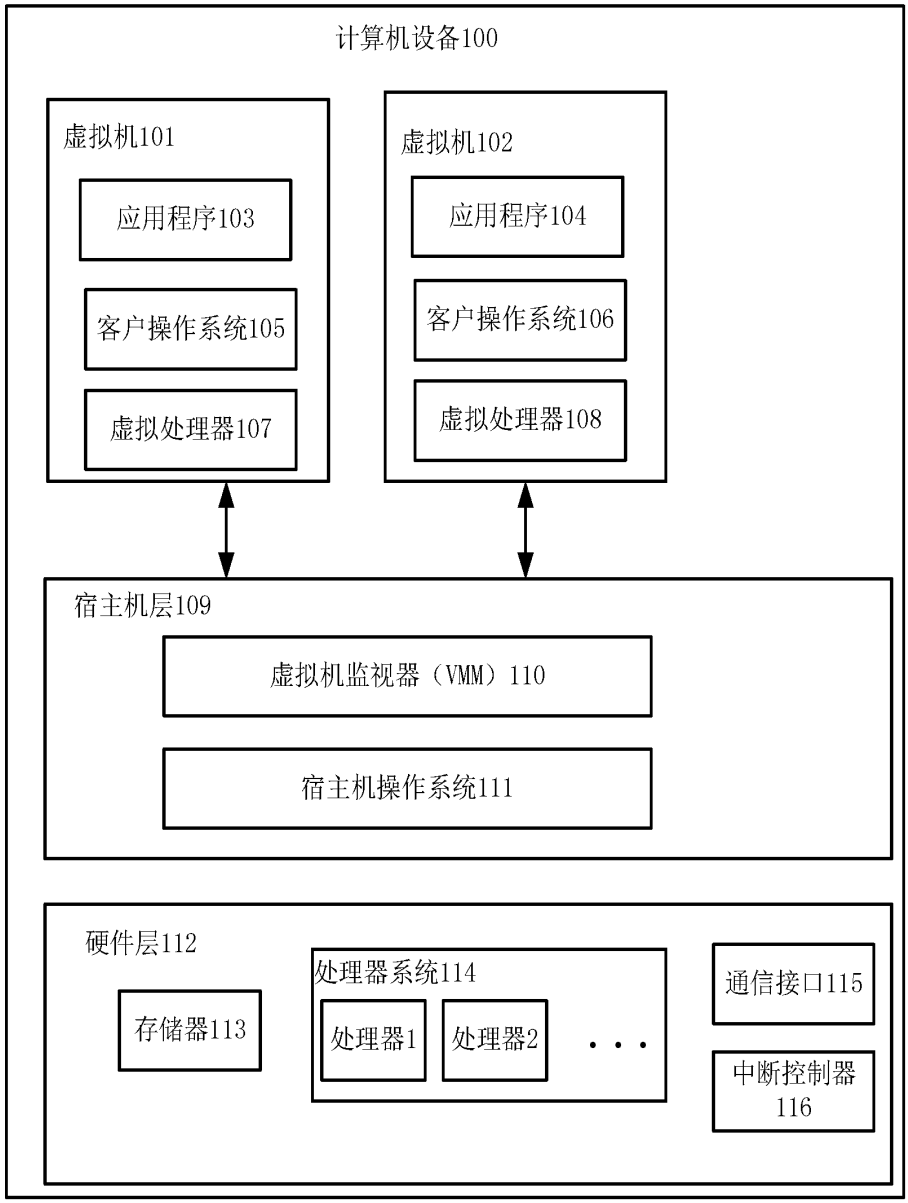
计算机设备100
虚拟机101
应用程序103
客户操作系统105
虚拟处理器107
虚拟机102
应用程序104
客户操作系统106
虚拟处理器108
宿主机层109
虚拟机监视器（VMM）110
宿主机操作系统111
硬件层112
存储器113
处理器系统114
处理器1
处理器2
. . .
通信接口115
中断控制器
116

