/kernel/timer.c

void timer\_init(void)

{

#if !PLATFORM\_HAS\_DYNAMIC\_TIMER

/\* register for a periodic timer tick \*/

platform\_set\_periodic\_timer(timer\_tick, NULL, 10); /\* 10ms \*/

#endif

系统时钟函数体

源码：$Magenta/magenta/kernel/kernel/thread.c

enum handler\_return thread\_timer\_tick(void)

{

thread\_t \*current\_thread = get\_current\_thread();

if (thread\_is\_real\_time\_or\_idle(current\_thread))

return INT\_NO\_RESCHEDULE;

current\_thread->remaining\_quantum--;

if (current\_thread->remaining\_quantum <= 0) {

return INT\_RESCHEDULE;

} else {

return INT\_NO\_RESCHEDULE;

}

}

## 线程优先级管理

线程优先级表现在当需要进行调度时，从哪个数据结构里，如何拿到就续的线程。get\_top\_thread()函数就是干这个的。

源码：$Magenta/magenta/kernel/kernel/thread.c

static thread\_t \*get\_top\_thread(int cpu)

{

thread\_t \*newthread;

uint32\_t local\_run\_queue\_bitmap = run\_queue\_bitmap;

while (local\_run\_queue\_bitmap) {

/\* find the first (remaining) queue with a thread in it \*/

uint next\_queue = HIGHEST\_PRIORITY - \_\_builtin\_clz(local\_run\_queue\_bitmap)

- (sizeof(run\_queue\_bitmap) \* 8 - NUM\_PRIORITIES);

list\_for\_every\_entry(&run\_queue[next\_queue], newthread, thread\_t, queue\_node) {

#if WITH\_SMP

if (newthread->pinned\_cpu < 0 || newthread->pinned\_cpu == cpu)

#endif

{

list\_delete(&newthread->queue\_node);

if (list\_is\_empty(&run\_queue[next\_queue]))

run\_queue\_bitmap &= ~(1<<next\_queue);

return newthread;

}

}

local\_run\_queue\_bitmap &= ~(1<<next\_queue);

}

/\* no threads to run, select the idle thread for this cpu \*/

return idle\_thread(cpu);

}

## context切换

在中断返回的之前，把中断记录下来的上下文环境改变一下，就实现了线程切换。

CPU执行时，是没有线程的概念的，当内核处理中断返回时，你做了工作，本来是要执行进入中断时的那条指令的下一条指令，而在中断处理时，你把记录中断进入上下文环境context的那个数据结构frame给改了，于是，中断就如你所愿，按照你的指引，跑你预计的程序（另一个线程）中去了。

源码：$Magenta/magenta/kernel/kernel/thread.c

void thread\_resched(void) {

/\* do the low level context switch \*/

arch\_context\_switch(oldthread, newthread);

arch\_context\_switch()对应到具体平台上就是诸如arm\_context\_switch()这样的函数。

void arch\_context\_switch(thread\_t \*oldthread, thread\_t \*newthread)

{

// TRACEF("arch\_context\_switch: cpu %u old %p (%s), new %p (%s)\n", arch\_curr\_cpu\_num(), oldthread, oldthread->name, newthread, newthread->name);

#if ARM\_WITH\_VFP

arm\_fpu\_thread\_swap(oldthread, newthread);

#endif

arm\_context\_switch(&oldthread->arch.sp, newthread->arch.sp);

}

硬件中表示一个线程并不是用的thread\_t这样的复杂的数据结构，是一个与硬件相关的结构体arch\_thread，它的第一个参数必须是vaddr\_t sp，用来存储栈地址。

源码：$Magenta/magenta/kernel/arch/arm/arm/include/arch/arch\_thread.h

struct arch\_thread {

vaddr\_t sp;

/\* if non-NULL, address to return to on data fault \*/

void \*data\_fault\_resume;

#if ARM\_WITH\_VFP

/\* has this thread ever used the floating point state? \*/

bool fpused;

uint32\_t fpscr;

uint32\_t fpexc;

double fpregs[32];

#endif

};

源码：$Magenta/magenta/kernel/arch/arm/arm/asm.S

/\* context switch frame is as follows:

\* lr

\* r11

\* r10

\* r9

\* r8

\* r7

\* r6

\* r5

\* r4

\* cp15\_ro

\* cp15\_rw

\*/

/\* arm\_context\_switch(addr\_t \*old\_sp, addr\_t new\_sp) \*/

FUNCTION(arm\_context\_switch)

/\* save non callee trashed supervisor registers \*/

/\* spsr and user mode registers are saved and restored in the iframe by exceptions.S \*/

mrc p15, 0, r2, c13, c0, 2

mrc p15, 0, r3, c, c0, 3

push { r2-r11, lr }

/\* save old sp \*/

str sp, [r0]

/\* clear any exlusive locks that the old thread holds \*/

#if ARM\_ARCH\_LEVEL >= 7

/\* can clear it directly \*/

clrex

#elif ARM\_ARCH\_LEVEL == 6

/\* have to do a fake strex to clear it \*/

ldr r0, =strex\_spot

strex r3, r2, [r0]

#endif

/\* load new regs \*/

mov sp, r1

pop { r2-r11, lr }

mcr p15, 0, r2, c13, c0, 2

mcr p15, 0, r3, c13, c0, 3

bx lr

## 定时器

计时器属于操作系统中的基础组件，不管是用户空间的程序开发，还是内核空间的程序开发，很多时候都需要有定时器作为基础组件的支持。使用定时器的目的无非是为了周期性的执行某一任务，或者是到了一个指定时间去执行某一个任务。

源码：$Magenta/magenta/kernel/kernel/timer.c

void timer\_init(void)

{

timer\_lock = SPIN\_LOCK\_INITIAL\_VALUE;

for (uint i = 0; i < SMP\_MAX\_CPUS; i++) {

list\_initialize(&timers[i].timer\_queue);

}

#if !PLATFORM\_HAS\_DYNAMIC\_TIMER

/\* register for a periodic timer tick \*/

platform\_set\_periodic\_timer(timer\_tick, NULL, 10); /\* 10ms \*/

#endif

}

每个CPU核拥有一个定时器队列。不是设在硬件中断上的定时器，只有在系统tick时。才被检查是否到时间，可见其时间精度受系统时钟的精度影响。

## 线程抢先preempt的实现

一个中断向量程序执行完后，判断是否需要线程抢先，不需要抢，接着干原来线程的活。

源码：$Magenta/magenta/kernel/arch/arm/arm/exceptions.S

FUNCTION(arm\_irq)

#if TIMESTAMP\_IRQ

/\* read the cycle count \*/

mrc p15, 0, sp, c9, c13, 0

str sp, [pc, #\_\_irq\_cycle\_count - . - 8]

#endif

save\_offset #4

/\* r0 now holds pointer to iframe \*/

/\* track that we're inside an irq handler \*/

LOADCONST(r2, \_\_arm\_in\_handler)

mov r1, #1

str r1, [r2]

/\* call into higher level code \*/

bl platform\_irq

/\* clear the irq handler status \*/

LOADCONST(r1, \_\_arm\_in\_handler)

mov r2, #0

str r2, [r1]

/\* reschedule if the handler returns nonzero \*/

cmp r0, #0

blne thread\_preempt

restore

# 内存管理

内存管理可以分为页表机制和内存分配机制两大块。页表机制简单说来就是管理着设备真实物理地址与虚拟地址的一个动态或静态的映射，是基于硬件的MMU进行的。

## ARM MMU基本原理

CPU在访问VA（虚拟地址）时，TLB硬件完成VA到PA（物理地址）的转换，但是如果没有该VA的TLB entry，MMU的硬件单元translation table walk hardware（页表索引单元）会索引CP15寄存器c0提供的内存页表，进行地址转换，获取PA进行访问。并且会将该页表信息更新到TLB中，页表跟TLB可不是一个概念，TLB是针对于内存页表的一个缓存硬件！

也就是说ARM的MMU不仅使用TLB进行地址转换，还能够对内存中提供的页表进行解析并地址转换，而TLB中存储的是CPU最常用的一些地址。TLB速度快，这样可以加快地址转换效率。

如果都找不到该VA的页表信息，MMU会向CPU发出异常（根据data还是instruct不同，发出data abort或者instruct abort），异常处理函数中进行页表填充。

ARM的MMU使用内存页表如何完成地址转换，手册一张图将MMU操作页表的几种方式列了出来，如**错误!未找到引用源。**所示：

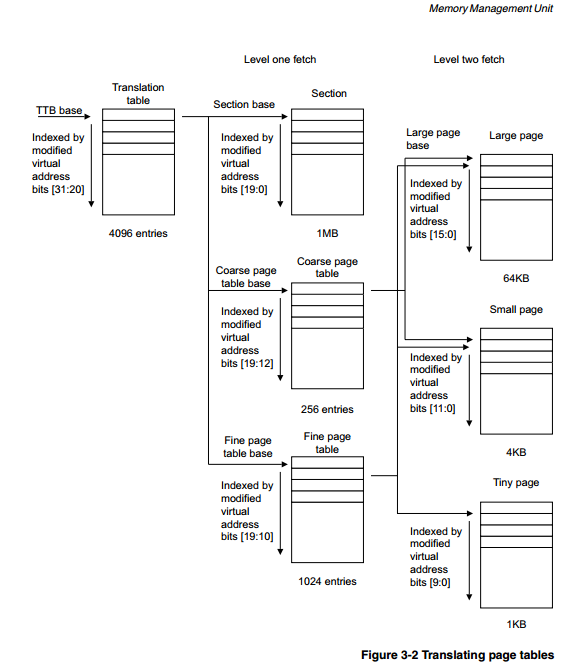


图 ‑1 ARM页表结构示意图

## 地址空间布局

### 虚拟地址规划

源码：$Magenta/magenta/kernel/include/kernel/vm.h

/\* kernel address space \*/

#define KERNEL\_ASPACE\_BASE ((vaddr\_t)0x80000000UL)

#define KERNEL\_ASPACE\_SIZE ((vaddr\_t)0x80000000UL)

/\* user address space, defaults to below kernel space with a 16MB guard gap on either side \*/

#define USER\_ASPACE\_BASE ((vaddr\_t)0x01000000UL)

#define USER\_ASPACE\_SIZE ((vaddr\_t)KERNEL\_ASPACE\_BASE - USER\_ASPACE\_BASE - 0x01000000UL)

/\*

\* user thread virtual memory layout:

\*

\* +-----------------------+ 0xFFFFFFFF

\* | |

\* | 内核空间 |

\* | |

\* +-----------------------+ KERNEL\_ASPACE\_BASE: 0x80000000UL

\* | | 警卫缝隙(Guard Gap)：16MB

\* +-----------------------+ USER\_ASPACE\_BASE：0x01000000

\* | |

\* | |

\* | 用户空间 |

\* | |

\* | |

\* +-----------------------+ USER\_ASPACE\_BASE：0x01000000

\* | | 警卫缝隙(Guard Gap)：16MB

### 物理内存管理

在系统Boot时，Boot程序本身会占用物理内存，当内核起动后，有些物理内存被新操作系统管理起来，但通常情况下，物理内存会被分割成几片。

物理内存管理的数据结构是pmm\_arena\_t。

源码：$Magenta/magenta/kernel/include/kernel/vm.h

/\* physical allocator \*/

typedef struct pmm\_arena {

struct list\_node node;

const char\* name;

uint flags;

uint priority;

paddr\_t base;

size\_t size;

size\_t free\_count;

struct vm\_page\* page\_array;

struct list\_node free\_list;

} pmm\_arena\_t;

系统初始化阶段，通过platform\_early\_init()函数，得到物理内存信息。

源码：$Magenta/magenta/kernel/kernel/vm/pmm.cpp

status\_t pmm\_add\_arena(pmm\_arena\_t\* arena)

源码：$Magenta/magenta/kernel/platform/qemu-virt/platform.c

static pmm\_arena\_t arena = {

.name = "ram",

.base = MEMORY\_BASE\_PHYS,

.size = DEFAULT\_MEMORY\_SIZE,

.flags = PMM\_ARENA\_FLAG\_KMAP,

};

void platform\_early\_init(void) {

/\* add the main memory arena \*/

pmm\_add\_arena(&arena);

## MMU页表组织

ARM中有两个协处理器寄存器用来存放一级页表基地址，页表基址寄存器TTBR0和TTBR1。操作系统把虚拟内存划分为内核空间和用户空间，TTBR0存放用户空间的一级页表基址，TTBR1存放内核空间的一级页表基址。

页表控制寄存器TTBCR。

ARM CPU中，TTBR0， TTBR1， TTBCR寄存器的操作指令mcr p15, 0, r10, c2, c0, 2。只是最后一个参数分别是0、1、2。

Magenta ARM平台彩用短描述符。

源码：$Magenta/magenta/kernel/arch/arm/arm/mmu.c

#if KERNEL\_ASPACE\_BASE != 0

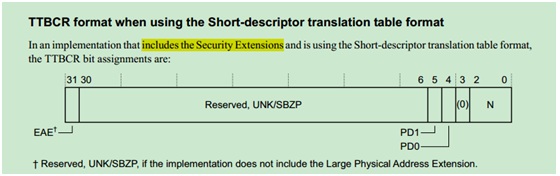
/\* bounce the ttbr over to ttbr1 and leave 0 unmapped \*/

uint32\_t n = \_\_builtin\_clz(KERNEL\_ASPACE\_BASE) + 1;

DEBUG\_ASSERT(n <= 7);

uint32\_t ttbcr = (1<<4) | n; /\* disable TTBCR0 and set the split between TTBR0 and TTBR1 \*/

arm\_write\_ttbr1(arm\_read\_ttbr0());



## 物理内存管理

源码：$Magenta/magenta/kernel/kernel/vm/pmm.cpp

STATIC\_COMMAND("pmm", "physical memory manager", &cmd\_pmm)

## 虚拟地址管理

源码：$Magenta/magenta/kernel/kernel/vm/vmm.cpp

STATIC\_COMMAND("vmm", "virtual memory manager", &cmd\_vmm)

## 虚实映射

源码：Magenta/magenta/kernel/arch/arm/arm/mmu.c

int arch\_mmu\_map(arch\_aspace\_t \*aspace, addr\_t vaddr, paddr\_t paddr, uint count, uint flags)

参数说明：

* aspace：页表地址

struct arch\_aspace {

/\* magic value for use-after-free detection \*/

uint32\_t magic;

/\* pointer to the translation table \*/

paddr\_t tt\_phys;

uint32\_t \*tt\_virt;

/\* range of address space \*/

vaddr\_t base;

size\_t size;

/\* list of pages allocated for these page tables \*/

struct list\_node pt\_page\_list;

};

* vaddr：虚拟地址空间
* paddr：物理地址
* count：页数
* flags：属性

# 中断

现代操作系统是中断驱动的。如果没有进程可执行，没有I/O设备可服务，没有用户可响应，那么操作系统就会安静的等待事件的发生。

事件的发生几乎总是通过中断或者陷阱来表征的。

陷阱（trap）或异常（exception）是因错误（如除0、非法访问内存）或者用户程序（执行操作系统服务）的特定请求所引起的软件生成中断。

对于中断，硬件可以随时通过系统总线向cpu发出信号，触发中断。

软件通过执行系统调用的特别操作触发中断。

对于每种类型的中断，操作系统都有一段独立的代码决定采取动作，中断服务子程序负责处理中断。

中断系统中的中断发生后，系统停止响应，并执行中断响应，这个过程就叫系统中断。

所谓中断是指CPU对系统发生的某个事件做出的一种反应，CPU暂停正在执行的程序，保留现场后自动地转去执行相应的处理程序，处理完该事件后再返回断点继续执行被“打断”的程序。

**中断可分为三类：**

第一类是由CPU外部引起的，称作中断，如I/O中断、时钟中断、控制台中断等。

第二类是来自CPU的内部事件或程序执行中的事件引起的过程，称作异常，如由于CPU本身故障（电源电压低于105V或频率在47～63Hz之外）、程序故障（非法操作码、地址越界、浮点溢出等）等引起的过程。

第三类由于在程序中使用了请求系统服务的系统调用而引发的过程，称作“陷入”(trap,或者陷阱)。

前两类通常都称作中断，它们的产生往往是无意、被动的，而陷入是有意和主动的。

**中断处理**

中断处理一般分为中断响应和中断处理两个步骤。

中断响应由硬件实施，中断处理主要由软件实施。

（1）中断响应

对中断请求的整个处理过程是由硬件和软件结合起来而形成的一套中断机构实施的。发生中断时，CPU暂停执行当前的程序，而转去处理中断。这个由硬件对中断请求作出反应的过程，称为中断响应。一般说来，中断响应顺序执行下述三步动作：

* 中止当前程序的执行；
* 保存原程序的断点信息（主要是程序计数器PC和程序状态寄存器PS的内容）；
* 从中断控制器取出中断向量，转到相应的处理程序。

通常CPU在执行完一条指令后，立即检查有无中断请求，如果有，则立即做出响应。

当发生中断时，系统作出响应，不管它们是来自硬件（如来自时钟或者外部设备）、程序性中断（执行指令导致“软件中断”—Software Interrupts），或者来自意外事件（如访问页面不在内存）。

如果当前CPU的执行优先级低于中断的优先级，那么它就中止对当前程序下条指令的执行，接受该中断，并提升处理机的执行级别（一般与中断优先级相同），以便在CPU处理当前中断时，能屏蔽其它同级的或低级的中断，然后保存断点现场信息，通过取得的中断向量转到相应的中断处理程序的入口。

（2）中断处理

CPU从中断控制器取得中断向量，然后根据具体的中断向量从中断向量表IDT中找到相应的表项，该表项应是一个中断门。于是，CPU就根据中断门的设置而到达了该通道的总服务程序的入口。

核心对中断处理的顺序主要由以下动作完成：

* 保存正在运行进程的各寄存器的内容，把它们放入核心栈的新帧面中。
* 确定“中断源”或核查中断发生，识别中断的类型（如时钟中断或盘中断）和中断的设备号（如哪个磁盘引起的中断）。系统接到中断后，就从机器那里得到一个中断号，它是检索中断向量表的位移。中断向量因机器而异，但通常都包括相应中断处理程序入口地址和中断处理时处理机的状态字。
* 核心调用中断处理程序，对中断进行处理。
* 中断处理完成并返回。中断处理程序执行完以后，核心便执行与机器相关的特定指令序列，恢复中断时寄存器内容和执行核心栈退栈，进程回到用户态。如果设置了重调度标志，则在本进程返回到用户态时做进程调度。

中断向量

中断必须将控制转移到合适的中断服务程序，处理这种转移最简单的方法是调用一个通用子程序以检查中断信息，接着，该子程序调用相应的中断处理程序。

处理中断必须要快，通过使用中断处理子程序的指针表可间接调用中断处理子程序，而不需要其他中间子程序。通常指针表位于低内存地址（前一百左右的位置）这些位置包含各种设备中断处理子程序的地址（即中断向量）．中断向量对于给定的中断请求通过唯一设备号来索引，以提供设备的中断处理子程序的地址。

中断体系结构也保持被中断指令的地址（系统堆栈中存储返回地址），处理中断后，保存的返回地址会装入程序计数器，被中断的计算可以重新开始，就好像中断没有发生过一样。

## 内核态中断编程

如果是多核CPU，下面这些函数都是针对当前核来说的。

源码：$Magenta/magenta/kernel/dev/interrupt/include/dev/interrupt.h

enum interrupt\_trigger\_mode {

IRQ\_TRIGGER\_MODE\_EDGE = 0,

IRQ\_TRIGGER\_MODE\_LEVEL = 1,

};

enum interrupt\_polarity {

IRQ\_POLARITY\_ACTIVE\_HIGH = 0,

IRQ\_POLARITY\_ACTIVE\_LOW = 1,

};

status\_t mask\_interrupt(unsigned int vector);

status\_t unmask\_interrupt(unsigned int vector);

// Configure the specified interrupt vector. If it is invoked, it muust be

// invoked prior to interrupt registration

status\_t configure\_interrupt(unsigned int vector,

enum interrupt\_trigger\_mode tm,

enum interrupt\_polarity pol);

//中断处理函数原型

typedef enum handler\_return (\*int\_handler)(void\* arg);

//注册中断向量

void register\_int\_handler(unsigned int vector, int\_handler handler, void\* arg);

bool is\_valid\_interrupt(unsigned int vector, uint32\_t flags);

unsigned int remap\_interrupt(unsigned int vector);

## 用户态中断编程

Magenta提供的用户态编程的API：

* mx\_handle\_t mx\_interrupt\_create(mx\_handle\_t handle, uint32\_t vector, uint32\_t flags)
* mx\_status\_t mx\_interrupt\_complete(mx\_handle\_t handle)

## 中断程序执行过程

ARM平台，中断IRQ都是从同一个函数platform\_irq开始工作的。

源码：$Magenta/magenta/kernel/arch/arm/arm/exceptions.S

FUNCTION(arm\_irq)

#if TIMESTAMP\_IRQ

/\* read the cycle count \*/

mrc p15, 0, sp, c9, c13, 0

str sp, [pc, #\_\_irq\_cycle\_count - . - 8]

#endif

save\_offset #4

/\* r0 now holds pointer to iframe \*/

/\* track that we're inside an irq handler \*/

LOADCONST(r2, \_\_arm\_in\_handler)

mov r1, #1

str r1, [r2]

/\* call into higher level code \*/

bl platform\_irq

/\* clear the irq handler status \*/

LOADCONST(r1, \_\_arm\_in\_handler)

mov r2, #0

str r2, [r1]

/\* reschedule if the handler returns nonzero \*/

cmp r0, #0

blne thread\_preempt

restore

源码：$Magenta/magenta/kernel/dev/interrupt/arm\_gic/arm\_gic.c

enum handler\_return platform\_irq(struct iframe \*frame)

{

#if WITH\_LIB\_SM

uint32\_t ahppir = GICREG(0, GICC\_AHPPIR);

uint32\_t pending\_irq = ahppir & 0x3ff;

struct int\_handler\_struct \*h;

uint cpu = arch\_curr\_cpu\_num();

LTRACEF("ahppir %d\n", ahppir);

if (pending\_irq < MAX\_INT && get\_int\_handler(pending\_irq, cpu)->handler) {

enum handler\_return ret = 0;

uint32\_t irq;

uint8\_t old\_priority;

spin\_lock\_saved\_state\_t state;

spin\_lock\_save(&gicd\_lock, &state, GICD\_LOCK\_FLAGS);

/\* Temporarily raise the priority of the interrupt we want to

\* handle so another interrupt does not take its place before

\* we can acknowledge it.

