Review LATX-X64 work

从开发到重构

SPC

Loongson Lab

2021 年 10 月 11 日

认知：从 X86 到 AMD64 的一些区别

- 寄存器层次的区别
- 指令层次的区别
- 地址空间的区别
- 运行模式的区别

寄存器层次的区别

64-Bit Mode 执行环境

- GPR
  - GPR 数量从 8 个增加到 16 个 (R8-R15)，位宽增加到 64 位
  - EFLAGS(RFLAGS) 变成 64 位宽度，高 32 位保留，低 32 位同 EFLAGS
- XMM/YMM
  数量从 8 个增加到 16 个
- Stack
  栈指针地址宽度固定 64 位，即只用 RSP 做寻址
- Control registers, ...
- RIP 为 64 位，并加入了对于 RIP 的相对寻址 *
- Flat address space*

寄存器层次的区别

字节寄存器的变动

- SIL，DIL，BPL，SPL 的加入[1]
- AH，BH，CH，DH 的调换[2]

[1]当 REX prefix 存在时（事实上，如果存在 R8-R15，REX 就一定存在）
[2]当 REX prefix 不存在时

寄存器层次的区别

字节寄存器的变动

- SIL，DIL，BPL，SPL 的加入[1]
- AH，BH，CH，DH 的调换[2]

寄存器运算：默认如果目标寄存器是 32 位的，高 32 位清零

```
01C3 ADD EBX,EAX ;32-bit add
Begin:  RAX = 0002_0001_8000_2201;
        RBX = 0002_0002_0123_3301;
Result: RBX = 0000_0000_8123_5502.
```

[1]当 REX prefix 存在时（事实上，如果存在 R8-R15，REX 就一定存在）
[2]当 REX prefix 不存在时

指令层次的区别

增加新前缀 REX

- 以前的 Prex 被称为 Legacy Prefixes
- 为了支持更多的寄存器，新增加 REX 的新前缀

- REX Prefix Fields [BITS: 0100WRXB] [3]
  - W: Operand Size: 0 = Default; 1 = 64 Bit Opsize
  - R: ModR/M
  - X: SIB index
  - B: ModR/M r/m, SIB base, or Opcode reg field

[3] Intel 64 and IA-32 Architectures Software Developer's Manual, 2.2.1 REX Prefixes

地址空间的区别

段寄存器的取消->Flat address space[4]

- 当然，他们还是会被正常装入 Segment-Register hidden part
- DS/ES/SS 对应隐藏部分被硬件忽略 (认为 `base = 0`)
- CS 对应隐藏部分只有部分属性可以使用 (L/D/DPL)
- FS/GS 对应隐藏部分只考虑 base
  1. Seg load 指令 (mov, pop) 只改变低 32 位地址
  2. 高 32 位地址映射到 MSR，通过指令 WRMSR 装入
     The FS.base MSR address is C000_0100h while the GS.base MSR address is C000_0101h.
  3. 装入 null selector 不改变地址
- GDTR/LDTR/SYS-Descriptor[5]
  1. LGDT/LIDT 可以加载 `m16&64`
  2. GDT 表项扩充到 128-bit（64-bit LDT/TSS/x Gate）

[4]AMD64 Architecture Programmer's Manual, Vol.2, 4.5.2 Segement Register
[5]AMD64 Architecture Programmer's Manual, Vol.2, 4.8.3 System Descriptors

地址空间的区别

RIP 相对寻址

- 在 x86 上，获取当前 PC 非常“痛苦”

```
        call _here
_here:  pop eax
        ; eax now holds the PC.
```

- AMD64 存在 `lea (rip), rax`
  - 在 64-bit mode 下打开，可以受 address-size prefix 改写 [6]
  - 当 `{mod,r/m} = 00101b` 时，启用 RIP + disp32 [7]

[6] AMD64 Architecture Programmer's Manual, Vol.1, 2.2.5.2 Effect of Address-Size Prefix on RIP-Relative Addressing