图 1

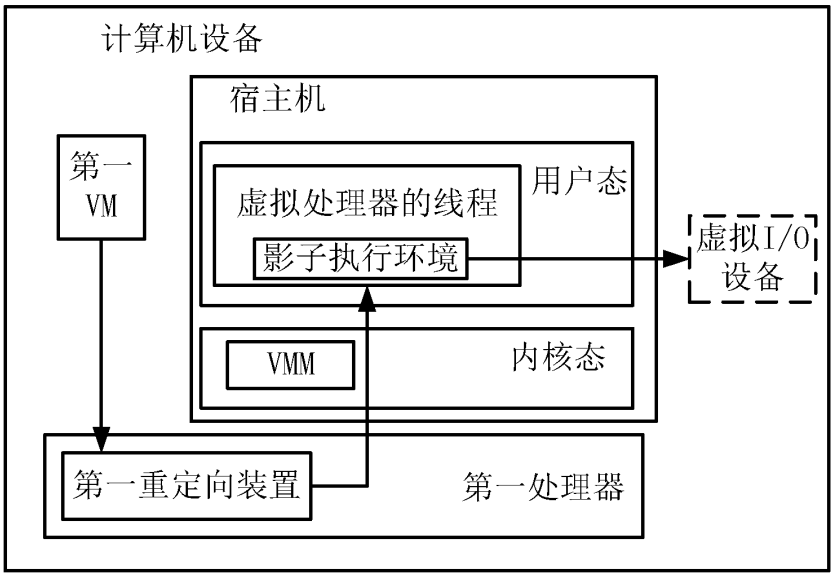
计算机设备
宿主机
第一
VM
虚拟处理器的线程
用户态
影子执行环境
虚拟I/O
设备
VMM
内核态
第一重定向装置
第一处理器