\*/

old\_priority = arm\_gic\_get\_priority(pending\_irq);

arm\_gic\_set\_priority\_locked(pending\_irq, 0);

DSB;

irq = GICREG(0, GICC\_AIAR) & 0x3ff;

arm\_gic\_set\_priority\_locked(pending\_irq, old\_priority);

spin\_unlock\_restore(&gicd\_lock, state, GICD\_LOCK\_FLAGS);

LTRACEF("irq %d\n", irq);

if (irq < MAX\_INT && (h = get\_int\_handler(pending\_irq, cpu))->handler)

ret = h->handler(h->arg);

else

TRACEF("unexpected irq %d != %d may get lost\n", irq, pending\_irq);

GICREG(0, GICC\_AEOIR) = irq;

return ret;

}

return sm\_handle\_irq();

#else

return \_\_platform\_irq(frame);

#endif

}

# 文件系统

总体上说 Magenta 下的文件系统主要可分为三大块：一是上层的文件系统的系统调用，二是虚拟文件系统 VFS(Virtual Filesystem System)，三是挂载到 VFS 中的各实际文件系统，例如 FAT16、FAT32 等。

VFS 是一种软件机制，也许称它为 Magenta 的文件系统管理者更确切点，与它相关的数据结构只存在于物理内存当中。所以在每次系统初始化期间，Linux 都首先要在内存当中构造一棵 VFS 的目录树(在 Linux 的源代码里称之为 namespace)，实际上便是在内存中建立相应的数据结构。VFS 目录树在 Linux 的文件系统模块中是个很重要的概念，希望读者不要将其与实际文件系统目录树混淆，在笔者看来，VFS 中的各目录其主要用途是用来提供实际文件系统的挂载点，当然在 VFS 中也会涉及到文件级的操作，本文不阐述这种情况。下文提到目录树或目录，如果不特别说明，均指 VFS 的目录树或目录。图 9‑1是一种可能的目录树在内存中的影像。

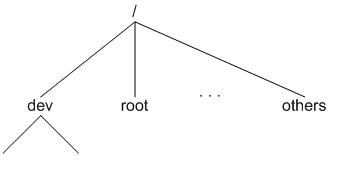


图 ‑1 Magenta文件系统结构

## 内核虚拟文件系统MXIO

mxio是一个接口约定，只要实现了这个接口函数，到系统里登记一下，就成为文件系统中的一部分了。

源码：$Magenta/magenta/system/ulib/mxio/private.h

// MXIO provides open/close/read/write io over various transports

// via the mxio\_t interface abstraction.

//

// The PIPE protocol uses message ports as simple, no-flow-control

// io pipes with a maximum message size of MX\_PIPE\_SIZE.

//

// The REMOTEIO protocol uses message ports to implement simple

// synchronous remoting of read/write/close operations.

//

// The NULL protocol absorbs writes and is never readable.

typedef struct mxio\_ops {

ssize\_t (\*read)(mxio\_t\* io, void\* data, size\_t len);

ssize\_t (\*read\_at)(mxio\_t\* io, void\* data, size\_t len, off\_t offset);

ssize\_t (\*write)(mxio\_t\* io, const void\* data, size\_t len);

ssize\_t (\*write\_at)(mxio\_t\* io, const void\* data, size\_t len, off\_t offset);

off\_t (\*seek)(mxio\_t\* io, off\_t offset, int whence);

mx\_status\_t (\*misc)(mxio\_t\* io, uint32\_t op, uint32\_t maxreply, void\* data, size\_t len);

mx\_status\_t (\*close)(mxio\_t\* io);

mx\_status\_t (\*open)(mxio\_t\* io, const char\* path, int32\_t flags, uint32\_t mode, mxio\_t\*\* out);

mx\_status\_t (\*clone)(mxio\_t\* io, mx\_handle\_t\* out\_handles, uint32\_t\* out\_types);

mx\_status\_t (\*wait)(mxio\_t\* io, uint32\_t events, uint32\_t\* pending, mx\_time\_t timeout);

ssize\_t (\*ioctl)(mxio\_t\* io, uint32\_t op, const void\* in\_buf, size\_t in\_len, void\* out\_buf, size\_t out\_len);

} mxio\_ops\_t;

程序调用关系：

typedef struct mxrio mxrio\_t;

struct mxrio {

// base mxio io object

mxio\_t io;

// message pipe handle for rpc

mx\_handle\_t h;

// event handle for device state signals

mx\_handle\_t e;

uint32\_t flags;

// TODO: replace with reply-pipes to allow

// true multithreaded io

mtx\_t lock;

};

创建一个文件系统。

mxio\_t\* mxio\_remote\_create(mx\_handle\_t h, mx\_handle\_t e) {

mxrio\_t\* rio = calloc(1, sizeof(\*rio));

if (rio == NULL)

return NULL;

rio->io.ops = &mx\_remote\_ops;

rio->io.magic = MXIO\_MAGIC;

rio->io.refcount = 1;

rio->h = h;

rio->e = e;

mtx\_init(&rio->lock, mtx\_plain);

return &rio->io;

}

源码：$Magenta/magenta/system/ulib/mxio/remoteio.c

static mx\_status\_t mxrio\_open(mxio\_t\* io, const char\* path, int32\_t flags, uint32\_t mode, mxio\_t\*\* out)

----打开，就是要打开句柄，于是这个函数调用mxio\_from\_handles ----🡪

源码：$Magenta/magenta/system/ulib/mxio/remoteio.c

mx\_status\_t mxio\_from\_handles(uint32\_t type, mx\_handle\_t\* handles, int hcount,

void\* extra, uint32\_t esize, mxio\_t\*\* out) {

case MXIO\_PROTOCOL\_REMOTE:

case MXIO\_PROTOCOL\_PIPE:

case MXIO\_PROTOCOL\_VMOFILE: {

源码：$Magenta/magenta/system/ulib/mxio/vmofile.c

typedef struct vmofile {

mxio\_t io;

mx\_handle\_t vmo;

mx\_off\_t off;

mx\_off\_t end;

mx\_off\_t ptr;

mtx\_t lock;

} vmofile\_t;

### 内置文件系统

系统一起动，就注册起来的几个文件系统，这几个文件系统都是内存文件系统。

源码：$Magenta/magenta/system/uapp/devmgr/vfs-memory.c

vnode\_t\* vfs\_get\_root(void) {

if (vfs\_root\_dn.vnode == NULL) {

vfs\_root\_dn.vnode = &vfs\_root.vn;

//TODO implement fs mount mechanism

dn\_add\_child(&vfs\_root\_dn, devfs\_get\_root()->dnode);

dn\_add\_child(&vfs\_root\_dn, bootfs\_get\_root()->dnode);

dn\_add\_child(&vfs\_root\_dn, memfs\_get\_root()->dnode);

\_mem\_create(&vfs\_root, &vn\_data, "data", 4, true);

}

return &vfs\_root.vn;

}

#### boot

Magenta/magenta/system/uapp/devmgr/vfs-boot.c

static dnode\_t vnb\_root\_dn = {

.name = "boot",

.flags = 4,

.children = LIST\_INITIAL\_VALUE(vnb\_root\_dn.children),

};

加载程序：

源码：$Magenta/magenta/system/uapp/userboot/userboot-elf.c

mx\_vaddr\_t elf\_load\_bootfs(mx\_handle\_t log, mx\_handle\_t proc\_self,

struct bootfs \*fs, mx\_handle\_t proc,

const char\* filename, mx\_handle\_t to\_child,

size\_t\* stack\_size) {

文件系统实现：

源码：$Magenta/magenta/system/uapp/userboot/bootfs.c

#### dev

源码：$Magenta/magenta/system/uapp/devmgr/vfs-device.c

static dnode\_t vnd\_root\_dn = {

.name = "dev",

.flags = 3,

.children = LIST\_INITIAL\_VALUE(vnd\_root\_dn.children),

};

#### data

data是通过这个函数创建的文件系统：

static mx\_status\_t \_mem\_create(mnode\_t\* parent, mnode\_t\*\* out,

const char\* name, size\_t namelen,

bool isdir);

#### tmp

源码：$Magenta/magenta/system/uapp/devmgr/vfs-memory.c

static dnode\_t mem\_root\_dn = {

.name = "tmp",

.flags = 3,

.children = LIST\_INITIAL\_VALUE(mem\_root\_dn.children),

};

# 设备驱动与管理

## 硬件IO

几乎对每一种外设的控制都是通过读写设备上的寄存器来进行的，通常包括控制寄存器、状态寄存器和数据寄存器三大类，外设的寄存器通常被连续地编址。根据CPU体系结构的不同，CPU对IO端口的编址方式有两种：

（1）I/O映射方式（I/O-mapped）

典型地，如X86处理器为外设专门实现了一个单独的地址空间，称为”I/O地址空间”或者”I/O端口空间”，CPU通过专门的I/O指令（如X86的IN和OUT指令）来访问这一空间中的地址单元。

（2）内存映射方式（Memory-mapped）

RISC指令系统的CPU（如ARM、PowerPC等）通常只实现一个物理地址空间，外设I/O端口成为内存的一部分。此时，CPU可以象访问一个内存单元那样访问外设I/O端口，而不需要设立专门的外设I/O指令。　但是，这两者在硬件实现上的差异对于软件来说是完全透明的，驱动程序开发人员可以将内存映射方式的I/O端口和外设内存统一看作是”I/O内存”资源。

一般来说，在系统运行时，外设的I/O内存资源的物理地址是已知的，由硬件的设计决定。但是CPU通常并没有为这些已知的外设I/O内存资源的物理地址预定义虚拟地址范围，驱动程序并不能直接通过物理地址访问I/O内存资源，而必须将它们映射到核心虚地址空间内（通过页表），然后才能根据映射所得到的核心虚地址范围，通过访内指令访问这些I/O内存资源。

Magenta提供的硬件IO API：

* mx\_status\_t sys\_mmap\_device\_memory(mx\_handle\_t hrsrc, uintptr\_t paddr, uint32\_t len,

mx\_cache\_policy\_t cache\_policy,

user\_ptr<void\*> out\_vaddr)

* mx\_status\_t sys\_alloc\_device\_memory(mx\_handle\_t hrsrc, uint32\_t len,

mx\_paddr\_t\* out\_paddr, void\*\* out\_vaddr)

## 驱动程序

驱动程序是安装在driver/$(MODULE\_NAME).so里的动态链接库，编译时模块类型为driver（MODULE\_TYPE := driver），驱动程序不是sysroot的一部分，不产生调用ABI残根、静态链接库等。

涉及到的make文件：

源码：Magenta/magenta/kernel/make/module-driver.mk

# all drivers have a so name so they get installed

ifeq ($(MODULE\_SO\_NAME),)

ifeq ($(MODULE\_NAME),)

MODULE\_NAME := $(basename $(notdir $(MODULE)))

endif

MODULE\_SO\_NAME := $(MODULE\_NAME)

endif

# by default drivers live in lib/driver/...

ifeq ($(MODULE\_SO\_INSTALL\_NAME),)

MODULE\_SO\_INSTALL\_NAME := lib/driver/$(MODULE\_SO\_NAME).so

endif

include make/module-userlib.mk

驱动的make文件示例：

源码：$Magenta/magenta/system/ulib/driver/rules.mk

LOCAL\_DIR := system/uapp/devmgr

MODULE := system/ulib/driver

MODULE\_NAME := driver

MODULE\_TYPE := userlib

MODULE\_SO\_NAME := driver

MODULE\_DEFINES := LIBDRIVER=1

MODULE\_COMPILEFLAGS := -fvisibility=hidden

MODULE\_SRCS := \

$(LOCAL\_DIR)/devhost.c \

$(LOCAL\_DIR)/devhost-api.c \

$(LOCAL\_DIR)/devhost-binding.c \

$(LOCAL\_DIR)/devhost-core.c \

$(LOCAL\_DIR)/devhost-rpc-server.c \

system/udev/kpci/kpci.c \

MODULE\_STATIC\_LIBS := ulib/acpisvc-client ulib/ddk

MODULE\_LIBS := ulib/mxio ulib/launchpad ulib/magenta ulib/musl

include make/module.mk

## 设备管理

随着计算机的周边外设越来越丰富，设备管理已经成为现代操作系统的一项重要任务，在物理上，外设之间是有一种层次关系的，比如把一个U盘插到笔记本上，实际上这个U盘是接在一个USB Hub上，USB Hub又是接在USB 2.0 Host Controller (EHCI)上，最终EHCI又是一个挂在PCI Bus上的设备。这里的一个层次关系是：PCI->EHCI->USB Hub->USB Disk。如果操作系统要进入休眠状态，首先要逐层通知所有的外设进入休眠模式，然后整个系统才可以休眠。因此，需要有一个树状的结构可以把所有的外设组织起来。这就是最初建立Linux设备模型的目的。

当然，Magenta设备模型给我们带来的便利远不止如此。既然已经建立了一个组织所有设备和驱动的树状结构，用户就可以通过这棵树去遍历所有的设备，建立设备和驱动程序之间的联系，根据类型不同也可以对设备进行归类，这样就可以更清晰的去“看”这颗枝繁叶茂的大树。另外，Linux驱动模型把很多设备共有的一些操作抽象出来，大大减少了重复造轮子的可能。同时Magenta设备模型提供了一些辅助的机制，比如引用计数，让开发者可以安全高效的开发驱动程序。达成了以上这些好处之后，我们还得到了一个非常方便的副产品，这就是/dev----一个虚拟的文件系统。/dev给用户提供了一个从用户空间去访问内核设备的方法，它在Magenta里的路径是/dev。这个目录并不是存储在硬盘上的真实的文件系统，只有在系统启动之后才会建起来。

### 设备节点

源码：$Magenta/magenta/system/uapp/devmgr/dnode.h

typedef struct dnode dnode\_t;

#define DN\_NAME\_MAX 255

#define DN\_NAME\_LEN(flags) ((flags) & 0xFF)

#define DN\_TYPE\_MASK 0xF00

#define DN\_TYPE\_DIR 0x100

#define DN\_TYPE\_FILE 0x200

#define DN\_TYPE\_DEVICE 0x300

#define DN\_TYPE\_SYMLINK 0x400

#define DN\_TYPE(flags) ((flags) & DN\_TYPE\_MASK)

struct dnode {

dnode\_t\* parent;

vnode\_t\* vnode;

list\_node\_t children;

list\_node\_t dn\_entry; // entry in parent's list

list\_node\_t vn\_entry; // entry in vnode's list

uint32\_t flags;

char name[];

};

## 设备管理应用devmgr

源码：$Magenta/magenta/system/uapp/devmgr/devmgr.c

## 虚拟文件系统vfs

虚拟文件系统（VFS）是Magenbta内核和具体I/O设备之间的封装的一层共通访问接口，通过这层接口，Magenta内核可以以同一的方式访问各种I/O设备。

虚拟文件系统本身是Magenta内核的一部分，是纯软件的东西，并不需要任何硬件的支持。

源码：$Magenta/magenta/system/uapp/devmgr/vfs.c

## 设备树DeviceTree

*这部分工作还没有纳入最终系统，可是内部设备管理有了，基于描述数据的设备管理，那就应该是肯定的。*

源码：$Magenta/magenta/kernel/lib/devicetree/include/lib/devicetree.h

typedef struct dt\_slice {

u8 \*data;

u32 size;

} dt\_slice\_t;

struct devicetree\_header {

u32 magic;

u32 size;

u32 off\_struct; // offset from start to DT 'structure'

u32 off\_strings; // offset from start to stringdata

u32 off\_reserve; // offset from start to reserve memory map

u32 version;

u32 version\_compat; // last compatible version

u32 boot\_cpuid;

u32 sz\_strings; // size of stringdata

u32 sz\_struct; // size of DT 'structure'

};

typedef struct devicetree {

dt\_slice\_t top;

dt\_slice\_t dt;

dt\_slice\_t ds;

struct devicetree\_header hdr;

void (\*error)(const char \*msg);

} devicetree\_t;

# 编程概念

## Dispatcher

操作系统中scheduler与dispatcher是一个问题的两个角度，scheduler是在计算机资源（计算的执行机构，CPU、IO等）的角度看问题，当我有资源了，要怎么调度？dispatcher是从计算，被调度体的角度看问题，你有CPU资源了，我这里有N个可被执行的（进程、线程、事件、锁等概念的综合体）对象；你有IO了，我这里有N个IO的对象。

Dispatcher是一个靠引用计数管理的用来管理句柄的一个c++类。

源码：$Magenta/magenta/kernel/lib/magenta/include/magenta/dispatcher.h

// The Kernel Objects. Keep this list sorted.

class DataPipeConsumerDispatcher;

class DataPipeProducerDispatcher;

class InterruptDispatcher;

class IoMappingDispatcher;

class IOPortDispatcher;

class LogDispatcher;

class MessagePipeDispatcher;

class PciDeviceDispatcher;

class PciInterruptDispatcher;

class ProcessDispatcher;

class SocketDispatcher;

class ThreadDispatcher;

class VmObjectDispatcher;

class WaitSetDispatcher;

class ResourceDispatcher;

class Dispatcher : public mxtl::RefCounted<Dispatcher> {

public:

Dispatcher();

virtual ~Dispatcher() {}

mx\_koid\_t get\_koid() const { return koid\_; }

void add\_handle();

void remove\_handle();

通过下面这段程序，了解一下句柄与Dispatcher的关系。

源码：$Magenta/magenta/kernel/lib/syscalls/syscalls\_magenta.cpp

mx\_handle\_t sys\_port\_create(uint32\_t options) {

LTRACEF("options %u\n", options);

mxtl::RefPtr<Dispatcher> dispatcher;

mx\_rights\_t rights;

mx\_status\_t result = IOPortDispatcher::Create(options, &dispatcher, &rights);

if (result != NO\_ERROR)

return result;

//$Magenta/magenta/system/ulib/mxtl/include/mxtl/type\_support.h

//template <typename T>

//constexpr typename remove\_reference<T>::type&& move(T&& t) {

/ return static\_cast<typename remove\_reference<T>::type&&>(t);

//}

HandleUniquePtr handle(MakeHandle(mxtl::move(dispatcher), rights));

if (!handle)

return ERR\_NO\_MEMORY;

auto up = ProcessDispatcher::GetCurrent();

//把handle变为外面可访问的值，隐藏实现信息

mx\_handle\_t hv = up->MapHandleToValue(handle.get());

up->AddHandle(mxtl::move(handle));

return hv;

}

源码：$Magenta/magenta/kernel/lib/magenta/io\_port\_dispatcher.cpp

mx\_status\_t IOPortDispatcher::Create(uint32\_t options,

mxtl::RefPtr<Dispatcher>\* dispatcher,

mx\_rights\_t\* rights) {

AllocChecker ac;

auto disp = new (&ac) IOPortDispatcher(options);

if (!ac.check())

return ERR\_NO\_MEMORY;

\*rights = kDefaultIOPortRights;

//持有一个引用计数

\*dispatcher = mxtl::AdoptRef<Dispatcher>(disp);

return NO\_ERROR;

}

## 信号Signal

信号（Signal）是Magenta对象间通讯的一种方式。它是一种异步的通知机制，用来提醒内核对象一个事件已经发生。

源码：$Magenta/magenta/system/public/magenta/types.h

typedef uint32\_t mx\_signals\_t;

#define MX\_SIGNAL\_NONE ((mx\_signals\_t)0u)

#define MX\_SIGNAL\_READABLE ((mx\_signals\_t)1u << 0)

#define MX\_SIGNAL\_WRITABLE ((mx\_signals\_t)1u << 1)

#define MX\_SIGNAL\_PEER\_CLOSED ((mx\_signals\_t)1u << 2)

#define MX\_SIGNAL\_SIGNALED MX\_SIGNAL\_SIGNAL0

#define MX\_SIGNAL\_SIGNAL0 ((mx\_signals\_t)1u << 3)

#define MX\_SIGNAL\_SIGNAL1 ((mx\_signals\_t)1u << 4)

#define MX\_SIGNAL\_SIGNAL2 ((mx\_signals\_t)1u << 5)

#define MX\_SIGNAL\_SIGNAL3 ((mx\_signals\_t)1u << 6)

#define MX\_SIGNAL\_SIGNAL4 ((mx\_signals\_t)1u << 7)

#define MX\_SIGNAL\_SIGNAL\_ALL ((mx\_signals\_t)31u << 3)

typedef struct {

mx\_signals\_t satisfied;

mx\_signals\_t satisfiable;

} mx\_signals\_state\_t;

数据结构mx\_signals\_state\_t用来存储信号状态。

数据结构mx\_signals\_state\_t中，satisfied是一个已经发生的信号的比特图bitmap，satisfiable是可能发生的信号的比特图bitmap。

#### 适定性(Satisfiability)问题

关于数据结构mx\_signals\_state\_t为什么要设两个域，satisfied、satisfiable的问题。

适定性(Satisfiability)问题，简称 SAT。k-适定性问题，简称 k-SAT。

所谓2-SAT就是2元可满足性问题。首先，作为众所周知的，任何布尔表达式，都可以化为合取范式的形式，即化为： () and () and () ...and () 其中括号里面的是用析取符号or 连接的变量或者变量的非的形式。我们一般称，变量或者变量的非为“文字”,而括号里的叫做子句。可满足性问题是要给所有的变量一个赋值（真或假）使得表达式值为真。而2元可满足性问题，就是化为合取范式后，每个子句最多有两个文字的可满足性问题。

<https://en.wikipedia.org/wiki/2-satisfiability>

In computer science, 2-satisfiability (abbreviated as 2-SAT or just 2SAT) is the problem of determining whether a collection of two-valued (Boolean or binary) variables with constraints on pairs of variables can be assigned values satisfying all the constraints. It is a special case of the general Boolean satisfiability problem, which can involve constraints on more than two variables, and of constraint satisfaction problems, which can allow more than two choices for the value of each variable. But in contrast to those more general problems, which are NP-complete, 2-satisfiability can be solved in polynomial time.

