# Arm64操作系统实现原理札记

目录

[Arm64操作系统实现原理札记 1](#_Toc17779)

[前言 1](#_Toc14184)

[基础篇 1](#_Toc8857)

[一、 启动原理 2](#_Toc17348)

[二、 中断 2](#_Toc1595)

[三、 异常 3](#_Toc8802)

[四、 物理内存与物理地址空间 3](#_Toc25338)

[五、 虚拟内存与虚拟地址空间 4](#_Toc25343)

[六、 进程管理 4](#_Toc23223)

[七、 线程管理 4](#_Toc5289)

[八、 调度器 4](#_Toc10804)

[九、 同步机制 4](#_Toc27486)

[十、 驱动 4](#_Toc32436)

[进阶篇 4](#_Toc27558)

# 前言

作者目前就职于国际知名通信厂商，从事ARM嵌入式领域约10年。硬件平台从C51、MSP430、STM8、STM32到ARM Cortex-M0,M3M4，再到Cortex-A53,A57的功能开发。也曾在Altera的FPGA上开发过图像缓存帧调度算法，基于X86开发过视频图像驱动芯片。软件系统从裸机代码到ucosii，再到zephyer，到vxworks，到qnx，到linux，到fuchsia。最终深耕在ARM v8的架构的芯片，微内核操作系统领域、嵌入式虚拟化领域的软件开发。

写这本书的目的一是给自己这么多年的工作做个总结；二是想将自己多年来在ARM v8架构操作系统领域的经验分享给大家。希望对大家有所帮助。

感谢自己投身于自己热爱的行业，也感谢自己坚持了下来。

# 基础篇

本篇主要讲解ARM架构操作系统的一些基本的概念，包括软件、硬件方面的概念。描述每个模块的功能职责，以及为什么需要这些模块。

## 启动原理

操作系统一般是由启动程序启动的，或者说是引导程序。启动程序对于操作系统而言非常重要，如果没有启动程序，操作系统根本无法运行。操作系统上运行那么多功能强大的软件更是无从谈起。那么启动到底对操作系统做了什么呢？

目前比较流行的操作系统，如linux可以由uboot引导启动或者IPL启动，但这仅仅是找到操作系统的入口，或者传递了一些配置资源给操作系统，以便操作系统可以根据该资源做一些配置。在找到操作系统入口之前的这些启动程序，不在本书的讲解范围内。本书主要讲解操作系统本身启动过程的启动原理，讲解启动过程，到底做了什么事。

其实对于操作而言，其启动过程主要是为操作系统准备物理环境，开启当前硬件平台的一些硬件特性。初始化一些硬件外设，是否开启缓存cache、内存管理单元MMU等。

试想操作系统在一个未初始化的硬件平台上，应该准备什么样的环境，操作系统才能正常运行起来。下面将从硬件和软件两方面进行说明。

硬件准备

CPU核、内存、IO交互设备，这是一个操作系统能运行起来的最基本的硬件需求。那么所以启动是需要一个CPU核来运行指令的，这个第一个启动的核一般称为主核。其次是内存，系统一般使用的是DDR易失性随机存储器，这个一般由启动程序初始化好。最后是交互设备，一般使用串口，输出一些启动信息，使得用户看得见系统的启动过程。

软件准备

软件需要准备些啥？前面cpu已经跑起来了，会执行代码定义和变量吧，会调用函数吧，有可能发生异常吧。所以，软件层面，需要准备函数调用和分配临时变量的栈，动态申请释放内存的堆。系统的异常向量表需要提前设置好，否则如果启动过程中发生异常或者中断，系统将会因为找不到代码执行路径而出现系统崩溃或其他未知的问题。导致系统无法正常运行下去。

## 中断

中断其实也算是一种异常，一般叫做异步异常。为了便于区分和学习中断，本书将单独分配一个章节讲解中断。那什么是中断？中断存在意义又是什么？在本章节我们将得到答案。

试想这样一个场景：你有一个快递将要送到你的家里，但是你并不知道具体的时间。那你是就待在家里一直等待，还是可以先出去做点其他事情然后让快递员给你打电话呢？我们可以认为，你正在外面（附近）做事，比如买菜什么的，接到快递员的电话，然后你放下手中的事，回去取快递。这样子的一个场景，可以称之为中断场景。当然，至于你取了快递又去不去继续买菜，还是去做其他的事情，就要根据具体情况具体分析。这又和中断返回时是否有其他优先级更高的事件场景相似，这个将在后文讲解。

上述场景仅仅是让大家初步认识，什么是中断。中断带来的好处有什么？

系统可以正常执行其他任务，而不必空转死等中断事件的到来。提高了系统的运行效率。

在ARMV8架构中，有一个用于管理中断源的控制器，叫做General Interrupt Controller通用中断控制器，简称GIC。ARM将中断源分为三类：

SGI，软件触发中断。比如，核间中断。

PPI，私有外设中断。比如，CPU的物理定时器和虚拟定时器。

SPI，共享外设中断。比如，GPIO、I2C、EMMC等外设发生的中断。

ARMV8的GIC V2版本支持1024个中断源，将这些中断源分类对应到上述类别：

0~15是SGI，16~31是PPI，32~1024是SPI。其中0~31是BANKED，即在每个CPU上都有一个独立的副本，每个CPU只能读走自己的副本，不能影响其他CPU上的中断信息。而SPI不一样，他是共享的，只要有一个CPU识别出中断源，该中断源就会清位，另一个CPU就无法再识别该中断源了。