图 2

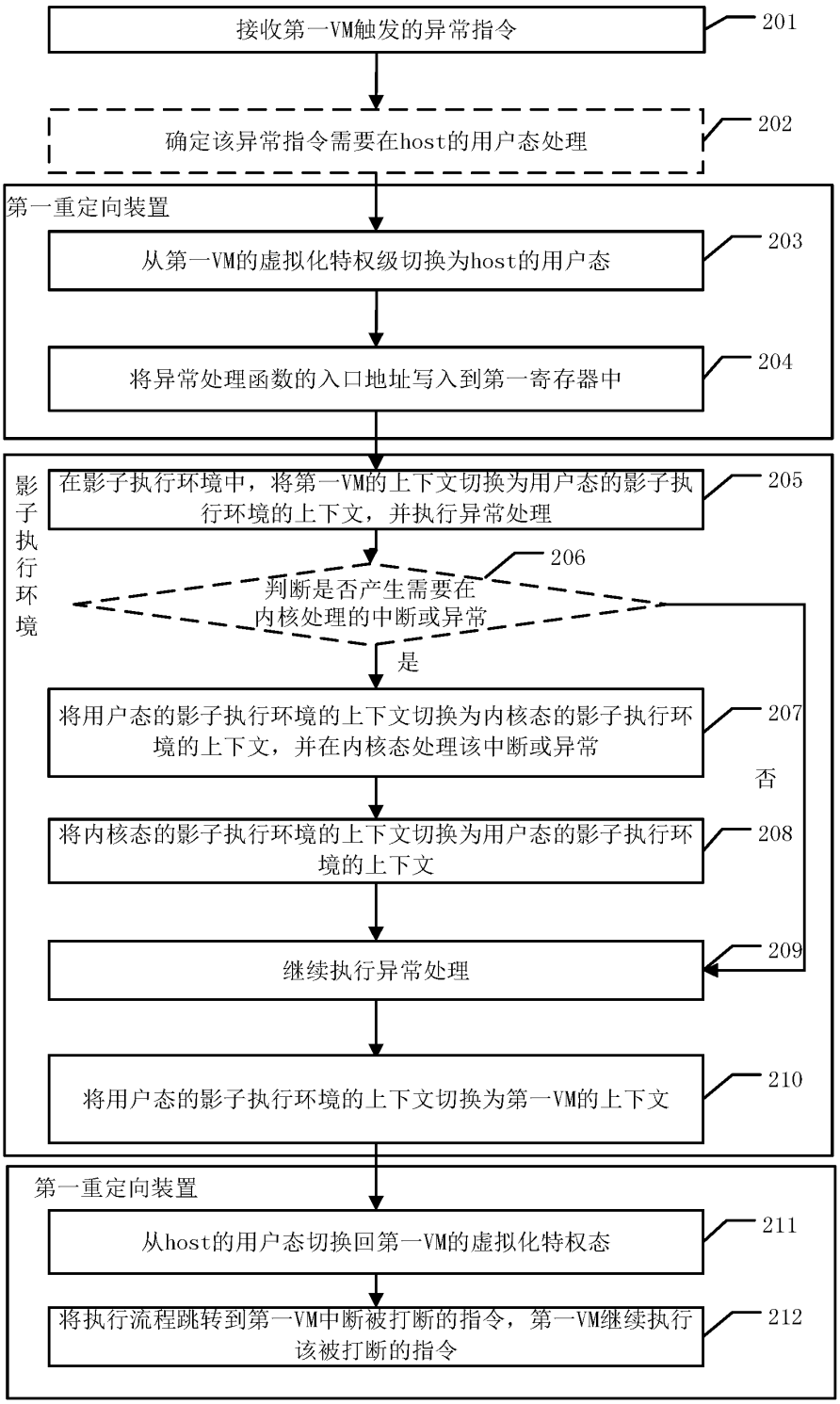
接收第一VM触发的异常指令
201
确定该异常指令需要在host的用户态处理
202
第一重定向装置
从第一VM的虚拟化特权级切换为host的用户态
203
将异常处理函数的入口地址写入到第一寄存器中
204
影子执行环境
在影子执行环境中，将第一VM的上下文切换为用户态的影子执行环境的上下文，并执行异常处理
205
判断是否产生需要在内核处理的中断或异常
206
是
否
将用户态的影子执行环境的上下文切换为内核态的影子执行环境的上下文，并在内核态处理该中断或异常
207
将内核态的影子执行环境的上下文切换为用户态的影子执行环境的上下文
208
继续执行异常处理
209
将用户态的影子执行环境的上下文切换为第一VM的上下文
210
第一重定向装置
从host的用户态切换回第一VM的虚拟化特权态
211
将执行流程跳转到第一VM中断被打断的指令，第一VM继续执行该被打断的指令
212

图 3

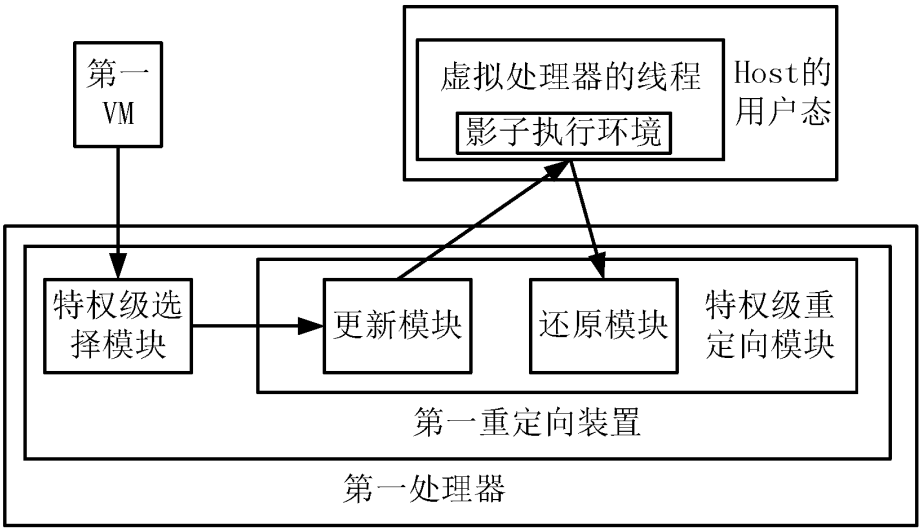
第一
VM
虚拟处理器的线程
影子执行环境
Host的
用户态
特权级选
择模块
更新模块
还原模块
特权级重
定向模块
第一重定向装置
第一处理器