<https://zh.wikipedia.org/wiki/%E5%B8%83%E5%B0%94%E5%8F%AF%E6%BB%A1%E8%B6%B3%E6%80%A7%E9%97%AE%E9%A2%98>

可满足性（英语：Satisfiability）是用来解决给定的布尔方程式，是否存在一组变量赋值，使问题为可满足。布尔可满足性问题（Boolean satisfiability problem；SAT)）属于决定性问题，是第一个被证明NP完全问题。为计算机科学上许多领域的重要问题，包括计算机科学基础理论、算法、人工智能、硬件设计等等。

布尔可满足性问题是第一个被证明的NPC问题。

**直观描述**

对于一个确定的逻辑电路，是否存在一种输入使得输出为真。

## 内核对象唯一标识值

每个内核对象都有一个唯一标识值，它是一个64位的整数。

源码：$Magenta/magenta/kernel/lib/magenta/dispatcher.cpp

mx\_koid\_t Dispatcher::GenerateKernelObjectId() {

return atomic\_add\_u64(&global\_koid, 1ULL);

}

## StateTracker/ StateObserver

一个事务，如套接字（socket）、消息管道（message pipe）都有需要调度者了解的状态信息，这些事务在编程者看来，是通过一个句柄表示的。于是有了状态跟踪与发现，比如非中断状态跟踪NonIrqStateTrackerTraits、中断状态跟踪IrqStateTrackerTraits。

using NonIrqStateTracker = internal::StateTrackerImpl<internal::NonIrqStateTrackerTraits>;

class IrqStateTracker : public internal::StateTrackerImpl<internal::IrqStateTrackerTraits>

源码：$Magenta/magenta/kernel/lib/magenta/include/magenta/state\_tracker.h

class StateTracker

源码：$Magenta/magenta/kernel/lib/magenta/include/magenta/state\_observer.h

// Observer base class for state maintained by StateTracker.

class StateObserver

#### Design Pattern Observer观察者模式

观察者模式定义了一种一对多的依赖关系，让多个观察者对象同时监听某一个主题对象。这个主题对象在状态上发生变化时，会通知所有观察者对象，使它们能够自动更新自己。

观察者模式是使用频率最高的设计模式之一，它用于建立一种对象与对象之间的依赖关系，一个对象发生改变时将自动通知其他对象，其他对象将相应作出反应。在观察者模式中，发生改变的对象称为观察目标，而被通知的对象称为观察者，一个观察目标可以对应多个观察者，而且这些观察者之间可以没有任何相互联系，可以根据需要增加和删除观察者，使得系统更易于扩展。

观察者模式定义如下： 观察者模式(Observer Pattern)：定义对象之间的一种一对多依赖关系，使得每当一个对象状态发生改变时，其相关依赖对象皆得到通知并被自动更新。观察者模式的别名包括发布-订阅（Publish/Subscribe）模式、模型-视图（Model/View）模式、源-监听器（Source/Listener）模式或从属者（Dependents）模式。观察者模式是一种对象行为型模式。

## 资源Resource

源码：$Magenta/magenta/kernel/lib/magenta/include/magenta/resource\_dispatcher.h

class ResourceDispatcher : public Dispatcher

## 异常处理ExceptionPort

CPU的异常发生后，把这个异常交给谁呢？哪些系统行为会引起异常？

* 线程

status\_t UserThread::SetExceptionPort(ThreadDispatcher\* td, mxtl::RefPtr<ExceptionPort> eport)

status\_t ThreadDispatcher::SetExceptionPort(mxtl::RefPtr<ExceptionPort> eport)

* 进程

status\_t ProcessDispatcher::SetExceptionPort(mxtl::RefPtr<ExceptionPort> eport)

## 事件对（EventPair）

EventPair，事件对，一个事件句柄有了啥signal，立马通知另外一个，操作系统内核帮你干的，对于应用程序来说，它们是“同时”有了 signal的。

“事件对”思想的由来

在Windows 98和Windows NT 3.X年代，Windows中的环境子系统(csrss)进程还负责着Windows的图像图形系统核心的任务，其他任何程序需要在屏幕上绘图，系统都需要通过IPC手段通知csrss让其根据相关数据去绘制，所以其他Windows程序进程跟csrss的通讯效率就至关重要，这里微软的程序员就为了csrss的高效通讯加入了一种内核对象，就是现在一直都存在并且再也不会更新的“EventPair”对象。

而后Windows NT将绘图的任务移入了内核模块win32k.sys，csrss肩负的东西一下就少了很多，到现在在绘图上面也仅仅是承担着对控制台窗口的图像绘制任务，但当年那个为了csrss而设置EventPair对象则一直存在于Windows内，并且直到今天的Win7、Win8。

而又由于这个对象本是为了csrss而设置的，而csrss很快又“残疾”了，所以现在微软依然没有把这个对象的相关接口公开进Win32 API里面，不过那么多年过来了，虽然这个对象没有更新功能接口，不过看样子微软也不准把它删掉，所以大家也可以放心的在自己的程序里使用。（注：商业程序请慎重考虑）

而为什么又叫做Pair呢？因为一个EventPair对象就是2个Event对象，有“高位”和“低位”之分，分别给Server\Client使用。

## 状态信息status\_t

This describes the set of userspace-exposed errors used in Magenta. The first section provides the canonical names and description of each error code. The second section provides the concrete values.

Within the kernel, errors are typically resulted as variables of type status\_t and errors are defined by macros of the form ERR\_CANONICAL\_NAME e.g. ERR\_INTERNAL. All error cases are negative values and success is represented by a non-negative value.

In userspace the syscall dispatch layer (libmagenta) exposes the result values as variables of type mx\_status\_t that currently use the same spelling and values as the kernel for errors, but which will transition to using 0 for success and positive values for errors.

See Kernel internal errors for a list of kernel-internal values.

### Descriptions

Each category represents a class of errors. The first error code in each category is the generic code for that category and is used when no more specific code applies. Further error codes (if any) within a category represent particular types of errors within the class. In general, more specific error codes are preferred where possible.

Errors are described in terms of an operation, arguments, a subject, and identifiers. An operation is typically a function or system call. Arguments are typically the parameters to the call. The subject of an operation is the primary object the operation acts on, typically a handle and typically passed as the first argument. Identifiers are typically numbers or strings intended to unambiguously identify a resource used in the operation.

### Categories

所有错误信息在这里定义。

源码：$Magenta/magenta/system/public/magenta/fuchsia-types.h

#### Success

NO\_ERROR Operation succeeded.

#### General errors

These indicate that the system hit a general error while attempting the operation.

INTERNAL The system encountered an otherwise unspecified error while performing the operation.

NOT\_SUPPORTED The operation is not supported, implemented, or enabled.

NO\_RESOURCES The system was not able to allocate some resource needed for the operation.

NO\_MEMORY The system was not able to allocate memory needed for the operation.

#### Parameter errors

These indicate that the caller specified a parameter that does not specify a valid operation or that is invalid for the specified operation.

INVALID\_ARGUMENT An argument is invalid.

WRONG\_TYPE The subject of the operation is the wrong type to perform the operation.

Example: Attempting a message\_read on a thread handle.

BAD\_SYSCALL The specified syscall number is invalid.

BAD\_HANDLE A specified handle value does not refer to a handle.

OUT\_OF\_RANGE An argument is outside the valid range for this operation.

Note: This is used when the argument may be valid if the system changes state, unlike INVALID\_ARGUMENT which is used when the argument will never be valid.

BUFFER\_TOO\_SMALL A caller provided buffer is too small for this operation.

#### Precondition or state errors

These indicate that the operation could not succeed because the preconditions for the operation are not satisfied or the system is unable to complete the operation in its current state.

BAD\_STATE The system is unable to perform the operation in its current state.

Note: FAILED\_PRECONDITION is a reserved alias for this error

NOT\_FOUND The requested entity was not found.

TIMED\_OUT The time limit for the operation elapsed before the operation completed.

ALREADY\_EXISTS An object with the specified identifier already exists.

Example: Attempting to create a file when a file already exists with that name.

ALREADY\_BOUND The operation failed because the named entity is already owned or controlled by another entity. The operation could succeed later if the current owner releases the entity.

HANDLE\_CLOSED A handle being waited on was closed.

REMOTE\_CLOSED The operation failed because the remote end of the subject of the operation was closed.

UNAVAILABLE The subject of the operation is currently unable to perform the operation.

Note: This is used when there's no direct way for the caller to observe when the subject will be able to perform the operation and should thus retry.

SHOULD\_WAIT The operation cannot be performed currently but potentially could succeed if the caller waits for a prerequisite to be satisfied, for example waiting for a handle to be readable or writable.

Example: Attempting to read from a message pipe that has no messages waiting but has an open remote will return SHOULD\_WAIT. Attempting to read from a message pipe that has no messages waiting and has a closed remote end will return REMOTE\_CLOSED.

#### Permission errors

ACCESS\_DENIED The caller did not have permission to perform the specified operation.

Input/output errors

IO Otherwise unspecified error occurred during I/O.

IO\_REFUSED The entity the I/O operation is being performed on rejected the operation.

Example: an I2C device NAK'ing a transaction or a disk controller rejecting an invalid command.

IO\_DATA\_INTEGRITY The data in the operation failed an integrity check and is possibly corrupted.

Example: CRC or Parity error.

IO\_DATA\_LOSS The data in the operation is currently unavailable and may be permanently lost.

Example: A disk block is irrecoverably damaged.

# 编程基础设施

## mxtl，c++模板

源码：$Magenta/magenta/system/ulib/mxtl/include/mxtl/ref\_ptr.h

namespace mxtl {

### 智能指针

#### ref\_ptr

智能指针可以自动管理用户在堆上创建的对象的生命周期，让用户不用负责内存回收，避免内存泄漏。一般的智能指针都定义为一个模板类，它的类型由被管理的对象类型初始化，内部包含了指向该对象的指针以及指向辅助生命周期管理的管理对象的指针。

源码：$Magenta/magenta/system/ulib/mxtl/include/mxtl/ref\_ptr.h

// RefPtr<T> holds a reference to an intrusively-refcounted object of type T.

//

// T should be a subclass of mxtl::RefCounted<>, or something that adheres to

// the

// same contract for AddRef() and Release().

//

// Except for initial construction (see below), this generally adheres to a

// subset of the interface for std::shared\_ptr<>. Unlike std::shared\_ptr<> this

// type does not support conversions between different pointer types, vending

// weak pointers, introspecting the reference count, or any operations that

// would result in allocating memory (unless T::AddRef or T::Release allocate

// memory).

//

// Construction: To create a RefPtr around a freshly created object, use the

// AdoptRef free function at the bottom of this header. To construct a RefPtr to

// hold a reference to an object that already exists use the copy or move

// constructor or assignment operator.

#### unique\_ptr

源码：$Magenta/magenta/system/ulib/mxtl/include/mxtl/unique\_ptr.h

auto\_ptr通过复制构造或者通过=赋值后,原来的auto\_ptr对象就报废了.所有权转移到新的对象中去了.而通过shared\_ptr可以让多个智能指针对象同时拥有某一块内存的访问权.但假如我们不希望多个内存块被多个智能指针对象共享,同时又不会像auto\_ptr那样不知不觉的就让原来的auto\_ptr对象失效,可咋整呢?

这个时候就要使用unique\_ptr了,顾名思义嘛,unique是唯一的意思.说明它跟auto\_ptr有点类似,就是同时只能有一个智能指针对象指向某块内存.但它还有些其他特性.

// This is a simplified version of std::unique\_ptr that supports custom

// stateless deleters but doesn't support type conversions between different

// pointer types.

### 数据类型支持type\_support

源码：$Magenta/magenta/system/ulib/mxtl/include/mxtl/type\_support.h

template <typename T>

constexpr typename remove\_reference<T>::type&& move(T&& t) {

return static\_cast<typename remove\_reference<T>::type&&>(t);

}

### 资源获取即初始化RAII

RAII是resource acquisition is initialization的缩写，意为“资源获取即初始化”。它是C++之父Bjarne Stroustrup提出的设计理念，其核心是把资源和对象的生命周期绑定，对象创建获取资源，对象销毁释放资源。

软件开发中，会用到各种各样的资源。狭义的资源指内存，而广义的资源包括文件、网络连接、数据库连接、信号量、事件、线程、内存等，甚至可以是状态。资源获取后由于种种原因导致永久不能释放的资源称为资源泄漏。针对资源泄漏，提出了各种各样的软件机制和程序设计惯用法,如垃圾收集、RRID、RAII、确定性资源清理等。

RAII是C++语言的一种管理资源、避免泄漏的惯用法。C++标准保证任何情况下，已构造的对象最终会销毁，即它的析构函数最终会被调用。简单的说，RAII 的做法是使用一个对象，在其构造时获取资源，在对象生命期控制对资源的访问使之始终保持有效，最后在对象析构的时候释放资源。

RAII的理念固然简单，不过在具体实现的时候仍有需要小心的地方。比如对于STL的auto\_ptr，可以视为资源的代理对象，auto\_ptr对象间的赋值是一个需要特别注意的地方。简单说来资源代理对象间赋值的语义不满足“赋值相等”，其语义是资源管理权的转移。

什么是“赋值相等”呢？比如：

int a;

int b = 10;

a = b; //这句话执行后 a == b

但对于资源代理对象，这是不满足的，比如：

auto\_ptr<int> a(null);

auto\_ptr<int> b(new int(123));

a = b; //这句话执行后a != b，赋值的语义是b把资源的管理权交给了a。

源码：$Magenta/magenta/system/ulib/mxtl/include/mxtl/auto\_call.h

template <typename T>

class AutoCall {

### 容器、链表等

* intrusive\_container\_utils.h
* intrusive\_double\_list.h：mxtl::DoublyLinkedList<>
* intrusive\_hash\_table.h：mxtl::HashTable<>
* intrusive\_pointer\_traits.h
* intrusive\_single\_list.h：mxtl::SinglyLinkedList<>
* intrusive\_wavl\_tree.h

// Implementation Notes:

//

// WAVLTree<> is an implementation of a "Weak AVL" tree; a self

// balancing binary search tree whose rebalancing algorithm was

// originally described in

//

// Bernhard Haeupler, Siddhartha Sen, and Robert E. Tarjan. 2015.

// Rank-Balanced Trees. ACM Trans. Algorithms 11, 4, Article 30 (June 2015), 26 pages.

// DOI=http://dx.doi.org/10.1145/2689412

//

// See also

// https://en.wikipedia.org/wiki/WAVL\_tree

// http://www.cs.princeton.edu/~sssix/papers/rb-trees-talg.pdf

//

// WAVLTree<>s, like HashTables, are associative containers and support all of

// the same key-centric operations (such as find() and insert\_or\_find()) that

// HashTables support.

//

// Additionally, WAVLTree's are internally ordered by key (unlike HashTables

// which are un-ordered). Iteration from begin() to end() runs in amortized

// constant time and will enumerate the elements in monotonically increasing

// order (as defined by the KeyTraits::LessThan operation).

//

// Two additional operations are supported because of the ordered nature of a

// WAVLTree:

// upper\_bound(key) : Finds the element (E) in the tree such that E.key > key

// lower\_bound(key) : Finds the element (E) in the tree such that E.key >= key

//

// The worst depth of a WAVL tree depends on whether or not the tree has ever

// been subject to erase operations.

// ++ If the tree has seen only insert operations, the worst case depth of the

// tree is log\_phi(N), where phi is the golden ratio. This is the same bound

// as that of an AVL tree.

// ++ If the tree has seen erase operations in addition to insert operations,

// the worst case depth of the tree is 2\*log\_2(N). This is the same bound as

// a Red-Black tree.

//

// Insertion runs in O(log) time; finding the location takes O(log) time while

// post-insert rebalancing runs in amortized constant time.

//

// Erase-by-key runs in O(log) time; finding the node to erase takes O(log) time

// while post-erase rebalancing runs in amortized constant time.

//

// Because of the intrusive nature of the container, direct-erase operations

// (AKA, erase operations where the reference to the element to be erased is

// already known) run in amortized constant time.

//

* intrusive\_wavl\_tree\_internal.h
* string\_piece.h：mxtl::StringPiece

// A string-like object that points to a sized piece of memory.

// The string data may or may not be null terminated.

// The string piece does not own the data it points to.

## 内核编程可用程序资源

内核编程头文件：Magenta/magenta/kernel/include/kernel ，这里提供了下列程序资源：

* AutoLock
* AutoSpinLock
* cond
* debug
* event：event\_t
* mp，多CPU支持
* mutex：mutex\_t
* novm：物理内存
* semaphore ：semaphore\_t
* spin\_lock
* thread：thread\_t
* timer：定时器
* vm：虚拟内存
* wait：等待队列

## 内核堆

内核堆在lk\_main中初始化。

源码：$Magenta/magenta/kernel/top/main.c

/\* called from arch code \*/

void lk\_main(ulong arg0, ulong arg1, ulong arg2, ulong arg3)

{

…… …… ……

dprintf(SPEW, "initializing heap\n");

heap\_init();

源码中的两个堆算法，cmpctmallc和miniheap，最后选择哪一个，是在编译阶段确定的。

源码：$Magenta/magenta/kernel/lib/heap/rules.mk

# pick a heap implementation

ifndef LK\_HEAP\_IMPLEMENTATION

LK\_HEAP\_IMPLEMENTATION=miniheap

endif

ifeq ($(LK\_HEAP\_IMPLEMENTATION),miniheap)

MODULE\_DEPS := lib/heap/miniheap

endif

ifeq ($(LK\_HEAP\_IMPLEMENTATION),cmpctmalloc)

MODULE\_DEPS := lib/heap/cmpctmalloc

endif

### cmpctmalloc

这个算法最早是lk工程里，chromium中也用到它。

源码：$Magenta/magenta/kernel/lib/heap/cmpctmalloc/cmpctmalloc.c

下面一段讨论的话来源于：<https://groups.google.com/forum/#!topic/dartino-discuss/rf-Q1MIfEDQ>

Q: Does it extensively use heap? Or does it use mostly Data and BSS sections. There is a notion in embedded industry (atleast in safety related applications) to stay away from using heap (malloc, free, etc). Since most requirements are already known at compile time and to avoid failures due to memory fragmentation (which are very hard to reproduce during tests) or lack of memory.

A: We try to avoid allocating on the malloc heap, but we haven't been through the system with a fine-toothed comb and there may still be silly places where we use it. Again, the debugger "doesn' count" since it won't be active on a production system. There's a malloc implementation that we normally use, cmpctmalloc, which is very eager to coalesce adjacent free areas, but of course you can still get fragmentation.

A: We provide full access to allocation on the C-heap from Dart code running in the VM through our FFI (foreign function interface) API, in order to integrate well with existing C libraries. However, that part is something that the programmer is in full control of. An alternative pattern to using BSS could be to allocate what is needed outside Dartino's own heap through malloc during startup.

### miniheap

源码：$Magenta/magenta/kernel/lib/heap/miniheap/miniheap.c

### 物理内存申请

源码：Magenta/magenta/kernel/lib/heap/page\_alloc.c

/\* A simple page-aligned wrapper around the pmm or novm implementation of

\* the underlying physical page allocator. Used by system heaps or any

\* other user that wants pages of memory but doesn't want to use LK

\* specific apis.

\*/

### c++ new/delete支持及AllocChecker

源码：$Magenta/magenta/kernel/lib/libc/include/new.h

class AllocChecker {

public:

AllocChecker();

~AllocChecker();

void arm(size\_t sz, bool result);

bool check();

private:

unsigned state\_;

};

源码：$Magenta/magenta/kernel/lib/heap/new.cpp

enum : unsigned {

alloc\_armed = 1,

alloc\_ok = 2,

};

void panic\_if\_armed(unsigned state) {

#if LK\_DEBUGLEVEL > 1

if (state & alloc\_armed)

panic("AllocChecker::check() needs to be called\n");

#endif

}

AllocChecker::AllocChecker() : state\_(0U) {

}

AllocChecker::~AllocChecker() {

panic\_if\_armed(state\_);

}

void AllocChecker::arm(size\_t sz, bool result) {

panic\_if\_armed(state\_);

state\_ = alloc\_armed |

((sz == 0u) ? alloc\_ok : (result ? alloc\_ok : 0u));

}

bool AllocChecker::check() {

state\_ &= ~alloc\_armed;

return (state\_ & alloc\_ok) == alloc\_ok;

}

void \*operator new(size\_t s, AllocChecker\* ac) {

auto mem = malloc(s);

ac->arm(s, mem != nullptr);

return mem;

}

void \*operator new[](size\_t s, AllocChecker\* ac) {

auto mem = malloc(s);

ac->arm(s, mem != nullptr);

return mem;

}

void \*operator new(size\_t , void \*p) {

return p;

}

void operator delete(void \*p) {

return free(p);

}

void operator delete[](void \*p) {

return free(p);

}

## 用户堆/c库

Magenta采用musl作为c库。musl里面有堆的实现。

musl的官网地址是：<https://www.musl-libc.org/> musl is lightweight, fast, simple, free, and strives to be correct in the sense of standards-conformance and safety.

