进程虚拟地址处理

**1 进程顶层抽象 与section**

每个进程抽象为一个ko\_process结构，其中包括进程的虚拟地址区间(section)的链表

struct ko\_process

{

int cpl;

struct km mem\_ctx;

struct ke\_spinlock vm\_list\_lock;

struct list\_head vm\_list;//section 链表

/\* Handle table \*/

void \*handle\_table;

spinlock\_t handle\_lock;

};

section链表用于描述进程已申请的一系列虚拟地址区间，每个section描述一段连续的虚拟地址，各section下根据需要还可进一步划分为若干sub-section。

**2 用户进程“眼中”的虚拟地址**

下图用户进程虚拟地址布局示例：



注：

1. Kernel section覆盖内核段全部虚拟地址空间

支持用户进程在内核态运行时，将vmalloc的物理页面映射到自身的虚拟地址空间中。

目前空间长度定义的是2G–4M

1. STACK section 不一定在用户虚拟地址段的高位，可能在任意位置

**3. 内核“眼中”的虚拟地址**

内核利用init\_prcess“进程”的section链表管理内核虚拟地址空间：



注：

1. init\_porcess 没有建立内核直接映射部分的section
2. 在高于内核直接映射部分的地址开始，建立了若干section，作为vmalloc物理页面真正的“拥有者”；用户进程仅仅是“共享映射关系”。

用户进程在执行过程中，根据需要从section中分配内核段虚拟空间，并将映射关系复制到自身页表中。

3 **用户进程section类型**

1. EXE section：

管理用户进程可执行二进制的虚拟地址空间

进程初始化过程中建立EXE section；分析二进制文件，将EXE section分为若干sub-section，每个sub-section对应一个二进制文件的segment 。

EXE section初始化后没有映射的物理地址页面，在运行过程中，由缺页中断处理各个sub-section的物理页面分配。

可分为以下若干sub-section

* BSS

管理BSS段地址，完全私有。

撤销BSS时，其映射的物理页可完全释放

BSS段判断条件：KM\_PROT\_WRITE ????

* 共享

管理与其他进程共享的地址，例如libc库函数，各个进程共享虚拟地址等于EXE段基地址+share.offset，各个进程共享部分的地址映射均复制自系统第一个用户进程。

Section撤销时，只能解除页表映射，不能释放物理页

共享段的pte表项设置PAGE\_FLAG\_FROM\_OTHER || READ 标记

* 其他类型

管理进程独有的二进制地址，为进程私有

pte表项设置为READ || WRITE

此类地址在section撤销时，释放物理页。

综上，EXE section在撤销时，扫描对应页表项，具有KM\_PROT\_WRITE标记的pte映射的物理页面可以释放。（这个是否正确）

1. Private类型的section

管理由malloc系列接口分配的用户段虚拟地址。

关闭private类型的section将释放映射的物理页。

1. STACK类型的section

管理栈的地址空间，完全私有的section，处理同private类型。

1. 共享类型的section

管理多进程“显示共享”的空间

这部分虚拟地址将映射多个进程共享的物理页面，缺页中断时，复制源进程的页表，并将本地pte项设置PAGE\_FLAG\_FROM\_OTHER标记

撤销该section时，只能清除虚拟地址映射，不能释放物理页。

1. FILE类型section

FILE类型section用于管理文件映射的地址

将文件读入文件系统缓存，在缺页中断中将文件内容读入，并将缓存页表映射复制到目标进程的页表中。

注：缓存的虚拟地址来自于kernel\_vm\_object section，kernel\_vm\_object section属于init\_process地址空间中，因此需要从init进程页表中复制。

kernel\_vm\_object映射的物理页属于系统全局物理页

目标进程释放section时，只解除页表映射，不释放物理页。

1. Kernel类型section

“映射”内核段虚拟地址

所有内核虚拟地址页面属于内核，当用户进程关闭撤销kernel section时，只撤销映射关系，不释放页面