图 4

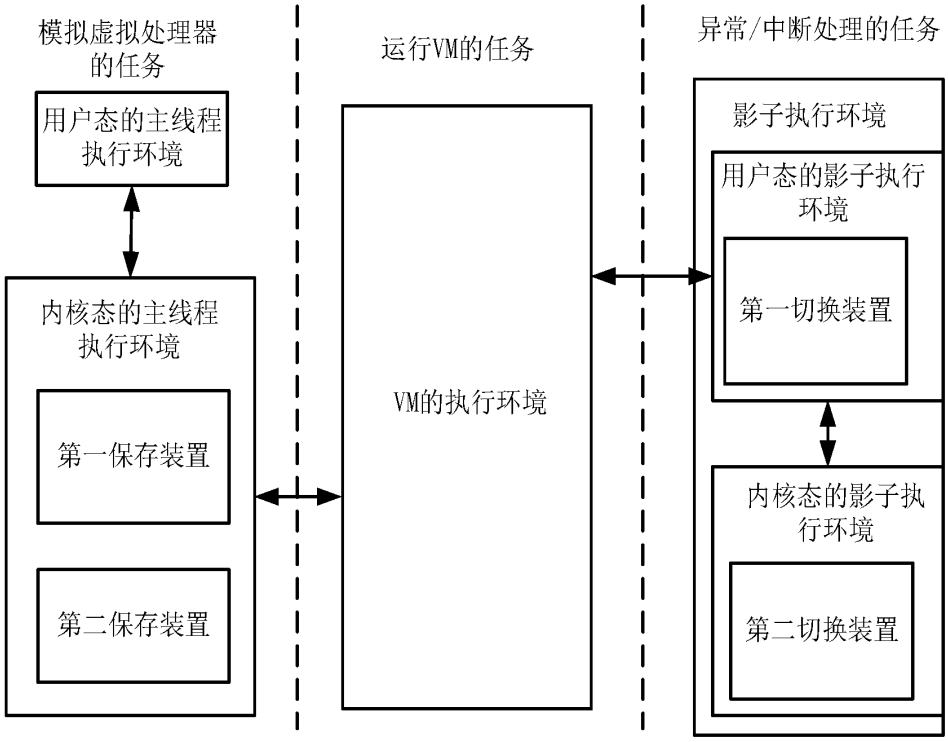
模拟虚拟处理器
的任务
用户态的主线程
执行环境
内核态的主线程
执行环境
第一保存装置
第二保存装置
运行VM的任务
VM的执行环境
异常/中断处理的任务
影子执行环境
用户态的影子执行
环境
第一切换装置
内核态的影子执
行环境
第二切换装置