## 互斥机制

#### 互斥锁与条件变量为什么要配合着使用

下面这节中所讲的pthread\_cond......的情况与pthread\_mutex......的情况相同。

参考：再谈互斥锁与条件变量！ <http://blog.chinaunix.net/uid-27164517-id-3282242.html>

pthread\_cond\_wait总和一个互斥锁结合使用。在调用pthread\_cond\_wait前要先获取锁。pthread\_cond\_wait函数执行时先自动释放指定的锁，然后等待条件变量的变化。在函数调用返回之前，自动将指定的互斥量重新锁住。

int pthread\_cond\_signal(pthread\_cond\_t \* cond);

pthread\_cond\_signal通过条件变量cond发送消息，若多个消息在等待，它只唤醒一个。pthread\_cond\_broadcast可以唤醒所有。调用pthread\_cond\_signal后要立刻释放互斥锁，因为pthread\_cond\_wait的最后一步是要将指定的互斥量重新锁住，如果pthread\_cond\_signal之后没有释放互斥锁，pthread\_cond\_wait仍然要阻塞。

无论哪种等待方式，都必须和一个互斥锁配合，以防止多个线程同时请求pthread\_cond\_wait()（或pthread\_cond\_timedwait()，下同）的竞争条件（Race Condition）。mutex互斥锁必须是普通锁（PTHREAD\_MUTEX\_TIMED\_NP）或者适应锁 （PTHREAD\_MUTEX\_ADAPTIVE\_NP），且在调用pthread\_cond\_wait()前必须由本线程加锁 （pthread\_mutex\_lock()），而在更新条件等待队列以前，mutex保持锁定状态，并在线程挂起进入等待前解锁。在条件满足从而离开 pthread\_cond\_wait()之前，mutex将被重新加锁，以与进入pthread\_cond\_wait()前的加锁动作对应。

激发条件有两种形式，pthread\_cond\_signal()激活一个等待该条件的线程，存在多个等待线程时按入队顺序激活其中一个；而pthread\_cond\_broadcast()则激活所有等待线程。

下面是另一处说明：给出了函数运行全过程。 为什么在唤醒线程后要重新mutex加锁？

了解 pthread\_cond\_wait() 的作用非常重要 -- 它是 POSIX 线程信号发送系统的核心，也是最难以理解的部分。

首先，让我们考虑以下情况：线程为查看已链接列表而锁定了互斥对象，然而该列表恰巧是空的。这一特定线程什么也干不了 -- 其设计意图是从列表中除去节点，但是现在却没有节点。因此，它只能：

锁定互斥对象时，线程将调用 pthread\_cond\_wait(&mycond,&mymutex)。pthread\_cond\_wait() 调用相当复杂，因此我们每次只执行它的一个操作。

pthread\_cond\_wait() 所做的第一件事就是同时对互斥对象解锁（于是其它线程可以修改已链接列表），并等待条件 mycond 发生（这样当 pthread\_cond\_wait() 接收到另一个线程的“信号”时，它将苏醒）。现在互斥对象已被解锁，其它线程可以访问和修改已链接列表，可能还会添加项。 【要求解锁并阻塞是一个原子操作】

此时，pthread\_cond\_wait() 调用还未返回。对互斥对象解锁会立即发生，但等待条件 mycond 通常是一个阻塞操作，这意味着线程将睡眠，在它苏醒之前不会消耗 CPU 周期。这正是我们期待发生的情况。线程将一直睡眠，直到特定条件发生，在这期间不会发生任何浪费 CPU 时间的繁忙查询。从线程的角度来看，它只是在等待 pthread\_cond\_wait() 调用返回。

现在继续说明，假设另一个线程（称作“2 号线程”）锁定了 mymutex 并对已链接列表添加了一项。在对互斥对象解锁之后，2 号线程会立即调用函数 pthread\_cond\_broadcast(&mycond)。此操作之后，2 号线程将使所有等待 mycond 条件变量的线程立即苏醒。这意味着第一个线程（仍处于 pthread\_cond\_wait() 调用中）现在将苏醒。

现在，看一下第一个线程发生了什么。您可能会认为在 2 号线程调用 pthread\_cond\_broadcast(&mymutex) 之后，1 号线程的 pthread\_cond\_wait() 会立即返回。不是那样！实际上，pthread\_cond\_wait() 将执行最后一个操作：重新锁定 mymutex。一旦 pthread\_cond\_wait() 锁定了互斥对象，那么它将返回并允许 1 号线程继续执行。那时，它可以马上检查列表，查看它所感兴趣的更改。

来看一个例子（你是否能理解呢?）：

In Thread1:

pthread\_mutex\_lock(&m\_mutex);

pthread\_cond\_wait(&m\_cond,&m\_mutex);

pthread\_mutex\_unlock(&m\_mutex);

In Thread2:

pthread\_mutex\_lock(&m\_mutex);

pthread\_cond\_signal(&m\_cond);

pthread\_mutex\_unlock(&m\_mutex);

为什么要与pthread\_mutex 一起使用呢？ 这是为了应对 线程1在调用pthread\_cond\_wait()但线程1还没有进入wait cond的状态的时候，此时线程2调用了 cond\_singal 的情况。 如果不用mutex锁的话，这个cond\_singal就丢失了。加了锁的情况是，线程2必须等到 mutex 被释放（也就是 pthread\_cod\_wait() 释放锁并进入wait\_cond状态 ，此时线程2上锁） 的时候才能调用cond\_singal.

pthread\_cond\_signal即可以放在pthread\_mutex\_lock和pthread\_mutex\_unlock之间，也可以放在pthread\_mutex\_lock和pthread\_mutex\_unlock之后，但是各有有缺点。

之间：

pthread\_mutex\_lock

xxxxxxx

pthread\_cond\_signal

pthread\_mutex\_unlock

缺点：在某下线程的实现中，会造成等待线程从内核中唤醒（由于cond\_signal)然后又回到内核空间（因为cond\_wait返回后会有原子加锁的 行为），所以一来一回会有性能的问题。但是在LinuxThreads或者NPTL里面，就不会有这个问题，因为在Linux 线程中，有两个队列，分别是cond\_wait队列和mutex\_lock队列， cond\_signal只是让线程从cond\_wait队列移到mutex\_lock队列，而不用返回到用户空间，不会有性能的损耗。

所以在Linux中推荐使用这种模式。

之后：

pthread\_mutex\_lock

xxxxxxx

pthread\_mutex\_unlock

pthread\_cond\_signal

优点：不会出现之前说的那个潜在的性能损耗，因为在signal之前就已经释放锁了

缺点：如果unlock和signal之前，有个低优先级的线程正在mutex上等待的话，那么这个低优先级的线程就会抢占高优先级的线程（cond\_wait的线程)，而这在上面的放中间的模式下是不会出现的。

#### 示例程序

源码：$Magenta/magenta/kernel/app/tests/thread\_tests.c

### cond

条件变量是条件相关的数据结构。它允许线程在某些条件变为真之前被阻塞。例如，thread\_push可能希望检查队列是否已满，如果是这样，就在队列未满之前阻塞。所以我们感兴趣的“条件”就是“队列未满”。与之相似，thread\_pop希望等待“队列非空”的条件。

源码：$Magenta/magenta/kernel/include/kernel/cond.h

void cond\_init(cond\_t \*cond);

void cond\_destroy(cond\_t \*cond);

status\_t cond\_wait\_timeout(cond\_t \*cond, mutex\_t \*mutex, lk\_time\_t timeout);

void cond\_signal(cond\_t \*cond);

void cond\_broadcast(cond\_t \*cond);

### mutex

源码：$Magenta/magenta/kernel/include/kernel/mutex.h

/\* Rules for Mutexes:

\* - Mutexes are only safe to use from thread context.

\* - Mutexes are non-recursive.

\*/

void mutex\_init(mutex\_t \*);

void mutex\_destroy(mutex\_t \*);

status\_t mutex\_acquire\_timeout(mutex\_t \*, lk\_time\_t); /\* try to acquire the mutex with a timeout value \*/

void mutex\_release(mutex\_t \*);

### semaphore

信号量（semaphore）又称为信号灯，它是用来协调不同进程间的数据对象的，而最主要的应用是共享内存方式的进程间通信。本质上，信号量是一个计数器，它用来记录对某个资源（如共享内存）的存取状况。一般说来，为了获得共享资源，进程需要执行下列操作：

1. 测试控制该资源的信号量。
2. 若此信号量的值为正，则允许进行使用该资源。进程将信号量减1。
3. 若此信号量为0，则该资源目前不可用，进程进入睡眠状态，直至信号量值大于0，进程被唤醒，转入步骤（1）。
4. 当进程不再使用一个信号量控制的资源时，信号量值加1。如果此时有进程正在睡眠等待此信号量，则唤醒此进程。

源码：$Magenta/magenta/kernel/include/kernel/semaphore.h

void sem\_init(semaphore\_t \*, unsigned int);

void sem\_destroy(semaphore\_t \*);

int sem\_post(semaphore\_t \*, bool resched);

status\_t sem\_wait(semaphore\_t \*);

status\_t sem\_trywait(semaphore\_t \*);

status\_t sem\_timedwait(semaphore\_t \*, lk\_time\_t);

### spinlock

自旋锁（spinlock）它是为为实现保护共享资源而提出一种锁机制。其实，自旋锁与互斥锁比较类似，它们都是为了解决对某项资源的互斥使用。无论是互斥锁，还是自旋锁，在任何时刻，最多只能有一个保持者，也就说，在任何时刻最多只能有一个执行单元获得锁。但是两者在调度机制上略有不同。对于互斥锁，如果资源已经被占用，资源申请者只能进入睡眠状态。但是自旋锁不会引起调用者睡眠，如果自旋锁已经被别的执行单元保持，调用者就一直循环在那里看是否该自旋锁的保持者已经释放了锁，“自旋”一词就是因此而得名。

#### 自旋锁一般原理

跟互斥锁一样，一个执行单元要想访问被自旋锁保护的共享资源，必须先得到锁，在访问完共享资源后，必须释放锁。如果在获取自旋锁时，没有任何执行单元保持该锁，那么将立即得到锁；如果在获取自旋锁时锁已经有保持者，那么获取锁操作将自旋在那里，直到该自旋锁的保持者释放了锁。由此我们可以看出，自旋锁是一种比较低级的保护数据结构或代码片段的原始方式，这种锁可能存在两个问题：死锁和过多占用CPU资源。

#### 自旋锁适用情况

自旋锁比较适用于锁使用者保持锁时间比较短的情况。正是由于自旋锁使用者一般保持锁时间非常短，因此选择自旋而不是睡眠是非常必要的，自旋锁的效率远高于互斥锁。信号量和读写信号量适合于保持时间较长的情况，它们会导致调用者睡眠，因此只能在进程上下文使用，而自旋锁适合于保持时间非常短的情况，它可以在任何上下文使用。如果被保护的共享资源只在进程上下文访问，使用信号量保护该共享资源非常合适，如果对共享资源的访问时间非常短，自旋锁也可以。但是如果被保护的共享资源需要在中断上下文访问（包括底半部即中断处理句柄和顶半部即软中断），就必须使用自旋锁。自旋锁保持期间是抢占失效的，而信号量和读写信号量保持期间是可以被抢占的。自旋锁只有在内核可抢占或SMP（多处理器）的情况下才真正需要，在单CPU且不可抢占的内核下，自旋锁的所有操作都是空操作。另外格外注意一点：自旋锁不能递归使用。

源码：$Magenta/magenta/kernel/include/kernel/spinlock.h

/\* interrupts should already be disabled \*/

static inline void spin\_lock(spin\_lock\_t \*lock)

{

arch\_spin\_lock(lock);

}

/\* Returns 0 on success, non-0 on failure \*/

static inline int spin\_trylock(spin\_lock\_t \*lock)

{

return arch\_spin\_trylock(lock);

}

/\* interrupts should already be disabled \*/

static inline void spin\_unlock(spin\_lock\_t \*lock)

{

arch\_spin\_unlock(lock);

}

static inline void spin\_lock\_init(spin\_lock\_t \*lock)

{

arch\_spin\_lock\_init(lock);

}

static inline bool spin\_lock\_held(spin\_lock\_t \*lock)

{

return arch\_spin\_lock\_held(lock);

}

/\* spin lock irq save flags: \*/

/\* Possible future flags:

\* SPIN\_LOCK\_FLAG\_PMR\_MASK = 0x000000ff

\* SPIN\_LOCK\_FLAG\_PREEMPTION = 0x00000100

\* SPIN\_LOCK\_FLAG\_SET\_PMR = 0x00000200

\*/

/\* Generic flags \*/

#define SPIN\_LOCK\_FLAG\_INTERRUPTS ARCH\_DEFAULT\_SPIN\_LOCK\_FLAG\_INTERRUPTS

/\* same as spin lock, but save disable and save interrupt state first \*/

static inline void spin\_lock\_save(

spin\_lock\_t \*lock,

spin\_lock\_saved\_state\_t \*statep,

spin\_lock\_save\_flags\_t flags)

{

arch\_interrupt\_save(statep, flags);

spin\_lock(lock);

}

/\* restore interrupt state before unlocking \*/

static inline void spin\_unlock\_restore(

spin\_lock\_t \*lock,

spin\_lock\_saved\_state\_t old\_state,

spin\_lock\_save\_flags\_t flags)

{

spin\_unlock(lock);

arch\_interrupt\_restore(old\_state, flags);

}

/\* hand(ier) routines \*/

#define spin\_lock\_irqsave(lock, statep) spin\_lock\_save(lock, &(statep), SPIN\_LOCK\_FLAG\_INTERRUPTS)

#define spin\_unlock\_irqrestore(lock, statep) spin\_unlock\_restore(lock, statep, SPIN\_LOCK\_FLAG\_INTERRUPTS)

### Futexes

Futex，Fast Userspace muTEXes，作为linux下的一种快速同步（互斥）机制，已经存在了很长一段时间了（since linux 2.5.7）。

Magenta中，futex是一个底层同步设施，在它上面建设有pthread\_mutex\_t和pthread\_cond\_t.这样的方便编程的程序库。

A futex is a Fast Userspace muTEX. It is a low level synchronization primitive which is a building block for higher level APIs such as pthread\_mutex\_t and pthread\_cond\_t.

Futexes are designed to not enter the kernel or allocate kernel resources in the uncontested case.

#### 参考文献

* Fuss, Futexes and Furwocks: Fast Userlevel Locking in Linux <https://www.kernel.org/doc/ols/2002/ols2002-pages-479-495.pdf> , Hubertus Franke and Rusty Russell. This is the original white paper describing the Linux futex. It documents the history and design of the original implementation, prior (failed) attempts at creating a fast userspace synchronization primitive, and performance measurements.
* Futexes Are Tricky <https://www.akkadia.org/drepper/futex.pdf> , Ulrich Drepper This paper describes some gotchas and implementation details of futexes in Linux. It discusses the kernel implementation, and goes into more detail about correct and efficient userspace implementations of mutexes, condition variables, and so on.

#### 与Linux的差别

源码：$Magenta/magenta/kernel/lib/magenta/include/magenta/futex\_context.h

源码：$Magenta/magenta/kernel/lib/magenta/futex\_context.cpp

与Linux上的futex的实现有差异，class FutexContext没有记录指向用户空间的虚拟地址的字段。Linux中靠这个字段区分进程内私有futex操作，还是跨进程的futex操作。

As noted above, all of our futex operations leave the value of the futex unmodified from the kernel. Other potential operations, such as Linux's FUTEX\_WAKE\_OP, requires atomic manipulation of the value from the kernel, which our current implementation does not require.

## 进程间通信（IPC）

### 网络套接字（socket）

socket就是在不同计算机之间进行通信的一个抽象。他工作于TCP/IP协议中应用层和传输层之间的一个抽象。如图 12‑1所示。

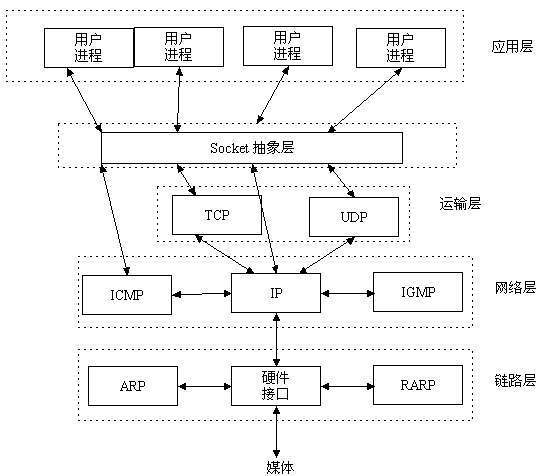


图 ‑1 socket示意图

## 看门狗（watchdog）

源码：$Magenta/magenta/kernel/lib/watchdog/watchdog.c

## 调试debug机制

### LTRACEF

头文件：#include <trace.h>

//#define \_\_FUNC\_\_ \_\_PRETTY\_FUNCTION\_\_

#define \_\_FUNC\_\_ \_\_func\_\_

/\* trace routines \*/

#define TRACE\_ENTRY printf("%s: entry\n", \_\_FUNC\_\_)

#define TRACE\_EXIT printf("%s: exit\n", \_\_FUNC\_\_)

#define TRACE\_ENTRY\_OBJ printf("%s: entry obj %p\n", \_\_FUNC\_\_, this)

#define TRACE\_EXIT\_OBJ printf("%s: exit obj %p\n", \_\_FUNC\_\_, this)

#define TRACE printf("%s:%d\n", \_\_FUNC\_\_, \_\_LINE\_\_)

#define TRACEF(str, x...) do { printf("%s:%d: " str, \_\_FUNC\_\_, \_\_LINE\_\_, ## x); } while (0)

/\* trace routines that work if LOCAL\_TRACE is set \*/

#define LTRACE\_ENTRY do { if (LOCAL\_TRACE) { TRACE\_ENTRY; } } while (0)

#define LTRACE\_EXIT do { if (LOCAL\_TRACE) { TRACE\_EXIT; } } while (0)

#define LTRACE\_ENTRY\_OBJ do { if (LOCAL\_TRACE) { TRACE\_ENTRY\_OBJ; } } while (0)

#define LTRACE\_EXIT\_OBJ do { if (LOCAL\_TRACE) { TRACE\_EXIT\_OBJ; } } while (0)

#define LTRACE do { if (LOCAL\_TRACE) { TRACE; } } while (0)

#define LTRACEF(x...) do { if (LOCAL\_TRACE) { TRACEF(x); } } while (0)

#define LTRACEF\_LEVEL(level, x...) do { if (LOCAL\_TRACE >= (level)) { TRACEF(x); } } while (0)

### DEBUG\_ASSERT

头文件：#include <assert.h>

#if (LK\_DEBUGLEVEL > 1)

#define DEBUG\_ASSERT(x) \

do { \

if (unlikely(!(x))) { \

PANIC("DEBUG ASSERT FAILED at (%s:%d): %s\n", \_\_FILE\_\_, \_\_LINE\_\_, #x); \

} \

} while (0)

#define DEBUG\_ASSERT\_MSG(x, msg, msgargs...) \

do { \

if (unlikely(!(x))) { \

PANIC("DEBUG ASSERT FAILED at (%s:%d): %s\n" msg "\n", \

\_\_FILE\_\_, \_\_LINE\_\_, #x, ## msgargs); \

} \

} while (0)

### DEBUGLOG

把系统工作（如：起动）时的输出信息管理。

源码：$Magenta/magenta/kernel/lib/debuglog/include/lib/debuglog.h

源码：$Magenta/magenta/kernel/lib/debuglog/debuglog.c

#define DLOG\_SIZE (64 \* 1024)

static uint8\_t DLOG\_DATA[DLOG\_SIZE];

static dlog\_t DLOG = {

.lock = MUTEX\_INITIAL\_VALUE(DLOG.lock),

.size = DLOG\_SIZE,

.data = DLOG\_DATA,

.readers = LIST\_INITIAL\_VALUE(DLOG.readers),

};

### 系统控制台console

系统控制台。

源码：$Magenta/magenta/kernel/lib/io/console.c

/\* enable this to cause the kernel-originated messages to splat messages out of the platform

\* putc mechanism immediately instead of going through the debug log

\*/

#ifndef ENABLE\_KERNEL\_LL\_DEBUG

#define ENABLE\_KERNEL\_LL\_DEBUG 0

#endif

## 调优profile机制

### THREAD\_STATS

如果打开宏THREAD\_STATS，则系统运行过程中，收集线程运行中的统计信息。

源码：$Magenta/magenta/kernel/include/kernel/thread.h

struct thread\_stats {

lk\_bigtime\_t idle\_time;

lk\_bigtime\_t last\_idle\_timestamp;

ulong reschedules;

ulong context\_switches;

ulong preempts;

ulong yields;

ulong interrupts; /\* platform code increment this \*/

ulong timer\_ints; /\* timer code increment this \*/

ulong timers; /\* timer code increment this \*/

#if WITH\_SMP

ulong reschedule\_ipis;

#endif

};

### KTRACE

源码：$Magenta/magenta/kernel/lib/ktrace/ktrace.cpp

LK\_INIT\_HOOK(ktrace, ktrace\_init, LK\_INIT\_LEVEL\_APPS - 1);

源码：Magenta/magenta/kernel/lib/syscalls/syscalls\_debug.cpp

mx\_ssize\_t sys\_ktrace\_read(mx\_handle\_t handle, void\* ptr, uint32\_t off, uint32\_t len)

mx\_status\_t sys\_ktrace\_control(mx\_handle\_t handle, uint32\_t action, uint32\_t options)

程序中，写KTRACE示例，注意宏WITH\_LIB\_KTRACE的使用：

#if WITH\_LIB\_KTRACE

ktrace(TAG\_CONTEXT\_SWITCH, (uint32\_t)newthread->user\_tid, cpu | (oldthread->state << 16),