## 异常

本章节的异常专指同步异常，如系统调用、缺页异常、除零错误等。异常在操作系统中同样有着非常重要的作用。如果一个操作系统仅仅是一个单核单线程任务，而且没有用户态内核态的应用，也不会发生任务异常错误。那么确实，这种操作系统是不需要什么中断异常的、也不需要什么调度器、虚拟内存的。但是这种操作系统是没有什么实际应用价值的，它不仅没有充分利用硬件平台资源，也无法做一些复杂、可动态变化的任务。

异常机制对于操作系统而言是不可或缺的一部分。异常最重要的用途主要有如下几点：

1. 实现系统调用功能，用户态可以通过系统调用接口，向内核请求服务，完成用户态到内核态的切换。
2. 缺页异常机制，通过该异常机制，实现即使修复没有映射物理地址的虚拟地址，从而使得该程序继续恢复运行。该功能使得极大地解决了物理内存不够使用的问题。
3. 实现同步捕获操作系统中正在运行的任务发生的异常错误。及时发现错误，做出对应的处理措施，从而避免错误的进一步扩散。

## 物理内存与物理地址空间

本文一般指操作系统对物理内存和物理地址空间的管理。我们知道在没有开启MMU内存管理单元时，CPU会直接从物理内存读取指令和数据，然后执行程序。这种执行状态x86一般称之为实模式，ARM一般称为裸机模式。开启MMU之后，CPU从虚拟地址获取指令和数据，然后执行。虚拟内存和虚拟地址空间将在后文讲解。物理内存的管理其目的之一就是为了更好更快地服务于虚拟内存。下面将一一描述。

操作系统拿到一块物理内存之后，如何管理是本章节重点描述内容。考虑如下几点：

这块物理内存有多大。

应该按多少字节的粒度去管理一个物理内存页面。

这么多的页面应该使用什么方法管理起来。

申请单页面怎么处理，释放单页面怎么释处理。

申请多页面怎么处理，释放多页面怎么处理。

申请多个连续页面怎么处理，该连续页面又该如何释放。

系统最小分配内存大小如何考虑。

上述就是一个操作系统拿到一块物理内存之后，会经常思考的问题。

## 虚拟内存与虚拟地址空间

从物理内存章节可知，cpu可以直接从物理内存读取指令和数据，然后运行程序。那么虚拟内存又有什么用呢？试想一下，如果整个操作系统只运行了一个程序，那么系统中的所有物理资源都归这一个程序所有，运行过程不会出现什么问题。但操作系统不可能只运行一个程序吧。如果有两个程序同时运行，那么操作系统如何给这两个程序分配内存空间，让它们正常运行呢？还有，如果有更多的程序同时运行，操作系统又该如何考虑分配物理资源呢？这些都能在本章节找到答案。

同样，我们将虚拟地址指向的内存叫做虚拟内存。当前程序可以看见的地址范围，叫做虚拟地址空间。因为虚拟地址空间的存在，每个程序都认为当前操作系统中，只有自己一个任务存在，不知道系统中还有其他任务。所以操作系统任务之一便是，有效地管理程序的虚拟地址到物理地址地的映射关系，而且各个程序真正使用的物理地址一般不重叠。ARM使用内存管理单元MMU管理虚拟地址到物理地址的映射关系。

## 进程管理

操作系统中，进程比线程拥有更大的资源范围。通常一个进程包含，数个线程、当前线程运行的地址空间、已映射的物理地址、当前进程的环境变量、已开启的文件信息等等。所以进程切换将会比线程切换的开销大得多。

## 线程管理

操纵系统中，线程是最小的调度单位。一个线程的正常运行至少需要使用通用寄存器、栈指针寄存器、状态寄存器。因此不同线程之间的切换，需要切换通用寄存器、栈指针寄存器和状态寄存器。由于在进行线程切换时，使用中的通用寄存器会被按序压入栈中，切换回来的时候，这些通用寄存器会被弹栈恢复，因此未使用的通用寄存器就可以不必压栈保存。

## 调度器

从线程管理章节可知，线程是最小的调度单位。做线程切换时，最小切换内容是：通用寄存器和栈（一般指栈基址）。做切换工作的角色主要是调度器完成的。除了做轻量级的线程任务切换，调度器还需要做进程任务切换，这是操作系统中比较常见的切换常见，也称为上下文切换。通常上下文切换，指从当前任务执行环境切换到另一个任务的执行环境，这个任务可以是同进程的线程，也可以是不同进程的任务，甚至有可能是不同虚拟机内的任务。

这里主要讲解一下进程级的上下文切换，一般会切换些什么内容。

通用寄存器x0~x30

浮点寄存器V0~V31

一些状态寄存器，如SPSR

用户态转换表基址寄存器TTBR0\_EL1和TTBR0

线程ID寄存器，TPIDRXX

地址空间ID，ASID

## 同步机制

## 驱动

# 进阶篇

主要将结合实际代码来操作理解操作系统中的概念。

Armv8相关寄存器

主要包含了31个通用寄存器和几个特殊寄存器。如SP，LR等。

cache介绍

MMU介绍

MMU全称，Memory manage unit内存管理单元，管理物理内存映射到虚拟地址空间的地址、权限等。通过MMU可以实现多进程任务之间的虚拟地址空间隔离，使得每个进程任务都满足当前虚拟地址空间中，只有它一个进程任务。

用户态与内核态

调试异常