图 5

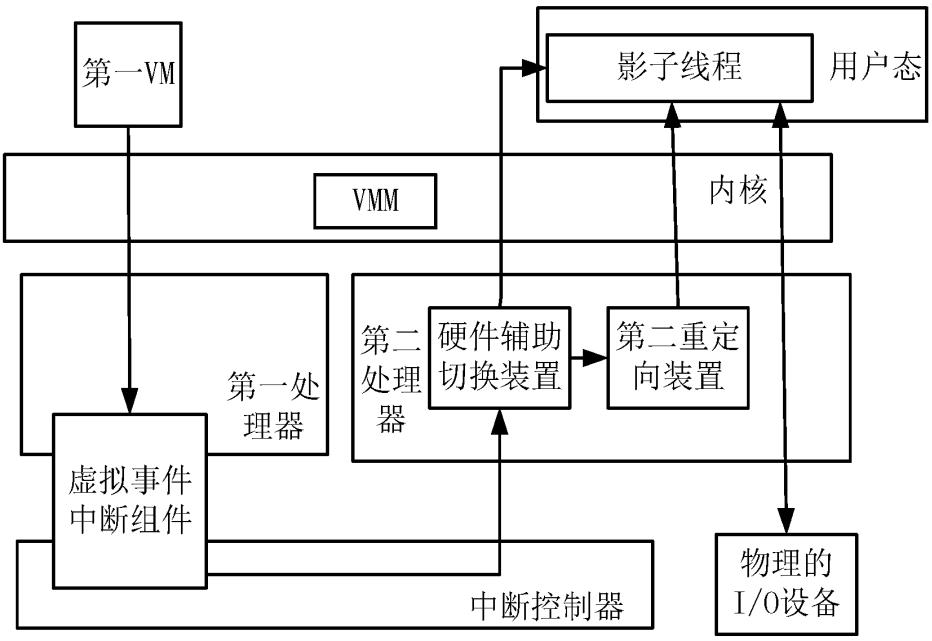
第一VM
影子线程
用户态
VMM
内核
第一处理器
虚拟事件中断组件
第二处理器
硬件辅助切换装置
第二重定向装置
中断控制器
物理的I/O设备

图 6

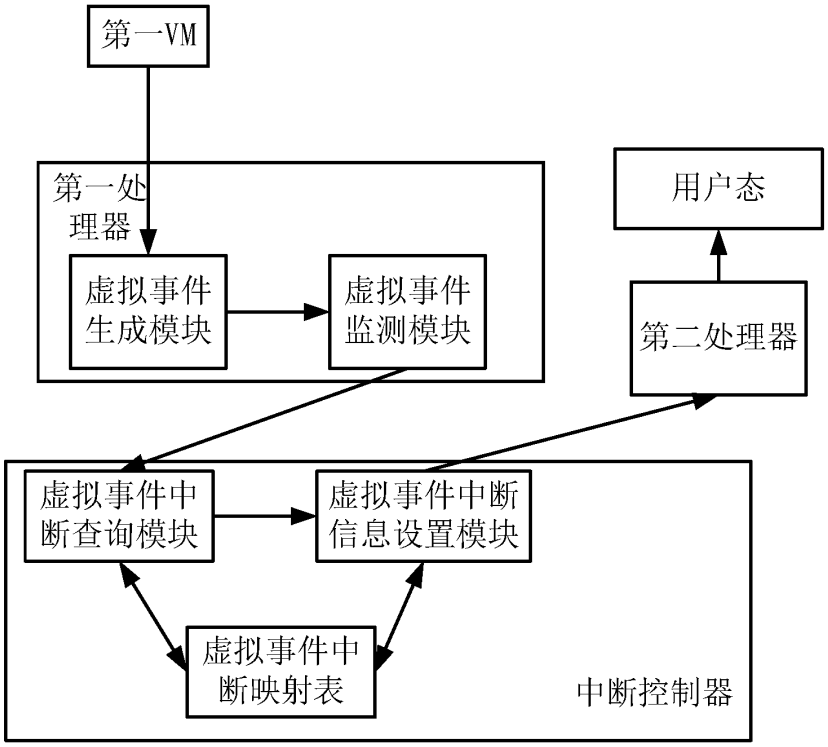
第一VM
第一处理器
虚拟事件生成模块
虚拟事件监测模块
用户态
第二处理器
虚拟事件中断查询模块
虚拟事件中断信息设置模块
虚拟事件中断映射表
中断控制器