(uint32\_t)(uintptr\_t)oldthread, (uint32\_t)(uintptr\_t)newthread);

#endif

### KLOG

源码：$Magenta/magenta/kernel/lib/klog/klog.c

STATIC\_COMMAND("klog", "commands for manipulating klog", &cmd\_klog)

### 内核事件EVLOG（kernel event log）

宏WITH\_KERNEL\_EVLOG需要打开，否则系统不记录这个log。

EVLOG包括如下种类的事件，程序通过这里定义的宏记录evlog：

源码：$Magenta/magenta/kernel/include/kernel/debug.h

enum {

KERNEL\_EVLOG\_NULL = 0,

KERNEL\_EVLOG\_CONTEXT\_SWITCH, //上下文切换

KERNEL\_EVLOG\_PREEMPT, //线程抢占

KERNEL\_EVLOG\_TIMER\_TICK, //定时器滴答声

KERNEL\_EVLOG\_TIMER\_CALL, //定时器回调函数执行

KERNEL\_EVLOG\_IRQ\_ENTER, //中断进入

KERNEL\_EVLOG\_IRQ\_EXIT, //中断退出

};

#define KEVLOG\_THREAD\_SWITCH(from, to) kernel\_evlog\_add(KERNEL\_EVLOG\_CONTEXT\_SWITCH, (uintptr\_t)from, (uintptr\_t)to)

#define KEVLOG\_THREAD\_PREEMPT(thread) kernel\_evlog\_add(KERNEL\_EVLOG\_PREEMPT, (uintptr\_t)thread, 0)

#define KEVLOG\_TIMER\_TICK() kernel\_evlog\_add(KERNEL\_EVLOG\_TIMER\_TICK, 0, 0)

#define KEVLOG\_TIMER\_CALL(ptr, arg) kernel\_evlog\_add(KERNEL\_EVLOG\_TIMER\_CALL, (uintptr\_t)ptr, (uintptr\_t)arg)

#define KEVLOG\_IRQ\_ENTER(irqn) kernel\_evlog\_add(KERNEL\_EVLOG\_IRQ\_ENTER, (uintptr\_t)irqn, 0)

#define KEVLOG\_IRQ\_EXIT(irqn) kernel\_evlog\_add(KERNEL\_EVLOG\_IRQ\_EXIT, (uintptr\_t)irqn, 0)

源码：$Magenta/magenta/kernel/kernel/debug.c

static int cmd\_kevlog(int argc, const cmd\_args \*argv)

源码：$Magenta/magenta/kernel/lib/evlog/evlog.c

status\_t evlog\_init(evlog\_t \*e, uint len, uint unitsize)

## 监控运行log机制

### LogDispatcher

内核调试信息记录与管理。

### 内核诊断信息diagnostics

源码：$Magenta/magenta/kernel/lib/magenta/diagnostics.cpp

STATIC\_COMMAND("mx", "magenta diagnostics", &cmd\_diagnostics)

# 调试Magenta

## 用QEMU+gdb调试Magenta

### 通过QEMU跑起来Magenta。

参考：

<http://jingxuanzhang.elastos.org/2015/02/02/qemu%E4%BB%BF%E7%9C%9F%E4%B8%8Egdb%E8%BF%9C%E7%A8%8B%E8%B0%83%E8%AF%95/>

xilong@xilong-OptiPlex-7010:~/swap/Magenta/magenta$ ./scripts/run-magenta-arm32 -s 1

坑1：

Note that this library provides an implementation for the weak symbol

"platform\_reset". It also assumes that r0 contains the size of memory reserved

for the secure OS.

### 起调试器arm-none-eabi-gdb

xilong@xilong-OptiPlex-7010:~/swap/Magenta/magenta$ arm-none-eabi-gdb

GNU gdb (Sourcery CodeBench Lite 2013.11-24) 7.6.50.20130726-cvs

Copyright (C) 2013 Free Software Foundation, Inc.

License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>

This is free software: you are free to change and redistribute it.

There is NO WARRANTY, to the extent permitted by law. Type "show copying"

and "show warranty" for details.

This GDB was configured as "--host=i686-pc-linux-gnu --target=arm-none-eabi".

Type "show configuration" for configuration details.

For bug reporting instructions, please see:

<https://sourcery.mentor.com/GNUToolchain/>.

Find the GDB manual and other documentation resources online at:

<http://www.gnu.org/software/gdb/documentation/>.

For help, type "help".

Type "apropos word" to search for commands related to "word".

(gdb) target remote:1234

Remote debugging using :1234

0x40010000 in ?? ()

(gdb) file /home/xilong/swap/Magenta/magenta/build-magenta-qemu-arm32/magenta.elf

A program is being debugged already.

Are you sure you want to change the file? (y or n) y

Reading symbols from /home/xilong/swap/Magenta/magenta/build-magenta-qemu-arm32/magenta.elf...done.

(gdb) ni

0x40010024 in ?? ()

(gdb) x/10i $pc

=> 0x40010024: mrc 15, 0, r12, cr1, cr0, {0}

0x40010028: bic r12, r12, #4096 ; 0x1000

0x4001002c: bic r12, r12, #5

0x40010030: orr r12, r12, #4096 ; 0x1000

0x40010034: orr r12, r12, #4

0x40010038: mcr 15, 0, r12, cr1, cr0, {0}

0x4001003c: ldr r4, [pc, #672] ; 0x400102e4

0x40010040: sub r11, pc, #12

0x40010044: sub r11, r11, r4

0x40010048: mrc 15, 0, r12, cr0, cr0, {5}

(gdb)

### QEMU跑操作系统的第一条指令

QEMU doesn’t provide NOR flash emulation on the goldfish platform. To make things simple, we will use RAM to create a boot-up process that is similar to the boot process from NOR flash. This approach builds a binary image that includes U-Boot, the Linux kernel, and the RAMDISK image and passes this image to QEMU through the –kernel option.

Before we start, let’s look at how QEMU boots a Linux kernel. To boot up a Linux kernel, the bootloader prepares the following environment:

* The processor is in SVC (Supervisor) mode and IRQ and FIQ are disabled.
* MMU is disabled.
* Register r0 is set to 0.
* Register r1 contains the ARM Linux machine type.
* Register r2 contains the address of the kernel parameter list.

After power-up, QEMU starts to run from address 0x00000000. Before it loads a kernel image, QEMU prepares the environment described previously; it then jumps to address 0x00010000. [Figure 10.4](javascript:popUp('/content/images/chap10_9780134030005/elementLinks/10fig04_alt.jpg'))shows a memory dump before the point at which QEMU launches a kernel image. Notice the five lines of assembly code before control is transferred to the kernel image—these lines are hard-coded by QEMU when the system starts. The first line (0x00000000) sets register r0 to 0. The second line (0x00000004) and third line (0x00000008) set register r1 to 0x5a1, which is the machine type of the goldfish platform. The fourth line (0x0000000c) sets the value of register r2 to 0x100, which is the start address of the kernel parameter list. The fifth line (0x00000010) sets the register pc to 0x10000, so the execution jumps to address 0x10000. QEMU assumes the kernel image is loaded at address 0x10000.

### 经验总结

用gdb远程调试操作系统Magenta，gdb这端的地址表示可能与remote的不一致。因为当MMU还没有工作时，被调试的操作系统还是跑的物理地址，程序都是基于物理地址进行寻址的，而你的gdb这边，它不知道，它按照ELF里面的信息提示给你。这设了的断点无法工作。怎么办才能把断点设到合适的位置上？

#define MEMBASE 0X40000000

#define MEMSIZE 0X08000000

#define KERNEL\_BASE 0X80000000

#define KERNEL\_LOAD\_OFFSET 0X10000

## 用 Python 拓展 GDB

### 如何用Python 拓展 GDB

参考：<http://python.jobbole.com/85415/>

python脚本完成了，该怎么运行呢？在gdb里使用python脚本，需要用source命令：

(gdb) so ~/move.py

(gdb) mv 1 binary\_search.cpp:18

我们最后把自定义命令的实现放到~/.gdbinit里面。这样gdb每次启动时就会运行它，而无需手动source。直接把python代码放进~/.gdbinit当然是不行的。需要变通一下，在~/.gdbinit加入source ~/move.py。这样gdb每次启动时都会替我们source一下。

有两点需要注意的是：

* gdb会用python 3来解释你的python脚本，除非你用的gdb还处于版本感人的上古时代。
* 跟一般情况不同，gdb环境中的sys.path是不包括当前目录的。这意味着，如果你的脚本依赖于当前目录下的其他模块，你需要手工修改sys.path。比如(gdb) python import sys; sys.path.append('')

### Magenta中的python调试角本

ELinOS is a cross development platform for either Linux or Windows host allowing you to even use your Windows desktop for the development of sophisticated embedded Linux applications.

ELinOS is a commercial development environment for embedded Linux. It consists of a Linux distribution for the target embedded system and development tools for a development host computer. The development host computer usually is a standard desktop computer running Linux or Windows. The Linux system and the application software for the target device are both created on the development host.

ELinOS focuses on industrial applications. For that purpose optional extensions for the Linux kernel are provided. For example, real-time patches from OSADL can be used to improve timing behavior. The kernel will always be specifically compiled for the embedded system. Userspace applications are provided as precompiled binaries in order to save time for compilation. Most of the ELinOS software packages are open source and licensed under the GPL.

ELinOS provides embedded Linux as a standalone operating system or it can be integrated into the PikeOS virtualization platform if safety and security demands cannot be met by Linux alone. The latter might be the case if a certification according to a strict industry standard is required.

Eclipse is the technical basis for the functionality provided by the integrated development environment (IDE) on the development host. ELinOS was first published in 1999.

角本：Magenta/magenta/prebuilt/downloads/arm-eabi-5.3.0-Linux-x86\_64/share/gdb/system-gdbinit/elinos.py

"""Configure GDB using the ELinOS environment."""

WRS/Linux是美国 Wind River System 公司（WRS 公司）出的Linux版本。Wind River Linux provides the exceptional security and flexibility necessary for meeting the dynamic performance, reliability, and scaling needs of the Internet of Things (IoT), helping safely and securely tap into new sources of data for operational improvements and business transformation.

网址：<http://www.windriver.com/products/linux/>

角本：Magenta/magenta/prebuilt/downloads/arm-eabi-5.3.0-Linux-x86\_64/share/gdb/system-gdbinit/wrs-linux.py

"""Configure GDB using the WRS/Linux environment."""

# Magenta系统功能调用

## 句柄Handles

### handle\_close

#### 简述

关闭一个句柄。

#### 函数原型

#include <magenta/syscalls.h>

mx\_status\_t mx\_handle\_close(mx\_handle\_t handle);

#### 参数说明

|  |  |
| --- | --- |
| 参数 | 说明 |
| handle | 句柄 |

#### 功能

handle\_close()关闭一个句柄，这将引起它对应的句柄资源的释放——引用计算减一，如果引用计数减至0，则对象被释放。

#### 返回值

成功，handle\_close()返回NO\_ERROR；失败，一个代表错误值的负数。

#### 出错信息

|  |  |
| --- | --- |
| 错误值 | 说明 |
| ERR\_INVALID\_ARGS(-10) | 无效句柄 |

### handle\_duplicate

#### 简述

复制一个句柄。

#### 函数原型

#include <magenta/syscalls.h>

mx\_handle\_t mx\_handle\_duplicate(mx\_handle\_t handle, mx\_rights\_t rights);

#### 参数说明

|  |  |
| --- | --- |
| 参数 | 说明 |
| handle | 句柄 |
| rights | * 无权 * MX\_RIGHT\_SAME\_RIGHTS(1u<<31)，与原句柄权限相同 * 其它值，必须比原句柄权限小 |

#### 功能

handle\_duplicate()复制一个句柄，这个句柄指向原句柄handle对应的同一个对象，但是权限是新的rights表示的权限。

#### 返回值

成功，handle\_duplicate()返回复制得到的句柄；失败，一个代表错误值的负数。

#### 出错信息

|  |  |
| --- | --- |
| 错误值 | 说明 |
| ERR\_BAD\_HANDLE(-12) | 源句柄无效 |
| ERR\_INVALID\_ARGS(-10) | 无效句柄 |
| ERR\_ACCESS\_DENIED | 源句柄没有MX\_RIGHT\_DUPLICATE权限 |
| ERR\_NO\_MEMORY (-4) | 没内存 |

### handle\_replace

#### 简述

替换一个句柄。

#### 函数原型

#include <magenta/syscalls.h>

mx\_handle\_t mx\_handle\_replace(mx\_handle\_t handle, mx\_rights\_t rights);

#### 参数说明

|  |  |
| --- | --- |
| 参数 | 说明 |
| handle | 句柄 |
| rights | * 无权 * MX\_RIGHT\_SAME\_RIGHTS(1u<<31)，与原句柄权限相同 * 其它值，必须比原句柄权限小 |

#### 功能

handle\_duplicate()替换一个句柄，这个句柄指向原句柄handle对应的同一个对象，但是权限是新的rights表示的权限。

#### 返回值

成功，handle\_duplicate()返回复制得到的句柄；失败，一个代表错误值的负数。

#### 出错信息

|  |  |
| --- | --- |
| 错误值 | 说明 |
| ERR\_BAD\_HANDLE(-12) | 源句柄无效 |
| ERR\_INVALID\_ARGS(-10) | 无效句柄 |
| ERR\_NO\_MEMORY (-4) | 没内存 |

### handle\_wait\_many

#### 简述

等待多个句柄上的信号（signal）。

#### 函数原型

#include <magenta/syscalls.h>

mx\_status\_t mx\_handle\_wait\_many(uint32\_t count, const mx\_handle\_t\* handles,

const mx\_signals\_t\* signals,

mx\_time\_t timeout,

uint32\_t\* result\_index,

mx\_signals\_state\_t\* signals\_states);

#### 参数说明

|  |  |
| --- | --- |
| 参数 | 说明 |
| count | 句柄数。最大值：kMaxWaitHandleCount(256u) |
| handles | 句柄，里面存有count个句柄 |
| signals | 信号，里面存有count个信号 |
| timeout | 超时值，从当前开始时的纳秒nanosecond，0表示立即返回，MX\_TIME\_INFINITE(UINT64\_MAX)则表示无限期等待。 |
| result\_index | 结果索引。必须有足够空间。 |
| signals\_states | 信号状态。必须有足够空间容纳信号状态。 |

typedef struct {

mx\_signals\_t satisfied;

mx\_signals\_t satisfiable;

} mx\_signals\_state\_t;

typedef uint32\_t mx\_signals\_t;

#### 功能

handle\_wait\_many()等待句柄上的信号直到超时，这些句柄上至少有一个产生了信号，则返回。

成功返回时，signals\_states中记录了哪个句柄产生了信号。

Upon return, if non-null, the signals\_states array is filled with a pair of bitmaps for each of the count specified handles, indicating which signals are pending and which are satisfiable on that particular handle.

It is possible to have the call return with a signals\_states array with values different than the values that caused the wait to complete if other threads are further modifing the objects behind the handles.

If non-null and the return value is NO\_ERROR or ERR\_CANCELLED, result\_index set to first handle that satisfied the wait (or was closed, respectively).

#### 返回值

成功，handle\_duplicate()返回复制得到的句柄；失败，一个代表错误值的负数。

handle\_wait\_many() returns NO\_ERROR on success when the wait was satisfied by the signals input, ERR\_BAD\_STATE when one of the signals inputs became unsatisfiable, or ERR\_TIMED\_OUT if the wait completed because timeout nanoseconds have elapsed.

In the event of ERR\_TIMED\_OUT, signals\_states may reflect state changes that occurred after the timeout but before the syscall returned.

#### 出错信息

|  |  |
| --- | --- |
| 错误值 | 说明 |
| ERR\_BAD\_HANDLE(-12) | 源句柄无效 |
| ERR\_INVALID\_ARGS(-10) | 无效句柄 |
| ERR\_NO\_MEMORY (-4) | 没内存 |

ERR\_INVALID\_ARGS handle isn't a valid handle or result\_index or or signals\_states were invalid pointers.

ERR\_ACCESS\_DENIED One or more of the provided handles does not have MX\_RIGHT\_READ and may not be waited upon.

ERR\_CANCELLED One or more of the provided handles was invalidated (e.g., closed) during the wait.

ERR\_NO\_MEMORY (Temporary) failure due to lack of memory.

### handle\_wait\_one

#### 简述

等待一个句柄上的信号。

#### 函数原型

#include <magenta/syscalls.h>

mx\_status\_t mx\_handle\_wait\_one(mx\_handle\_t handle,

mx\_signals\_t signals,

mx\_time timeout,

mx\_signals\_t\* signals\_state);

#### 参数说明

|  |  |
| --- | --- |
| 参数 | 说明 |
| handle | 句柄 |
| signals | 信号 |
| timeout | 超时 |
| signals\_state | 信号状态 |

#### 功能

handle\_duplicate()替换一个句柄，这个句柄指向原句柄handle对应的同一个对象，但是权限是新的rights表示的权限。

#### 返回值

成功，handle\_duplicate()返回复制得到的句柄；失败，一个代表错误值的负数。

#### 出错信息

|  |  |
| --- | --- |
| 错误值 | 说明 |
| ERR\_BAD\_HANDLE(-12) | 源句柄无效 |
| ERR\_INVALID\_ARGS(-10) | 无效句柄 |
| ERR\_NO\_MEMORY (-4) | 没内存 |

## 消息管道（Message Pipes）

管道通信是消息传递的一种特殊方式。所谓“管道”，是指用于连接一个“读”和一个“写”以实现它们之间通信的一个机制。向管道提供输入的发送者，以字符流形式将大量的数据送入（写）管道；而接收管道输出的接收者，则从管道中接收（读）数据。

为了协调双方的通信，管道机制必须提供以下三方面的协调能力：互斥、同步和确定对方的存在。

### msgpipe\_create

#### 简述

创建一个消息管道。

#### 函数原型

#include <magenta/syscalls.h>

mx\_status\_t mx\_msgpipe\_create(mx\_handle\_t handles[2], uint32\_t flags);

#### 参数说明

|  |  |
| --- | --- |
| 参数 | 说明 |
| handles | 容纳两个句柄的数组，out参数 |
| flags | 0 or MX\_FLAG\_REPLY\_PIPE((1u << 0)) |

#### 功能

msgpipe\_create()创建一个消息管道，一个双向数据报（bi-directional datagram-style）风格的数据传输机制。

句柄将要有下列权限：

|  |  |
| --- | --- |
| 权限 | 能力 |
| MX\_RIGHT\_TRANSFER | 允许这个句柄被通过消息管道发送到其它进程 |
| MX\_RIGHT\_WRITE | 允许数据包被队列化 |
| MX\_RIGHT\_READ | 允许读数据包 |

constexpr mx\_rights\_t kDefaultIOPortRights =

MX\_RIGHT\_DUPLICATE | MX\_RIGHT\_TRANSFER | MX\_RIGHT\_READ | MX\_RIGHT\_WRITE;

A reply pipe behaves like a regular message pipe except for mx\_msgpipe\_write() which must include itself as the last handle being transfered.