[7] AMD64 Architecture Programmer's Manual, Vol.3, 1.7 RIP-Relative Addressing

运行模式的区别

x86 运行模式

- Real Mode
- Virtual-8086 Mode
- Protected Mode

AMD64 运行模式

- Legacy Mode
  - Real Mode
  - Virtual-8086 Mode
  - Protected Mode
- Long Mode
  - Compatibility Mode
  - 64-Bit Mode

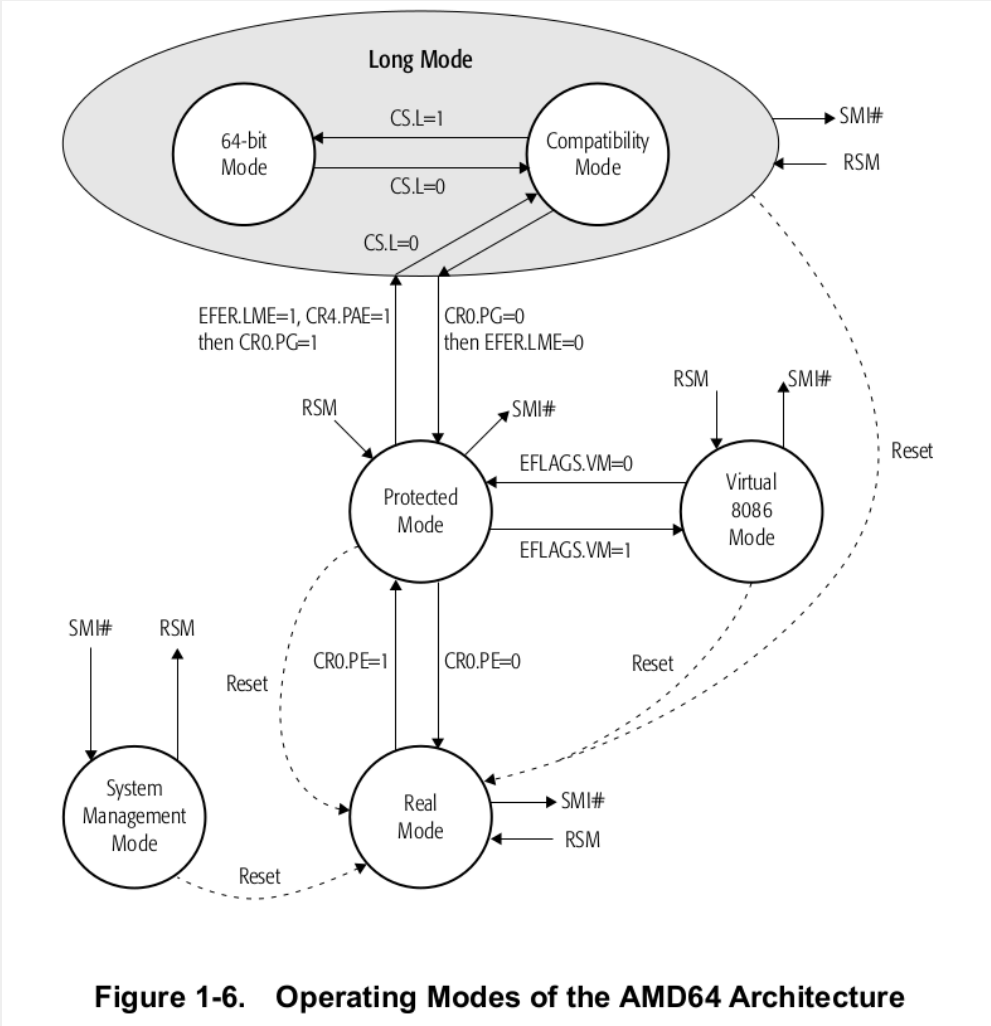

Figure 1-6. Operating Modes of the AMD64 Architecture

开发：以功能为导向

重构：以任务为驱动

- 红-绿-重构：CI 的角色
- Bug track & CM
- Code Review
- Patch and branch

红-绿-重构

红-绿-重构：CI 的角色

Bug track & CM

Code Review

Patch and branch