

OS Readings

Dr. GuoJun LIU

Updated on February 25, 2019

目录

1	系统架构概览	1
1.1	系统级体系结构概览	1
1.2	实模式和保护模式转换	1
1.3	80x86 系统指令寄存器	1
1.4	系统指令	2
2	保护模式内存管理	3
2.1	内存管理概览	3
2.2	分段机制	3
2.3	逻辑地址和线性地址的转换	3
2.4	描述符的分类	4
3	中断和异常处理	5
3.1	中断和异常处理概述	5
3.2	有关中断和异常了解性的内容	5
3.3	中断描述符表	5
3.4	IDT 描述符	5
3.5	中断与异常处理	6

4 任务管理	7
4.1 任务管理概述	7
4.1.1 任务的结构	7
4.1.2 任务状态	7
4.1.3 任务的执行	7
4.2 任务的数据结构	8
4.3 任务切换	8
4.4 任务链	8
4.5 任务地址空间	8

第 1 章

系统架构概览

1.1 系统级体系结构概览

参照图 2.1，需要了解图中的所有系统级寄存器和数据结构，在后面的章节中都有介绍。

以下内容是要重点掌握的：

- 🔍 Global and Local Descriptor Tables
- 🔍 System Segments, Segment Descriptors, and Gates
- 🔍 Task-State Segments and Task Gates
- 🔍 Interrupt and Exception Handling
- 🔍 Memory Management
- 🔍 System Registers

1.2 实模式和保护模式转换

了解两种操作模式进行转换，所需要进行哪些修改。

1.3 80x86 系统指令寄存器

了解和掌握相关寄存器：

- 🔍 标志寄存器 EFLAGS
- 🔍 内存管理寄存器，包括 GDTR, LDTR, IDTR, TR
- 🔍 控制寄存器，包括 CR0 至 CR3

1.4 系统指令

了解和掌握相关系统指令：

☞ LGDT

☞ SGDT

☞ LIDT

☞ SIDT

☞ LLDT

☞ SLDT

☞ LTR

☞ STR

第2章

保护模式内存管理

2.1 内存管理概览

了解与掌握以下概念，并掌握它们之间的变换：

- ☞ 逻辑地址 Logical Address
- ☞ 线性地址 Linear Address
- ☞ 物理地址 Physical Address

有关分段管理的内容一定要掌握，有关分页的内容，我们会在以后的课程中详细介绍。

2.2 分段机制

了解以下分段模型：

- ☞ Basic Flat Model
- ☞ Protected Flat Model
- ☞ Multi-Segment Model

2.3 逻辑地址和线性地址的转换

重点掌握以下内容：

- ☞ 段选择子 Segment Selectors
- ☞ 段寄存器 Segment Registers，以及如何加载它们
- ☞ 段描述子 Segment Descriptors，掌握其结构

掌握以上概念后，思考如何将逻辑地址转换成线性地址的，处理器做了几件事？

2.4 描述符的分类

重点掌握有关描述符以下内容：

- ☞ 数据段描述符 Data segment Descriptor
- ☞ 代码段描述符 Code segment Descriptor
- ☞ 局部描述符表描述符 Local descriptor-table (LDT) segment descriptor
- ☞ 任务状态段描述符 Task-state segment (TSS) descriptor
- ☞ 调用门描述符 Call-gate descriptor
- ☞ 中断门描述符 Interrupt-gate descriptor
- ☞ 陷阱门描述符 Trap-gate descriptor
- ☞ 任务门描述符 Task-gate descriptor

第3章

中断和异常处理

3.1 中断和异常处理概述

- ☞ 什么是中断和异常？
- ☞ 处理器如何处理？

思考：模式和保护模式下，中断向量表一样吗？

3.2 有关中断和异常了解性的内容

- ☞ 中断和异常向量
- ☞ 中断源和异常源
- ☞ 异常的分类：故障、陷阱和中止
- ☞ 程序或任务的重新执行
- ☞ 开启和禁止中断
- ☞ 异常和中断的优先级

3.3 中断描述符表

- ☞ 如何构成？
- ☞ 如何获得中断处理程序的地址？
- ☞ 如何设置中断描述符表寄存器？

3.4 IDT 描述符

掌握以下描述符格式：

🔊 中断门

🔊 陷阱门

🔊 任务门

3.5 中断与异常处理

🔊 中断过程调用的流程是怎样的？

🔊 如何判断中断处理过程与被中断任务的优先级？

🔊 不同优先级上，处理方式一样吗？

🔊 如果发生堆栈切换，处理器会做哪些操作？

🔊 如果没发生堆栈切换，处理器会做哪些操作？

🔊 中断处理过程后，如何返回，处理器做了哪些操作？

🔊 异常和中断处理过程的保护

🔊 异常和中断处理过程的标志使用方式

🔊 中断门与陷阱门的唯一区别是什么？

第4章

任务管理

4.1 任务管理概述

- ☞ 什么是任务？
- ☞ 80x86 提供了哪些硬件支持？
- ☞ 描述符表中与任务相关的描述符有哪些？
- ☞ 任务切换与过程调用的区别是什么？

4.1.1 任务的结构

- ☞ 一个任务由几部分构成？
- ☞ 任务执行空间包括什么？
- ☞ 为什么会有多个特权级栈空间？

4.1.2 任务状态

- ☞ 当前正在执行的任务状态包括哪些内容？
- ☞ 掌握每一个被包含内容的含义？
- ☞ 为什么要包含这些内容？

4.1.3 任务的执行

- ☞ 任务的执行方式有几种？

- ☞ 熟悉掌握每一种执行方式的过程
- ☞ Linux 0.00 用的是哪种方式？
- ☞ 任务可以递归调用吗？为什么？

4.2 任务的数据结构

- ☞ 任务状态段 Task-State Segment (TSS)
- ☞ TSS 描述符
- ☞ 任务寄存器
- ☞ 任务门描述符 Task-Gate Descriptor

4.3 任务切换

此部分内容重点掌握：

- ☞ 什么时候发生任务切换？
- ☞ 发生任务切换时，处理器会执行哪些操作？
- ☞ 中断或异常向量指向 IDT 表中的中断门或陷阱门，会发生任务切换吗？

4.4 任务链

- ☞ 如何判断任务是否嵌套？
- ☞ 什么情况会发生任务嵌套？
- ☞ 任务嵌套时修改了哪些标志位？
- ☞ 任务嵌套时，如何返回前一任务？

4.5 任务地址空间

- ☞ 什么是任务地址空间？
- ☞ 任务地址空间包括什么？
- ☞ 了解把任务映射到线性和物理地址空间的方法？
- ☞ 了解任务逻辑地址空间，及如何在任务之间共享数据的方法？