当标志flags=MX\_FLAG\_REPLY\_PIPE时，只有handles[1] 是应答管道，handles[0]是正常管道。

#### 返回值

成功，msgpipe\_create() 返回NO\_ERROR；失败，一个代表错误值的负数。

#### 出错信息

|  |  |
| --- | --- |
| 错误值 | 说明 |
| ERR\_INVALID\_ARGS(-10) | 句柄数组是NULL |
| ERR\_NO\_MEMORY (-4) | 没内存 |

#### 程序示例

mx\_handle\_t h[2];

mx\_status\_t r;

if ((r = mx\_msgpipe\_create(h, 0)) < 0) {

…… ……

}

h[0], h[1]中有可供后续操作的句柄

### msgpipe\_read

#### 简述

从消息管道中读消息。

#### 函数原型

#include <magenta/syscalls.h>

mx\_status\_t mx\_msgpipe\_read(mx\_handle\_t handle,

void\* bytes, uint32\_t\* num\_bytes,

mx\_handle\_t\* handles, uint32\_t\* num\_handles,

uint32\_t flags);

#### 参数说明

|  |  |
| --- | --- |
| 参数 | 说明 |
| handle | 句柄 |
| bytes | 要读出的字节，out参数 |
| num\_bytes | 输入时：bytes空间大小，字节为单位。NULL表示不想读bytes。  输出时：读出的字节的数量 |
| handles | 读出的句柄，out参数 |
| num\_handles | 输入时：handles空间大小，句柄数。注意：不是字节数。NULL表示不想读handles。  输出时：读出的句柄的数量 |
| flags | （好象没用） |

#### 功能

msgpipe\_read()试图从消息队列中读出它的第一个消息到bytes或者handles中。

一次必须把一个消息报读完，不可以读消息报的一部分。

#### 返回值

成功，msgpipe\_read() 返回NO\_ERROR；失败，一个代表错误值的负数。

#### 出错信息

|  |  |
| --- | --- |
| 错误值 | 说明 |
| ERR\_INVALID\_ARGS(-10) | 参数错。   * handle不是有效的句柄 * num\_bytes如果不是NULL，不是有效地址；或者num\_bytes是NULL，而bytes不是NULL * num\_handles如果不是NULL，不是有效地址；或者num\_handles是NULL，而handles不是NULL |
| ERR\_ACCESS\_DENIED | 句柄没有读权限（MX\_RIGHT\_READ） |
| ERR\_BAD\_STATE | 管道内没消息 |
| ERR\_REMOTE\_CLOSED |  |
| ERR\_NO\_MEMORY (-4) | 没内存 |
| ERR\_NOT\_ENOUGH\_BUFFER | 缓冲区太小。就是你给的bytes或handles的空间太小，不足以容纳消息中的内容 |

### msgpipe\_write

#### 简述

向消息管道中写消息。

#### 函数原型

#include <magenta/syscalls.h>

mx\_status\_t mx\_msgpipe\_write(mx\_handle\_t handle,

void\* bytes, uint32\_t num\_bytes,

mx\_handle\_t\* handles, uint32\_t num\_handles,

uint32\_t flags);

#### 参数说明

|  |  |
| --- | --- |
| 参数 | 说明 |
| handle | 句柄 |
| bytes | 要写出的字节 |
| num\_bytes | bytes空间大小，字节为单位 |
| handles | 要写的句柄 |
| num\_handles | handles空间大小，句柄数。注意：不是字节数。 |
| flags | （好象没用） |

#### 功能

msgpipe\_write()试图向消息队列写一个消息，消息的内容在bytes和/或者handles中。

#### 返回值

成功，msgpipe\_write() 返回NO\_ERROR；失败，一个代表错误值的负数。

#### 出错信息

|  |  |
| --- | --- |
| 错误值 | 说明 |
| ERR\_INVALID\_ARGS(-10) | 参数错。   * handle不是有效的句柄 * num\_bytes如果不是NULL，不是有效地址；或者num\_bytes是NULL，而bytes不是NULL * num\_handles如果不是NULL，不是有效地址；或者num\_handles是NULL，而handles不是NULL |
| ERR\_NOT\_SUPPORTED |  |
| ERR\_ACCESS\_DENIED | 句柄没有写权限（MX\_RIGHT\_WRITE） |
| ERR\_BAD\_STATE | 管道的另一端已经关闭或者管道是一个应答管道（reply pipe） |
| ERR\_REMOTE\_CLOSED | 消息中有句柄，但是这个管道不是应答管道（reply pipe） |
| ERR\_NO\_MEMORY (-4) | 没内存 |
| ERR\_TOO\_BIG | 要传的消息太大。  kMaxMessageSize(65536u)  kMaxMessageHandles (1024u) |

## 数据管道（Data Pipe）

示例程序：$Magenta/magenta/system/utest/core/data-pipe/data-pipe.c

### datapipe\_create

#### 简述

创建一个数据管道。

#### 函数原型

#include <magenta/syscalls.h>

mx\_handle\_t mx\_datapipe\_create(uint32\_t options,

mx\_size\_t element\_size,

mx\_size\_t capacity,

mx\_handle\_t\* consumer\_handle);

#### 参数说明

|  |  |
| --- | --- |
| 参数 | 说明 |
| options |  |
| element\_size | >=1，字节为单位 |
| capacity | capacity % element\_size != 0u，字节为单位  0表示使用系统缺省管道大小  capacity=kDefaultDataPipeCapacity-(kDefaultDataPipeCapacity % element\_size);  if (capacity==0)  capacity = element\_size; |
| consumer\_handle | out参数，靠它返回消费者句柄 |

constexpr mx\_size\_t kDefaultDataPipeCapacity = 32 \* 1024u;

#### 功能

datapipe\_create()创建一个适用于无格式数据传输的单向数据管道。

成功则返回句柄，这个句柄将要有下列权限：

|  |  |
| --- | --- |
| 权限 | 能力 |
| MX\_RIGHT\_TRANSFER | 允许这个句柄被通过管道发送到其它进程 |
| MX\_RIGHT\_WRITE | 允许数据包被队列化 |
| MX\_RIGHT\_READ | 允许读数据包 |

通过参数返回的consumer\_handle将有下列权限：

|  |  |
| --- | --- |
| 权限 | 能力 |
| MX\_RIGHT\_TRANSFER | 允许这个句柄被通过消息管道发送到其它进程 |
| MX\_RIGHT\_READ | 允许读数据包 |

#### 返回值

成功，datapipe\_create() 返回一个有效的数据管道句柄（一个正整数）；失败，一个代表错误值的负数。不可能返回代表无效句柄的0（Zero，the "invalid handle"）。

#### 出错信息

|  |  |
| --- | --- |
| 错误值 | 说明 |
| ERR\_INVALID\_ARGS(-10) | 参数错 |
| ERR\_NO\_MEMORY (-4) | 没内存 |

### datapipe\_read

#### 简述

从数据管道中读数据。

#### 函数原型

#include <magenta/syscalls.h>

mx\_ssize\_t mx\_datapipe\_read(mx\_handle\_t consumer\_handle,

uint32\_t flags,

mx\_size\_t requested,

void\* buffer);

#### 参数说明

|  |  |
| --- | --- |
| 参数 | 说明 |
| consumer\_handle | 句柄 |
| flags | 函数行为 |
| requested |  |
| buffer |  |

// DISCARD, QUERY, and PEEK are mutually exclusive.

#define MX\_DATAPIPE\_READ\_FLAG\_ALL\_OR\_NONE 1u

#define MX\_DATAPIPE\_READ\_FLAG\_DISCARD 2u

#define MX\_DATAPIPE\_READ\_FLAG\_QUERY 4u

#define MX\_DATAPIPE\_READ\_FLAG\_PEEK 8u

// Mask for all the valid MX\_DATAPIPE\_READ\_FLAG\_... flags:

#define MX\_DATAPIPE\_READ\_FLAG\_MASK 15u

#### 功能

datapipe\_read()从数据管道中读出数据，具体行为（read/discarded/available/peeked）依赖于参数flags。

There are three mutually-exclusive mode flags that may be set in flags: MX\_DATAPIPE\_READ\_FLAG\_DISCARD, MX\_DATAPIPE\_READ\_FLAG\_QUERY, and MX\_DATAPIPE\_READ\_FLAG\_PEEK, which indicate the desired mode (none of these flags being set means "read"). If MX\_DATAPIPE\_READ\_FLAG\_ALL\_OR\_NONE is set, then either the entire requested operation is performed, or not at all.

In read mode, requested indicates the number of bytes (which must be a multiple of the element size) to be read (to buffer, which should have room for the requested number of bytes). On success, the number of bytes actually read is returned. Unless MX\_DATAPIPE\_READ\_FLAG\_ALL\_OR\_NONE is set in flags, this number may be less than requested (but will always be a multiple of the element size).

In discard mode, requested indicates the number of bytes to discard and the return value indicates the number of bytes actually discarded (with MX\_DATAPIPE\_READ\_FLAG\_ALL\_OR\_NONE operating as above). buffer is ignored in this case.

In query mode, both requested and buffer are ignored, as is the MX\_DATAPIPE\_READ\_FLAG\_ALL\_OR\_NONE flag. The return value is the number of bytes available to be read.

Peek模式类似于读（read）模式，只是它不象读模式那样，它在读完后不把数据从数据管道中移除。

#### 返回值

成功返回read/discarded/available/peeked的字节数；失败，一个代表错误值的负数。

#### 出错信息

|  |  |
| --- | --- |
| 错误值 | 说明 |
| ERR\_INVALID\_ARGS(-10) | 参数错。  flags has an invalid combination of flags set, requested is not a multiple of the data pipe's element size (and query mode is not specified), or buffer is an invalid pointer (or NULL). |
| ERR\_BAD\_HANDLE | consumer\_handle不是一个有效句柄 |
| ERR\_WRONG\_TYPE | consumer\_handle不是一个与DataPipe生产者有关联的句柄 |
| ERR\_ACCESS\_DENIED | 句柄没有读权限（MX\_RIGHT\_READ） |
| ERR\_NOT\_SUPPORTED | flag参数有非预期的标记 |
| ERR\_ALREADY\_BOUND | consumer\_handle is currently in a two-phase read. |
| ERR\_REMOTE\_CLOSED | (In read/discard/peek mode) The requested operation could not be performed (due to a lack of data) and the remote data pipe producer handle is closed. |
| ERR\_SHOULD\_WAIT | (In read/discard/peek mode) requested is nonzero and MX\_DATAPIPE\_READ\_FLAG\_ALL\_OR\_NONE is not set, but the data pipe is empty (and the producer is still open). |
| ERR\_OUT\_OF\_RANGE | (In read/discard/peek mode) requested is nonzero and MX\_DATAPIPE\_READ\_FLAG\_ALL\_OR\_NONE is set, but the data pipe does not have the requested amount of data available (and the producer is still open).  BUGS  The ERR\_OUT\_OF\_RANGE will be changed to ERR\_SHOULD\_WAIT once read thresholds are implemented (and a corresponding Mojo change is made). |

### datapipe\_begin\_read

#### 简述

开始从数据管道中两阶段（two-phase）读数据。

#### 函数原型

#include <magenta/syscalls.h>

mx\_ssize\_t mx\_datapipe\_begin\_read(mx\_handle\_t consumer\_handle,

uint32\_t flags,

uintptr\_t\* buffer);

#### 参数说明

|  |  |
| --- | --- |
| 参数 | 说明 |
| consumer\_handle | 句柄 |
| flags | 固定为0 |
| buffer | out参数，缓冲区指针，这个缓冲区指向的是管道里面的数据 |

#### 功能

datapipe\_begin\_read()开始对一个数据管道的两阶段读（two-phase read）。首先，它要确认是不是已经有一个ConsumerReadBegin()挂在这个数据管道上了，其次，它要确定这个管道是不是到了容量限制、不是处于活跃（active）状态，管道数据生产者在远端没有关闭这个管道，内存可以在当前进程访问。

如果管道地址不是连续的，则从管道中读出的数据可能少于管道中拥有的数据。

from a data pipe. That is, it first ensures that (some of) the data available to be read is accessible in the caller's address space, e.g., possibly by mapping memory, and then it provides that data's address in buffer. The amount of data available to be read starting from that address is returned (on success). (This address may not be written to; doing so may cause a fault.) Note that this amount may be strictly less than the total amount available to be read from the data pipe (e.g., if the data is not contiguous).

调用完datapipe\_begin\_read()之后，需要调用datapipe\_end\_read()来终止这个两阶段读，datapipe\_end\_read()将告诉数据管道数据被消费了。

#### 返回值

成功返回可以从管道中读出的内容的字节数，这些内容的起始地址通过参数buffer返回；失败，一个代表错误值的负数。

#### 出错信息

|  |  |
| --- | --- |
| 错误值 | 说明 |
| ERR\_BAD\_HANDLE | consumer\_handle不是一个有效句柄 |
| ERR\_WRONG\_TYPE | consumer\_handle不是一个与DataPipe生产者有关联的句柄 |
| ERR\_ACCESS\_DENIED | 句柄没有读权限（MX\_RIGHT\_READ） |
| ERR\_NOT\_SUPPORTED | flag参数有非预期的标记 |
| ERR\_ALREADY\_BOUND | consumer\_handle is currently in a two-phase read. |
| ERR\_INVALID\_ARGS(-10) | 参数错。  flags has an invalid combination of flags set, requested is not a multiple of the data pipe's element size (and query mode is not specified), or buffer is an invalid pointer (or NULL). |
| ERR\_REMOTE\_CLOSED | (In read/discard/peek mode) The requested operation could not be performed (due to a lack of data) and the remote data pipe producer handle is closed. |
| ERR\_SHOULD\_WAIT | (In read/discard/peek mode) requested is nonzero and MX\_DATAPIPE\_READ\_FLAG\_ALL\_OR\_NONE is not set, but the data pipe is empty (and the producer is still open). |
| ERR\_NO\_MEMORY | 内存不足 |

### datapipe\_end\_read

#### 简述

结束从数据管道中两阶段（two-phase）读数据。

#### 函数原型

#include <magenta/syscalls.h>

mx\_status\_t mx\_datapipe\_end\_read(mx\_handle\_t consumer\_handle, mx\_size\_t read);

#### 参数说明

|  |  |
| --- | --- |
| 参数 | 说明 |
| consumer\_handle | 句柄 |
| read | 具体读了多少 |

#### 功能

datapipe\_end\_read()结束从数据管道中读数据。其实就是通知管道管理机构，哪些内容我已经读了，你可以越过这些内容了。

#### 返回值

成功，返回NO\_ERROR；失败，一个代表错误值的负数。

#### 出错信息

|  |  |
| --- | --- |
| 错误值 | 说明 |
| ERR\_BAD\_HANDLE | consumer\_handle不是一个有效句柄 |
| ERR\_WRONG\_TYPE | consumer\_handle不是一个与DataPipe生产者有关联的句柄 |
| ERR\_ACCESS\_DENIED | 句柄没有读权限（MX\_RIGHT\_READ） |
| ERR\_BAD\_STATE | consumer\_handle is currently not in a two-phase read (i.e., there is no preceding call to datapipe\_begin\_read() not "terminated" by a corresponding call to datapipe\_end\_read()). |
| ERR\_INVALID\_ARGS(-10) | 参数错。参数read的值比调用datapipe\_begin\_read()返回的那个值大，或者不是管道元素大小的整数倍。  read is larger than the value returned by the preceding call to datapipe\_begin\_read() or is not a multiple of the data pipe's element size.. |

### datapipe\_write

#### 简述

向数据管道中写数据。

#### 函数原型

#include <magenta/syscalls.h>

mx\_ssize\_t mx\_datapipe\_write(mx\_handle\_t producer\_handle,

uint32\_t flags,

mx\_size\_t requested,

const void\* buffer);

#### 参数说明

|  |  |
| --- | --- |
| 参数 | 说明 |
| producer\_handle | 句柄 |
| flags |  |
| requested |  |
| buffer |  |

#### 功能

requested is the amount of data that the caller would like to write; it must be a multiple of the data pipe's element size. buffer is the source of the data (and should have requested bytes available to read).

If MX\_DATAPIPE\_WRITE\_FLAG\_ALL\_OR\_NONE is set in flags, this either writes the requested amount of data or none at all. Otherwise this may do a partial write (if the data pipe has insufficient available capacity to accomodate the entire requested write), with the amount of data written returned.

#### 返回值

成功返回写出去的字节数， this may be less than requested, but will always be a multiple of the data pipe's element size. ；失败，一个代表错误值的负数。

#### 出错信息

|  |  |
| --- | --- |
| 错误值 | 说明 |
| ERR\_INVALID\_ARGS(-10) | 参数错。  requested is not a multiple of the data pipe's element size, or buffer is an invalid pointer (or NULL). |
| ERR\_BAD\_HANDLE | consumer\_handle不是一个有效句柄 |
| ERR\_WRONG\_TYPE | consumer\_handle不是一个与DataPipe生产者有关联的句柄 |
| ERR\_ACCESS\_DENIED | 句柄没有读权限（MX\_RIGHT\_READ） |
| ERR\_NOT\_SUPPORTED | flag参数有非预期的标记 |
| ERR\_ALREADY\_BOUND | consumer\_handle is currently in a two-phase read. |
| ERR\_REMOTE\_CLOSED | (In read/discard/peek mode) The requested operation could not be performed (due to a lack of data) and the remote data pipe producer handle is closed. |
| ERR\_SHOULD\_WAIT | (In read/discard/peek mode) requested is nonzero and MX\_DATAPIPE\_READ\_FLAG\_ALL\_OR\_NONE is not set, but the data pipe is empty (and the producer is still open). |
| ERR\_OUT\_OF\_RANGE | (In read/discard/peek mode) requested is nonzero and MX\_DATAPIPE\_READ\_FLAG\_ALL\_OR\_NONE is set, but the data pipe does not have the requested amount of data available (and the producer is still open).  BUGS  The ERR\_OUT\_OF\_RANGE will be changed to ERR\_SHOULD\_WAIT once read thresholds are implemented (and a corresponding Mojo change is made). |

### datapipe\_begin\_write

#### 简述

开始一个向数据管道中两阶段（two-phase）写数据。

#### 函数原型

#include <magenta/syscalls.h>

mx\_ssize\_t mx\_datapipe\_begin\_write(mx\_handle\_t producer\_handle,

uint32\_t flags,

uintptr\_t\* buffer);

#### 参数说明

|  |  |
| --- | --- |
| 参数 | 说明 |
| producer\_handle | 句柄 |
| flags | （好象没用） |
| buffer | out参数，用来返回空间指针 |

#### 功能

datepipe\_begin\_write()试图开始一个向数据管道中两阶段（two-phase）写数据。所谓两阶段写就是先向管道服务机制申请一段空间，然后向这个空间里写数据。

#### 返回值

成功，datapipe\_begin\_write() 返回空间的大小；失败，一个代表错误值的负数。

#### 出错信息

|  |  |
| --- | --- |
| 错误值 | 说明 |
| ERR\_INVALID\_ARGS(-10) | 参数错。   * handle不是有效的句柄 * num\_bytes如果不是NULL，不是有效地址；或者num\_bytes是NULL，而bytes不是NULL * num\_handles如果不是NULL，不是有效地址；或者num\_handles是NULL，而handles不是NULL |
| ERR\_NOT\_SUPPORTED |  |
| ERR\_ACCESS\_DENIED | 句柄没有写权限（MX\_RIGHT\_WRITE） |
| ERR\_BAD\_STATE | 管道的另一端已经关闭或者管道是一个应答管道（reply pipe） |
| ERR\_REMOTE\_CLOSED | 消息中有句柄，但是这个管道不是应答管道（reply pipe） |
| ERR\_NO\_MEMORY (-4) | 没内存 |
| ERR\_TOO\_BIG | 要传的消息太大。  kMaxMessageSize(65536u)  kMaxMessageHandles (1024u) |

#### 程序示例

源码：$Magenta/magenta/system/utest/core/data-pipe/data-pipe.c

static bool loop\_write\_full(void) {

BEGIN\_TEST;

mx\_handle\_t producer;

mx\_handle\_t consumer;

mx\_status\_t status;

producer = mx\_datapipe\_create(0u, 1u, KB\_(32), &consumer);

ASSERT\_GT(producer, 0, "could not create producer data pipe");

ASSERT\_GT(consumer, 0, "could not create consumer data pipe");

for (int ix = 0; ; ++ix) {

uintptr\_t buffer = 0;

mx\_ssize\_t avail = mx\_datapipe\_begin\_write(producer, 0u, &buffer);

if (avail < 0) {

ASSERT\_EQ(avail, ERR\_SHOULD\_WAIT, "wrong error");

ASSERT\_EQ(ix, 8, "wrong capacity");

break;

}

memset((void\*)buffer, ix, KB\_(4));

status = mx\_datapipe\_end\_write(producer, KB\_(4));

ASSERT\_EQ(status, NO\_ERROR, "failed to end write");

}

ASSERT\_EQ(get\_satisfied\_signals(producer), 0u, "");

ASSERT\_EQ(get\_satisfiable\_signals(producer), MX\_SIGNAL\_WRITABLE | MX\_SIGNAL\_PEER\_CLOSED, "");

status = mx\_handle\_close(consumer);

ASSERT\_GE(status, NO\_ERROR, "failed to close data pipe");

ASSERT\_EQ(get\_satisfied\_signals(producer), MX\_SIGNAL\_PEER\_CLOSED, "");

ASSERT\_EQ(get\_satisfiable\_signals(producer), MX\_SIGNAL\_PEER\_CLOSED, "");

status = mx\_handle\_close(producer);

ASSERT\_GE(status, NO\_ERROR, "failed to close data pipe");

END\_TEST;

}

### datapipe\_end\_write

#### 简述

结束一个向数据管道中两阶段（two-phase）写数据。

#### 函数原型

#include <magenta/syscalls.h>

mx\_status\_t mx\_datapipe\_end\_write(mx\_handle\_t producer\_handle,

mx\_size\_t written);

#### 参数说明

|  |  |
| --- | --- |
| 参数 | 说明 |
| producer\_handle | 句柄 |
| written | 要写出内容的大小，字节为单位   * >=1 * <=datapipe\_begin\_write()中的缓存区大小 * written % element\_size\_ == 0u |

#### 功能

datepipe\_end\_write()真正一个向数据管道中写数据。程序示例参考datapipe\_begin\_write()中的程序示例。

#### 返回值

成功，datapipe\_end\_write()返回NO\_ERROR（0）；失败返回错误值。

## IO端口（IO Ports）

### port\_create

#### 简述

创建一个IO端口

#### 函数原型

#include <magenta/syscalls.h>

mx\_handle\_t mx\_port\_create(uint32\_t options);

#### 参数说明

|  |  |
| --- | --- |
| 参数 | 说明 |
| options | 0（好象没啥用） |

#### 功能

port\_create() 创建一个IO端口，一个可以对其实施等待操作的对象，用户态程序或内核可以对其读IO数据包。

返回句柄将有权限：

|  |  |
| --- | --- |
| 权限 | 能力 |
| MX\_RIGHT\_TRANSFER | 允许这个句柄被通过消息管道发送到其它进程 |
| MX\_RIGHT\_WRITE | 允许数据包被队列化 |
| MX\_RIGHT\_READ | 允许读数据包 |
| MX\_RIGHT\_DUPLICATE | 这个句柄可被复制 |

constexpr mx\_rights\_t kDefaultIOPortRights =

MX\_RIGHT\_DUPLICATE | MX\_RIGHT\_TRANSFER | MX\_RIGHT\_READ | MX\_RIGHT\_WRITE;

#### 返回值

成功，port\_create() 返回一个有效的IO端口句柄（一个正整数）；失败，一个代表错误值的负数。不可能返回代表无效句柄的0（Zero，the "invalid handle"）。

#### 出错信息

|  |  |
| --- | --- |
| 错误值 | 说明 |
| ERR\_INVALID\_ARGS(-10) | options中的值无效 |
| ERR\_NO\_MEMORY (-4) | 没内存 |

### port\_queue

#### 简述

把要发送内容送入IO端口发送队列

#### 函数原型

#include <magenta/syscalls.h>

mx\_status\_t mx\_port\_queue(mx\_handle\_t handle, const void\* packet, mx\_size\_t size);

#### 参数说明

|  |  |
| --- | --- |
| 参数 | 说明 |
| packet | 数据包 |
| size | 数据包的大小 |

#### 功能

port\_queue() 把一个数据包送入IO端口发送队列这个数据包的开始部分必须是数据结构mx\_packet\_header\_t，并且比MX\_PORT\_MAX\_PKT\_SIZE.（128u）小。

typedef struct mx\_packet\_header {

uint64\_t key;

uint32\_t type;

uint32\_t extra;

} mx\_packet\_header\_t;

key和exta的值暂保留，type的值必须是MX\_PORT\_PKT\_TYPE\_USER（2u），这个值是告诉系统这个数据包来源于port\_queue()，而不是来源于绑定的句柄，如果来源于绑定的句柄，这个type值是MX\_PORT\_PKT\_TYPE\_IOSN（1u）。

The queue is drained by calling port\_wait().

#### 返回值

成功，port\_queue() 返回NO\_ERROR（0）。

#### 出错信息

|  |  |
| --- | --- |
| 错误值 | 说明 |
| ERR\_INVALID\_ARGS(-10) | handle不是一个有效的IO端口，或者packet不是一个有效的指针，或者size比数据结构mx\_packet\_header\_t的尺寸还小。 |
| ERR\_ACCESS\_DENIED(-30) | 句柄没写（MX\_RIGHT\_WRITE.）权限 |
| ERR\_NOT\_ENOUGH\_BUFFER(-14) | 包太大 |

### port\_wait

#### 简述

在一个IO端口上等待一个包

#### 函数原型

#include <magenta/syscalls.h>

mx\_status\_t mx\_port\_wait(mx\_handle\_t handle, void\* packet, mx\_size\_t size);

#### 参数说明

|  |  |
| --- | --- |
| 参数 | 说明 |
| handle | 句柄 |
| packet | 数据包 |
| size | 数据包的大小 |

#### 功能

port\_wait() 调用将引起调用者等待，直到该IO端口上至少有一个包，而且包是有效的。包队列是先到先出FIFO序的。

不象mx\_wait\_one() 和mx\_wait\_many()，一个数据包只唤醒一个线程，这使得IO端口可被线程池服务。

如果使用mx\_port\_queue()把数据包送入IO端口数据队列，这个数据包的长度不是固定的，但这个数据包的开始部分一定是数据结构mx\_packet\_header\_t，并且成果type的值是MX\_PORT\_PKT\_TYPE\_USER（2u）。

typedef struct mx\_packet\_header {

uint64\_t key;

uint32\_t type;

uint32\_t extra;

} mx\_packet\_header\_t;

If using port\_bind() the dequeued packet is of type mx\_io\_packet\_t with hdr.type set to MX\_PORT\_PKT\_TYPE\_IOSN（1u）.

typedef struct mx\_io\_packet {

mx\_packet\_header\_t hdr;

mx\_time\_t timestamp;

mx\_size\_t bytes;

mx\_signals\_t signals;

uint32\_t reserved;

} mx\_io\_packet\_t;

The key field in the packet header is the key that was in the packet as send via mx\_port\_queue(), or the key that was provided to mx\_port\_bind() when the binding was made.

#### 返回值

成功，port\_queue() 返回NO\_ERROR（0）。

#### 出错信息

|  |  |
| --- | --- |
| 错误值 | 说明 |
| ERR\_INVALID\_ARGS(-10) | handle不是一个有效的IO端口，或者packet不是一个有效的指针，或者size比数据结构mx\_packet\_header\_t的尺寸还小。 |
| ERR\_ACCESS\_DENIED(-30) | 句柄没写（MX\_RIGHT\_WRITE.）权限 |
| ERR\_NOT\_ENOUGH\_BUFFER(-14) | 包太大 |

### port\_bind

#### 简述

把IO端口与一个内核对象绑定

#### 函数原型

#include <magenta/syscalls.h>

mx\_status\_t mx\_port\_bind(mx\_handle\_t handle, uint64\_t key,

mx\_handle\_t source, mx\_signals\_t signals);

#### 参数说明

|  |  |
| --- | --- |
| 参数 | 说明 |
| handle | 内核对象句柄 |
| key | 数据包的大小 |
| source | IO句柄 |
| signals | 信号：MX\_SIGNAL\_READABLE | MX\_SIGNAL\_PEER\_CLOSED |

#### 功能

io\_port\_bind() binds the waitable kernel object source to the IO port identified by handle. Whenever source signals match any of signals, the magenta kernel queues a packet of type mx\_io\_packet\_t to the IO port with the key key and type equal to MX\_PORT\_PKT\_TYPE\_IOSN.

To unbind a source from an IO port, simply close the source handle.

#### 返回值

成功，port\_bind() 返回NO\_ERROR（0）。

#### 出错信息

|  |  |
| --- | --- |
| 错误值 | 说明 |
| ERR\_INVALID\_ARGS(-10) | * handle不是一个有效的IO端口， * source不是一个有效的句柄，或者它不是一个可等待的句柄。 * signals是0 |
| ERR\_ACCESS\_DENIED(-30) | * 句柄没写（MX\_RIGHT\_WRITE.）权限 * source没有读（MX\_RIGHT\_READ）权限 |

## 线程（Threads）

### nanosleep

#### 简述

高精度睡眠

#### 函数原型

#include <magenta/syscalls.h>

mx\_status\_t mx\_nanosleep(mx\_time\_t nanoseconds);

#### 参数说明

|  |  |
| --- | --- |
| 参数 | 说明 |
| nanoseconds | 纳秒。0表示放弃当前线程的后续时间片，MX\_TIME\_INFINITE表示无限期等待。  飞秒（fs）：10-15秒  皮秒（ps）：10-12秒  纳秒（ns）：10-9秒  微秒（µs）：10-6秒  毫秒（ms）：10-3秒 |

// time in nanoseconds

typedef uint64\_t mx\_time\_t;

#### 功能

挂起当前线程至少nanoseconds纳秒。

#### 返回值

成功，mx\_nanosleep () 返回NO\_ERROR。

### thread\_arch\_prctl

### thread\_create

#### 简述

创建一个线程。

#### 函数原型

#include <magenta/syscalls.h>

mx\_handle\_t mx\_thread\_create(mx\_handle\_t process, const char\* name,

uint32\_t name\_len, uint32\_t flags);

#### 参数说明

|  |  |
| --- | --- |
| 参数 | 说明 |
| process | 进程句柄 |
| name | 线程名称 |
| name\_len | 线程名称长度，包括尾'\0'。如果线程名称（含'\0'）长度为MX\_MAX\_NAME\_LEN，则最后一个字母被忽略。 |
| flags | 标志 |

// Maximum string length for kernel names (process name, thread name, etc)

#define MX\_MAX\_NAME\_LEN (32)

#### 功能

thread\_create()指定的进程中创建一个线程，这个线程直到thread\_start()后才开始执行。

当指向一个线程的最后一个句柄关闭后，线程被销毁。

线程句柄可以被等待，这个等待直到收到信号（signal）MX\_SIGNAL\_SIGNALED，这个信号当线程停止时发出，终止一个线程的API是thread\_exit\*()。

#### 返回值

成功，thread\_create() 返回一个有效的线程句柄（一个正整数）；失败，一个代表错误值的负数。不可能返回代表无效句柄的0（Zero，the "invalid handle"）。

#### 出错信息

|  |  |
| --- | --- |
| 错误值 | 说明 |
| ERR\_INVALID\_ARGS(-10) | * 进程句柄无效 * 名字太长 * flags中的值非0 |
| ERR\_NO\_MEMORY (-4) | 没内存 |

### thread\_exit

#### 简述

终止当前线程。

#### 函数原型

#include <magenta/syscalls.h>

void mx\_thread\_exit(void);

#### 功能

mx\_thread\_exist()终止当前线程，没有参数，也没有返回值，这个函数执行完，当前线程就终止了，就以它不返回了。

这个函数执行完后，线程对象将得到信号（signal）MX\_SIGNAL\_SIGNALED，这个信号通过函数handle\_wait\_one()或handle\_wait\_many()监听线程句柄得到。

#define MX\_SIGNAL\_SIGNALED ((mx\_signals\_t)1u << 3)

### thread\_start

#### 简述

开始执行一个线程。

#### 函数原型

#include <magenta/syscalls.h>

mx\_status\_t mx\_thread\_start(mx\_handle\_t thread, uintptr\_t entry, uintptr\_t stack,

uintptr\_t arg1, uintptr\_t arg2);

#### 参数说明

|  |  |
| --- | --- |
| 参数 | 说明 |
| thread | 线程句柄，需要有写（MX\_RIGHT\_WRITE）权限。 |
| entry | 线程入口 |
| stack | 栈 |
| arg1 | 参数1 |
| arg2 | 参数2 |

typedef unsigned long uintptr\_t;

#### 功能

thread\_start()使得一个线程从程序入口entry处开始执行，执行的栈来源于参数stack，参数arg1和arg2，根据不同的平台，被组织到不同的寄存器中去，所有其它寄存器是0。

#### 返回值

成功，thread\_start() 返回NO\_ERROR；失败，一个代表错误值的负数。

#### 出错信息

|  |  |
| --- | --- |
| 错误值 | 说明 |
| ERR\_BAD\_HANDLE | 句柄无效 |
| ERR\_WRONG\_TYPE | 句柄thread不是一个线程句柄 |
| ERR\_ACCESS\_DENIED | 句柄没有写（MX\_RIGHT\_WRITE）权限 |
| ERR\_BAD\_STATE | 线程没有为运行准备好，thread is not ready to run or the process thread is part of is no longer alive. |

## 进程（Processes）

Magenta操作系统有Process的概念，但与传统操作系统的进程的概念有很大差异，它更强调它是一个计算容器。从代码上来看，这个概念还没有实现完，如系统调用mx\_process\_start()代码还不完整，从已经实现的代码上看，Google对这时的Process具体怎么定义，也是在探索中。

### process\_create

#### 简述

创建一个进程。

#### 函数原型

#include <magenta/syscalls.h>

mx\_handle\_t mx\_process\_create(const char\* name, uint32\_t name\_len, uint32\_t flags);

#### 参数说明

|  |  |
| --- | --- |
| 参数 | 说明 |
| name | 线程名称 |
| name\_len | 线程名称长度，包括尾'\0'。如果线程名称（含'\0'）长度为MX\_MAX\_NAME\_LEN，则最后一个字母被忽略。 |
| flags | 标志 |

// Maximum string length for kernel names (process name, thread name, etc)

#define MX\_MAX\_NAME\_LEN (32)

#### 功能

process\_create()创建一个进程，这个线程直到process\_start()后才开始执行。

当指向一个进程的最后一个句柄关闭后，进程被销毁。

进程句柄可以被等待，这个等待直到收到信号（signal）MX\_SIGNAL\_SIGNALED，这个信号当进程停止时发出，终止一个进程的API是

#### 返回值

成功，thread\_create() 返回一个有效的线程句柄（一个正整数）；失败，一个代表错误值的负数。不可能返回代表无效句柄的0（Zero，the "invalid handle"）。

#### 出错信息

|  |  |
| --- | --- |
| 错误值 | 说明 |
| ERR\_INVALID\_ARGS(-10) | * 进程句柄无效 * 名字太长 * flags中的值非0 |
| ERR\_NO\_MEMORY (-4) | 没内存 |

### process\_start

#### 简述

开始执行一个进程。

#### 函数原型

#include <magenta/syscalls.h>

mx\_status\_t mx\_process\_start(mx\_handle\_t process, mx\_handle\_t thread,

uintptr\_t entry, uintptr\_t stack,

mx\_handle\_t arg1, uintptr\_t arg2);

#### 参数说明

|  |  |
| --- | --- |
| 参数 | 说明 |
| process | 线程句柄，需要有写（MX\_RIGHT\_WRITE）权限。 |
| thread | 线程句柄，需要有写（MX\_RIGHT\_WRITE）权限。 |
| entry | 线程入口 |
| stack | 栈 |
| arg1 | 参数1 ??????为什么需要是句柄？ |
| arg2 | 参数2 |

typedef unsigned long uintptr\_t;

#### 功能

process\_start()类似于thread\_start()，它的目的是启动进程所属的第一个线程。

使得进程的第一个线程从程序入口entry处开始执行，执行的栈来源于参数stack，参数arg1和arg2，根据不同的平台，被组织到不同的寄存器中去，所有其它寄存器是0。

每一个参数arg1是一个句柄，它将被从调用进程传输到被起动的进程里去。

The first argument (arg1) is a handle, which will be transferred from the process of the caller to the process which is being started, and an appropriate handle value will be placed in arg1 for the newly started thread.

#### 返回值

成功，process\_start() 返回NO\_ERROR；失败，一个代表错误值的负数。

#### 出错信息

|  |  |
| --- | --- |
| 错误值 | 说明 |
| ERR\_BAD\_HANDLE | 句柄无效 |
| ERR\_WRONG\_TYPE | 句柄thread不是一个进程句柄，或者thread不是一个线程句柄 |
| ERR\_ACCESS\_DENIED | 句柄没有写（MX\_RIGHT\_WRITE）权限，或者线程thread不从属于进程process |
| ERR\_INVALID\_ARGS | 参数arg1不是一个有传输权限（MX\_RIGHT\_TRANSFER）的有效句柄。 |
| ERR\_BAD\_STATE | 进程已经处于运行状态或者已经退出。 |

### process\_map\_vm

#### 简述

为进程保留一块内存。

#### 函数原型

#include <magenta/syscalls.h>

mx\_status\_t sys\_process\_map\_vm(mx\_handle\_t proc\_handle, mx\_handle\_t vmo\_handle,

uint64\_t offset, mx\_size\_t len, mxtl::user\_ptr<uintptr\_t> user\_ptr,

uint32\_t flags);

#### 参数说明

|  |  |
| --- | --- |
| 参数 | 说明 |
| proc\_handle | 进程句柄 |
| vmo\_handle | 内存对象句柄 |
| offset |  |
| len |  |
| user\_ptr |  |
| flags | 标志 |

#### 功能

The mapping retains a reference to the underlying virtual memory object, which means closing the VMO handle does not remove the mapping added by this function.

A virtual memory object can be larger than the address space, which means you should check for overflow before converting the uint64\_t size of the VMO to mx\_process\_map\_vm's mx\_size\_t len parameter.

#### 返回值

成功，process\_map\_vm() 返回NO\_ERROR；失败，一个代表错误值的负数。

#### 出错信息

|  |  |
| --- | --- |
| 错误值 | 说明 |
| ERR\_INVALID\_ARGS(-10) |  |
|  |  |

### process\_protect\_vm

#### 简述

设置一块内存的保护属性。

#### 函数原型

#include <magenta/syscalls.h>

mx\_status\_t mx\_process\_protect\_vm(mx\_handle\_t proc\_handle,

uintptr\_t address, mx\_size\_t len,

uint32\_t prot);

#### 参数说明

|  |  |
| --- | --- |
| 参数 | 说明 |
| proc\_handle | 进程句柄 |
| address | 内存对象句柄 |
| len |  |
| prot | PROT\_NONE(0)与一个或多个PROT\_READ(1)、PROT\_WRITE(2)和PROT\_EXEC(4).的或（OR）值。 |

#### 功能

process\_protect\_vm() alters the access protections for the memory region in which address is located. The prot argument should be either PROT\_NONE or the bitwise OR of one or more of PROT\_READ, PROT\_WRITE, and PROT\_EXEC.

Behavior is undefined if address was not mapped via the process\_vm\_map() function.

#### 返回值

成功，process\_protect\_vm() 返回NO\_ERROR；失败，一个代表错误值的负数。

#### 出错信息

|  |  |
| --- | --- |
| 错误值 | 说明 |
| ERR\_INVALID\_ARGS(-10) | proc\_handle isn't a valid process handle, or address is not from a valid mapped region, or prot is an unsupported combination of flags (e.g., PROT\_WRITE but not PROT\_READ). |
| ERR\_ACCESS\_DENIED | proc\_handle句柄没有写权限（MX\_RIGHT\_WRITE） |

### process\_unmap\_vm

## Objects

### object\_signal

#### 简述

向一个句柄发信号

#### 函数原型

#include <magenta/syscalls.h>

mx\_status\_t mx\_object\_signal(mx\_handle\_t handle, uint32\_t clear\_mask, uint32\_t set\_mask);

#### 参数说明

|  |  |
| --- | --- |
| 参数 | 说明 |
| clear\_mask |  |
| set\_mask |  |

#### 功能

mx\_object\_signal() 向一个内核对象发信号。

## 等待集（Wait Sets）

### waitset\_create

#### 简述

创建一个等待集

#### 函数原型

#include <magenta/syscalls.h>

mx\_status\_t mx\_waitset\_create(void);

#### 功能

mx\_waitset\_create() 创建一个等待集（waitset），一个可以对其实施等待操作的对象，可以向这个对象中加入多个其它种类的句柄。

返回句柄将有权限：

|  |  |
| --- | --- |
| 权限 | 能力 |
| MX\_RIGHT\_WRITE | 允许写 |
| MX\_RIGHT\_READ | 允许读 |

#### 返回值

成功，port\_create() 返回一个有效的句柄（一个正整数）；失败，一个代表错误值的负数。不可能返回代表无效句柄的0（Zero，the "invalid handle"）。

#### 出错信息

|  |  |
| --- | --- |
| 错误值 | 说明 |
| ERR\_NO\_MEMORY (-4) | 没内存 |

### waitset\_add

#### 简述

向等待集中增加一个入口。

#### 函数原型

#include <magenta/syscalls.h>

mx\_status\_t mx\_waitset\_add(mx\_handle\_t waitset\_handle,

mx\_handle\_t handle,

mx\_signals\_t signals,

uint64\_t cookie);

#### 参数说明

|  |  |
| --- | --- |
| 参数 | 说明 |
| waitset\_handle | 等待集句柄，需要有写（MX\_RIGHT\_WRITE）权限。 |
| handle | 要加入等待集中的对象，需要有读（MX\_RIGHT\_READ）权限。 |
| signals |  |
| cookie |  |

#### 功能

waitset\_add() adds an entry to a wait set; an entry consists of a handle, a set of signals that the wait set will "watch", and a cookie to uniquely identify the entry. Note that there may be multiple entries with the same handle (with the same or different set of signals to watch), but that each entry must have a distinct cookie to identify it.

#### 返回值

成功，waitset\_add() 返回NO\_ERROR；失败，一个代表错误值的负数。

#### 出错信息

|  |  |
| --- | --- |
| 错误值 | 说明 |
| ERR\_NO\_MEMORY | 没内存 |
| ERR\_BAD\_HANDLE | waitset\_handle不是一个有效的句柄。 |
| ERR\_INVALID\_ARGS | waitset\_handle指向的不是等待集WaitSet或者handle不是一个有效句柄。 |
| ERR\_ACCESS\_DENIED | waitset\_handle句柄没有写（MX\_RIGHT\_WRITE）权限，或者handle句柄没有读（MX\_RIGHT\_READ）权限 |
| RR\_NOT\_SUPPORTED | handle指向的不是一个可等待对象 |
| ERR\_ALREADY\_EXISTS | 等待集中已经有同样的入口并且同样的cookie的入口handle |

### waitset\_remove

#### 简述

移除等待集中的一个入口。

#### 函数原型

#include <magenta/syscalls.h>

mx\_status\_t mx\_waitset\_remove(mx\_handle\_t waitset\_handle, uint64\_t cookie);

#### 参数说明

|  |  |
| --- | --- |
| 参数 | 说明 |
| waitset\_handle | 等待集句柄，需要有写（MX\_RIGHT\_WRITE）权限。 |
| cookie |  |

#### 功能

waitset\_remove()移除等待集中的一个入口。

#### 返回值

成功，waitset\_remove() 返回NO\_ERROR；失败，一个代表错误值的负数。

#### 出错信息

|  |  |
| --- | --- |
| 错误值 | 说明 |
| ERR\_BAD\_HANDLE | waitset\_handle不是一个有效的句柄。 |
| ERR\_INVALID\_ARGS | waitset\_handle指向的不是等待集WaitSet。 |
| ERR\_ACCESS\_DENIED | waitset\_handle句柄没有写（MX\_RIGHT\_WRITE）权限 |
| ERR\_NOT\_FOUND | 等待集中没有cookie指定的入口 |

### waitset\_wait

#### 简述

等待一个WaitSet。

#### 函数原型

#include <magenta/syscalls.h>

mx\_status\_t mx\_waitset\_wait(mx\_handle\_t waitset\_handle,

mx\_time\_t timeout,

uint32\_t\* num\_results,

mx\_waitset\_result\_t\* results,

uint32\_t\* max\_results);

#### 参数说明

|  |  |
| --- | --- |
| 参数 | 说明 |
| waitset\_handle | 等待集句柄，需要有读（MX\_RIGHT\_READ）权限。 |
| timeout | 超时时间，0表示不等待，INFINITE\_TIME表示无限期等待 |
| num\_results | in-out参数。  输入是results参数的空间大小  输出是实际写到results中的结果集大小  它可能是NULL，因为num\_results可以是0 |
| results | 等待结果集 |
| max\_results | waitset\_handle这个等待集中等待入口的数量 |

// time in nanoseconds

typedef uint64\_t mx\_time\_t;

#define MX\_TIME\_INFINITE UINT64\_MAX

#define INFINITE\_TIME UINT32\_MAX

typedef struct mx\_waitset\_result {

uint64\_t cookie;

mx\_status\_t wait\_result;

uint32\_t reserved;

mx\_signals\_state\_t signals\_state;

} mx\_waitset\_result\_t;

#### 功能

waitset\_wait() waits until one of its entries has a result to report (is satisfied, has become unsatisfiable, or was "cancelled") or the specified timeout has elapsed.

Each result (entry in the results buffer) is an mx\_waitset\_result\_t:

cookie is set to the cookie for the entry with a result to report (as provided to waitset\_add()); each entry yields at most one result. wait\_result is NO\_ERROR if the watched signals provided to waitset\_add() were satisfied, ERR\_BAD\_STATE if the watched signals became unsatisfiable, or ERR\_HANDLE\_CLOSED if the entry's handle was closed. signals\_state is set to the state of the entry's handle's signals at some point shortly before waitset\_wait() returned. reserved is set to zero.

#### 返回值

成功，waitset\_wait() 返回NO\_ERROR，此时，各输出参数中填入了预期的值；失败，一个代表错误的负数，超时也是一种失败，返回ERR\_TIMED\_OUT。

#### 出错信息

|  |  |
| --- | --- |
| 错误值 | 说明 |
| ERR\_NO\_MEMORY | 内存不足 |
| ERR\_BAD\_HANDLE | waitset\_handle不是一个有效的句柄。 |
| ERR\_INVALID\_ARGS | waitset\_handle指向的不是等待集WaitSet。  num\_results无效  results无效  max\_results无效 |
| ERR\_ACCESS\_DENIED | waitset\_handle句柄没有读（MX\_RIGHT\_READ）权限 |
| ERR\_TIMED\_OUT | 超时 |

## Events and Event Pairs

### event\_create

#### 简述

创建一个事件。

#### 函数原型

#include <magenta/syscalls.h>

mx\_handle\_t mx\_event\_create(uint32\_t options);

#### 参数说明

|  |  |
| --- | --- |
| 参数 | 说明 |
| options |  |

#### 功能

event\_create()创建一个事件，也就是一个可以有信号的对象。这个对象可以有4个信号，被命名为：MX\_SIGNAL\_SIGNALn (0<=n<=4)。对象信号可以通过object\_signal()操作。

#define MX\_SIGNAL\_SIGNALED MX\_SIGNAL\_SIGNAL0

#define MX\_SIGNAL\_SIGNAL0 ((mx\_signals\_t)1u << 3)

#define MX\_SIGNAL\_SIGNAL1 ((mx\_signals\_t)1u << 4)

#define MX\_SIGNAL\_SIGNAL2 ((mx\_signals\_t)1u << 5)

#define MX\_SIGNAL\_SIGNAL3 ((mx\_signals\_t)1u << 6)

#define MX\_SIGNAL\_SIGNAL4 ((mx\_signals\_t)1u << 7)

#define MX\_SIGNAL\_SIGNAL\_ALL ((mx\_signals\_t)31u << 3)

返回句柄将有权限：

|  |  |
| --- | --- |
| 权限 | 能力 |
| MX\_RIGHT\_TRANSFER | 允许这个句柄被通过消息管道等机制发送到其它进程 |
| MX\_RIGHT\_WRITE | 允许数据包被队列化 |
| MX\_RIGHT\_READ | 允许读数据包 |
| MX\_RIGHT\_DUPLICATE | 这个句柄可被复制 |

#### 返回值

成功，event\_create() 返回一个有效的句柄（一个正整数）；失败，一个代表错误值的负数。不可能返回代表无效句柄的0（Zero，the "invalid handle"）。

#### 出错信息

|  |  |
| --- | --- |
| 错误值 | 说明 |
| ERR\_NO\_MEMORY (-4) | 没内存 |

### eventpair\_create

#### 简述

创建一个事件对（pair）。

#### 函数原型

#include <magenta/syscalls.h>

mx\_status\_t mx\_eventpair\_create(mx\_handle\_t handles[2], uint32\_t flags);

#### 参数说明

|  |  |
| --- | --- |
| 参数 | 说明 |
| handles | out参数，创建的事件句柄，两个事件对象组成一对 |
| flags |  |

#### 功能

eventpair\_create()创建一个事件对（eventpair），也就是两个可以有信号的对象。这两个对象可以有4个信号，被命名为：MX\_SIGNAL\_SIGNALn (0<=n<=4)。对象信号可以通过object\_signal()操作。

#define MX\_SIGNAL\_SIGNALED MX\_SIGNAL\_SIGNAL0

#define MX\_SIGNAL\_SIGNAL0 ((mx\_signals\_t)1u << 3)

#define MX\_SIGNAL\_SIGNAL1 ((mx\_signals\_t)1u << 4)

#define MX\_SIGNAL\_SIGNAL2 ((mx\_signals\_t)1u << 5)

#define MX\_SIGNAL\_SIGNAL3 ((mx\_signals\_t)1u << 6)

#define MX\_SIGNAL\_SIGNAL4 ((mx\_signals\_t)1u << 7)

#define MX\_SIGNAL\_SIGNAL\_ALL ((mx\_signals\_t)31u << 3)

返回句柄将有权限：

|  |  |
| --- | --- |
| 权限 | 能力 |
| MX\_RIGHT\_TRANSFER | 允许这个句柄被通过消息管道等机制发送到其它进程 |
| MX\_RIGHT\_WRITE | 允许数据包被队列化 |
| MX\_RIGHT\_READ | 允许读数据包 |
| MX\_RIGHT\_DUPLICATE | 这个句柄可被复制 |

示例程序：$Magenta/magenta/system/utest/core/event-pair/event-pair.c

#### 返回值

成功，event\_create() 返回一个有效的句柄（一个正整数）；失败，一个代表错误值的负数。不可能返回代表无效句柄的0（Zero，the "invalid handle"）。

#### 出错信息

|  |  |
| --- | --- |
| 错误值 | 说明 |
| ERR\_NO\_MEMORY (-4) | 没内存 |
| ERR\_INVALID\_ARGS | handles指针错 |
| ERR\_NOT\_SUPPORTED | flags错，应该是0 |

## 中断Interrupt

### interrupt\_create

#### 简述

创建一个中断事件

#### 函数原型

#include <magenta/syscalls.h>

#### 功能

mx

返回句柄将有权限：

|  |  |
| --- | --- |
| 权限 | 能力 |
| MX\_RIGHT\_WRITE | 允许写 |
| MX\_RIGHT\_READ | 允许读 |

#### 返回值

成功，port\_create() 返回一个有效的句柄（一个正整数）；失败，一个代表错误值的负数。不可能返回代表无效句柄的0（Zero，the "invalid handle"）。

#### 出错信息

|  |  |
| --- | --- |
| 错误值 | 说明 |
| ERR\_NO\_MEMORY (-4) | 没内存 |

### interrupt\_complete

## 硬件IO（Device Memory）

### mmap\_device\_memory

### alloc\_device\_memory

## 快速用户区互斥futex

### futex\_wait

#### 简述

等待一个futex。

#### 函数原型

#include <magenta/syscalls.h>

mx\_status\_t mx\_futex\_wait(int\* value\_ptr, int current\_value,

mx\_time\_t timeout);

#### 参数说明

|  |  |
| --- | --- |
| 参数 | 说明 |
| value\_ptr |  |
| current\_value |  |
| timeout | 超时 |

// time in nanoseconds

typedef uint64\_t mx\_time\_t;

#define MX\_TIME\_INFINITE UINT64\_MAX

#### 功能

等待或占有一个futex将引起线程睡眠，直到mx\_futex\_wake()，或者超时。

#### 返回值

成功，返回NO\_ERROR；出错，返回一个表示错误信息的整数值。

#### 出错信息

|  |  |
| --- | --- |
| 错误值 | 说明 |
| ERR\_INVALID\_ARGS | value\_ptr不是一个合法指针 |
| ERR\_ALREADY\_BOUND | current\_value与value\_ptr中的当前值不相等 |
| ERR\_TIMED\_OUT | 线程在超时之前未唤醒 |

### futex\_wake

#### 简述

唤醒等待在futex上的多个线程。

#### 函数原型

#include <magenta/syscalls.h>

mx\_status\_t mx\_futex\_wake(int\* value\_ptr, uint32\_t wake\_count);

#### 参数说明

|  |  |
| --- | --- |
| 参数 | 说明 |
| value\_ptr |  |
| wake\_count | 要唤醒的线程数量。0表示不做任何动作。 |

#### 功能

唤醒等待在futex上的多个线程。

#### 返回值

成功，返回NO\_ERROR。futex\_wake()永远成功，唤醒0个线程也不出错。

### futex\_requeue

#### 简述

唤醒一些等待在futex上的线程，把更多的等待线程移到另外一个等待队列中去。

#### 函数原型

#include <magenta/syscalls.h>

mx\_status\_t mx\_futex\_requeue(int\* value\_ptr, uint32\_t wake\_count,

int current\_value, int\* requeue\_ptr,

uint32\_t requeue\_count);

#### 参数说明

|  |  |
| --- | --- |
| 参数 | 说明 |
| value\_ptr | 等待队列 |
| wake\_count | 唤醒的线程数量 |
| current\_value | 当前值 |
| requeue\_ptr | 新的等待队列 |
| requeue\_count | 移动的等待线程数 |

#### 功能

Requeuing is a generalization of waking. First, the kernel verifies that the value in wake\_count matches the value of the futex at value\_ptr, and if not reports ERR\_ALREADY\_BOUND. After waking wake\_count threads, requeue\_count threads are moved from the original futex's wait queue to the wait queue corresponding to requeue\_ptr, another futex.

This requeueing behavior may be used to avoid thundering herds on wake.

#### 返回值

成功，返回NO\_ERROR；出错，返回一个表示错误信息的整数值。

#### 出错信息

|  |  |
| --- | --- |
| 错误值 | 说明 |
| ERR\_INVALID\_ARGS | value\_ptr不是一个合法指针 |
| ERR\_ALREADY\_BOUND | current\_value与value\_ptr中的当前值不相等 |

## Cryptographically Secure RNG

### cprng\_draw

#### 简述

利用内核的CPRNG机制在一个缓冲区内生成随机内容。

#### 函数原型

#include <magenta/syscalls.h>

mx\_ssize\_t mx\_cprng\_draw(void\* buffer, mx\_size\_t len);

#### 参数说明

|  |  |
| --- | --- |
| 参数 | 说明 |
| buffers | 缓冲区 |
| len | 缓冲区大小 |

// Buffer size limits on the cprng syscalls

#define MX\_CPRNG\_DRAW\_MAX\_LEN 256

#### 功能

mx\_cprng\_draw()利用内核的CPRNG机制在一个绘冲区内生成随机内容。

#### 返回值

写到缓冲区里的字节数。

#### 出错信息

|  |  |
| --- | --- |
| 错误值 | 说明 |
| ERR\_INVALID\_ARGS | 参数错 |

### cprng\_add\_entropy

#### 简述

增加熵（entropy）到内核CPRNG。

#### 函数原型

#include <magenta/syscalls.h>

mx\_status\_t mx\_cprng\_add\_entropy(void\* buffer, mx\_size\_t len);

#### 参数说明

|  |  |
| --- | --- |
| 参数 | 说明 |
| buffers | 缓冲区 |
| len | 缓冲区大小 |

// Buffer size limits on the cprng syscalls

#define MX\_CPRNG\_ADD\_ENTROPY\_MAX\_LEN 256

#### 功能

mx\_cprng\_add\_entropy增加熵给内核的CPRNG机制。

#### 返回值

状态信息，成功返回NO\_ERROR，失败则返回一个表示出错信息的负数。

#### 出错信息

|  |  |
| --- | --- |
| 错误值 | 说明 |
| ERR\_INVALID\_ARGS | 参数错 |

## 系统运行log

// Defines and structures for mx\_log\_\*()

typedef struct mx\_log\_record {

uint32\_t reserved;

uint16\_t datalen;

uint16\_t flags;

mx\_time\_t timestamp;

char data[0];

} mx\_log\_record\_t;

#define MX\_LOG\_RECORD\_MAX 256

#define MX\_LOG\_FLAG\_KERNEL 0x0100

#define MX\_LOG\_FLAG\_DEVMGR 0x0200

#define MX\_LOG\_FLAG\_CONSOLE 0x0400

#define MX\_LOG\_FLAG\_DEVICE 0x0800

#define MX\_LOG\_FLAG\_MASK 0x0F00

#define MX\_LOG\_FLAG\_WAIT 0x80000000

#define MX\_LOG\_FLAG\_READABLE 0x40000000

### log\_create

int mx\_log\_create(uint32\_t flags);

### log\_write

int mx\_log\_write(mx\_handle\_t log\_handle, uint32\_t len, mxtl::user\_ptr<const void> ptr, uint32\_t flags)

### log\_read

int mx\_log\_read(mx\_handle\_t log\_handle, uint32\_t len, mxtl::user\_ptr<void> ptr, uint32\_t flags) {

# 开发工具链

## Make文件

源码：$Magenta/magenta/makefile

LKMAKEROOT := .

LKROOT := kernel

LKINC := system third\_party

BUILDROOT ?= .

DEFAULT\_PROJECT ?= magenta-pc-x86-64

TOOLCHAIN\_PREFIX ?=

ENABLE\_BUILD\_SYSROOT ?= false

# if true, $BUILDDIR/sysroot/{lib,include,...} will be populated with

# public libraries, headers, and other "build artifacts" necessary

# for a toolchain to compile binaries for Magenta.

ENABLE\_BUILD\_LISTFILES ?= false

# If true, various verbose listings (\*.lst, \*.sym, \*,dump, etc) will

# be generated for the kernel and userspace binaries. These can be

# useful for debugging, but are large and can slow the build some.

# check if LKROOT is already a part of LKINC list and add it only if it is not

ifneq ($(findstring $(LKROOT),$(LKINC)), $(LKROOT))

LKINC := $(LKROOT) $(LKINC)

endif

export LKMAKEROOT

export LKROOT

export LKINC

export BUILDROOT

export DEFAULT\_PROJECT

export TOOLCHAIN\_PREFIX

# vaneer makefile that calls into the engine with lk as the build root

# if we're the top level invocation, call ourselves with additional args

$(MAKECMDGOALS) \_top:

@$(MAKE) -C $(LKMAKEROOT) --no-print-directory -rR -f $(LKROOT)/engine.mk $(addprefix -I,$(LKINC)) $(MAKECMDGOALS)

.PHONY: \_top

## 源代码管理

参考：<https://github.com/fuchsia-mirror/manifest>。这里用到的工具jiri，可以通过这个链接<https://github.com/fuchsia-mirror/jiri> 了解更详细信息。

xilong@xilong-OptiPlex-7010:~$ curl -s https://raw.githubusercontent.com/fuchsia-mirror/jiri/master/scripts/bootstrap\_jiri | bash -s fuchsia

Please add /home/xilong/fuchsia/.jiri\_root/scripts to your PATH

xilong@xilong-OptiPlex-7010:~$ cd fuchsia/

xilong@xilong-OptiPlex-7010:~/fuchsia$ export PATH=`pwd`/.jiri\_root/scripts:$PATH

xilong@xilong-OptiPlex-7010:~/fuchsia$ jiri import fuchsia https://fuchsia.googlesource.com/manifest

xilong@xilong-OptiPlex-7010:~/fuchsia$ jiri update

[10:11:58.96] >> move project "manifest" located in "/tmp/jiri-load278940617/manifest\_ad81d9e784efd6cc" to "/home/xilong/fuchsia/manifest" and advance it to "578ca153"

[10:12:01.15] >> OK

[10:12:01.15] >> create project "apps/compositor" in "/home/xilong/fuchsia/apps/compositor" and advance it to "HEAD"

[10:12:07.06] >> OK

[10:12:07.06] >> create project "apps/dart\_content\_handler" in "/home/xilong/fuchsia/apps/dart\_content\_handler" and advance it to "HEAD"

[10:12:11.93] >> OK

[10:12:11.93] >> create project "apps/ledger" in "/home/xilong/fuchsia/apps/ledger" and advance it to "HEAD"

[10:12:17.87] >> OK

# Magenta深入开发

稳定性测试

连续运行能力

MTBF,即平均故障间隔时间，英文全称是“Mean Time Between Failure”。

内存泄漏

其它资源泄漏

平台移植

MIPS、PPC平台支持

可靠性、安全性策略支持

safety策略

security策略

容错计算

恢复块技术recovery支持

# 问答Q&A

## 程序技术问题

#### 下面这两行ARM汇编，str那句什么意思？

mrc p15, 0, sp, c9, c13, 0

str sp, [pc, #\_\_irq\_cycle\_count - . - 8]

答：

str sp, [pc, <offset>] 其中offset为\_\_irq\_cycle\_count地址减去本指令地址再减去8。

#### WITH宏定义

一个模块，是否编译进内核，最终编译的c/c++头文件是config-kernel.h，它是在make阶段生成的。

源码：$Magenta/magenta/kernel/engine.mk

# generate a config-kernel.h file with all of the KERNEL\_DEFINES laid out in #define format

kernelconfigheader:

$(KERNEL\_CONFIG\_HEADER): kernelconfigheader

@$(call MAKECONFIGHEADER,$@,KERNEL\_DEFINES,"")

源码：$Magenta/magenta/kernel/make/module.mk

# kernel module

# add a local include dir to the global include path for kernel code

KERNEL\_INCLUDES += $(MODULE\_SRCDIR)/include

KERNEL\_DEFINES += $(addsuffix =1,$(addprefix WITH\_,$(MODULE\_SHORTNAME)))

MODULE\_SRCDEPS += $(KERNEL\_CONFIG\_HEADER)

以evlog为例解释一下这些角本的工作：

MODULE\_SHORTNAME：lib/evlog

KERNEL\_DEFINES中增加的内容：WITH\_lib/evlog=1

经过MAKECONFIGHEADER宏，把KERNEL\_DEFINES中增加的内容变为：

#define WITH\_LIB\_EVLOG 1

写到config-kernel.h中，然后其它依赖于这个库的地方，就通过宏WITH\_LIB\_EVLOG判断库evlog（位于目录：kernel/lib/evlog）是否编译到内核里面了。

#### 如何让一个kernel/lib参与内核编译

kernel/lib如下evlog（Magenta/magenta/kernel/lib/evlog/rules.mk），它要想参加编译，需要加到$Magenta/magenta/kernel/lib/magenta/rules.mk 文件中。

MODULE\_DEPS := \

lib/dpc \

lib/mxtl \

lib/evlog \

dev/interrupt \

编译内核时，会定义一个宏

KERNEL\_DEFINES += WITH\_lib/evlog=1

在编译模块时，在该模块的make文件中，加编译需要定义的宏。如evlog，参加编译后，需要提供宏：WITH\_KERNEL\_EVLOG。

源码：$Magenta/magenta/kernel/lib/evlog/rules.mk

LOCAL\_DIR := $(GET\_LOCAL\_DIR)

MODULE := $(LOCAL\_DIR)

KERNEL\_DEFINES += WITH\_KERNEL\_EVLOG=1

MODULE\_SRCS += \

$(LOCAL\_DIR)/evlog.c

include make/module.mk

#### mxtl::move()之于移动构造

RefPtr这样的智能指针本身是一个结构体struct，它里面有成员负责记录被它管理的资源的指针，然后是引用计算之类的东西，当一个RefPtr在函数间传递时，调用者拥有的RefPtr结构体里面的内容，需要装到被调用者的RefPtr结构体里面去，并且调用者的RefPtr的生命周期不再与它管理的资源的指针一致，这就涉及到c++的移动构造的问题。

首先读懂mxtl::move()模板，知道mxtl::move()是如何把类型右值化。

请特别注意T类移动构造和移动赋值函数的参数的类型，它是T&&。没错，是两个&&符号：

* + 如果是T&&（两个&&符号），则表示是T的右值引用类型。
  + 如果是T&（一个&符号），则表示是T的引用类型。和右值引用相比，这种引用也叫左值引用。

什么是左值，什么是右值？

* + 左值是有名字的，并且可以取地址。
  + 右值是无名的，不能取地址。

源码：$Magenta/magenta/system/ulib/mxtl/include/mxtl/type\_support.h

template <typename T>

struct remove\_reference {

using type = T;

};

template <typename T>

struct remove\_reference<T&> {

using type = T;

};

template <typename T>

struct remove\_reference<T&&> {

using type = T;

};

template <typename T>

constexpr typename remove\_reference<T>::type&& move(T&& t) {

return static\_cast<typename remove\_reference<T>::type&&>(t);

}

以下面这段程序为例（注意带下划线的内容）：

UserThread::UserThread(mx\_koid\_t koid,

mxtl::RefPtr<ProcessDispatcher> process,

uint32\_t flags)

: koid\_(koid),

process\_(mxtl::move(process)),

state\_tracker\_(true, mx\_signals\_state\_t{0u, MX\_SIGNAL\_SIGNALED}) {

LTRACE\_ENTRY\_OBJ;

}

// process\_的定义如下：

// a ref pointer back to the parent process

mxtl::RefPtr<ProcessDispatcher> process\_;

我们希望process\_ 这个赋值是一个移动构造，把RefPtr中指向的内容移到我新的RefPtr中，在翻译原RefPtr时，不要把它原来指向的内容指针给释放了。

RefPtr的移动构造函数如下所示：

template <typename T>

class RefPtr final {

public:

// Move

RefPtr(RefPtr&& r) : ptr\_(r.ptr\_) {

r.ptr\_ = nullptr;

}

## 高阶逻辑在操作系统开发中的应用

* 我在程序运行过程中，详细记录它的运行时信息，如函数的进、出，中断上下文的切换等等，我可不可能利用高阶逻辑验证这个程序的状态，如是否死机，是否处于安全safety状态？

你说的是软件漏洞检测问题，现在很多归为测试来研究的，被测进程状态可控可测是一个难点。如果是需要做实时检测，面临大状态空间的效率问题，符号模型检测甚至随机模型检测可能需要的，有的还可以结合仿真模型做跟踪性检测，以前用spin的状态机模型，现在这些自动机模型花样很多的，因为运行时环境变化必然导致模型也在改变，必须频繁进行检测，这种检测会受到系统能力的约束，所以倒不如说运行时模型诊断好，诊断系统行为和安全属性是否符合安全方面的需求和规范，建议关注一下这些研究，静态的测试和漏洞挖掘再结合模型检测。

# 结语

vxWorks、QNX之类的比RTOS大，比Linux小的操作系统们要当心了，可能是来抢你们的饭碗的。是不是Google要用到你们这个级别的操作系统，你们开价太高了，气得Google决定自己开发一个？