图 7A

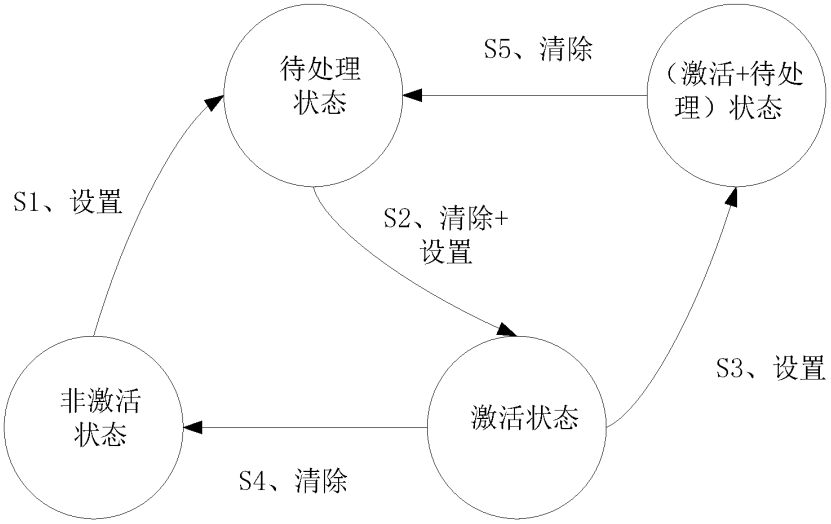
待处理状态
S5、清除
（激活+待处理）状态
S1、设置
S2、清除+设置
S3、设置
非激活状态
激活状态
S4、清除

图 7B

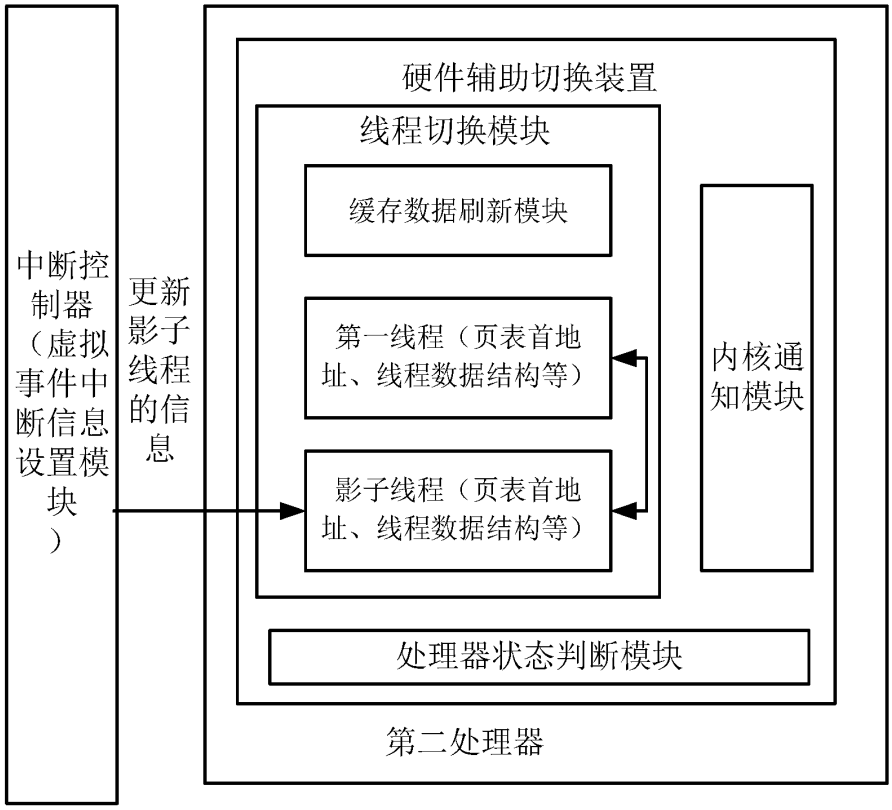
中断控制器（虚拟事件中断信息设置模块）
更新影子线程的信息
硬件辅助切换装置
线程切换模块
缓存数据刷新模块
第一线程（页表首地址、线程数据结构等）
影子线程（页表首地址、线程数据结构等）
内核通知模块
处理器状态判断模块
第二处理器

图 8

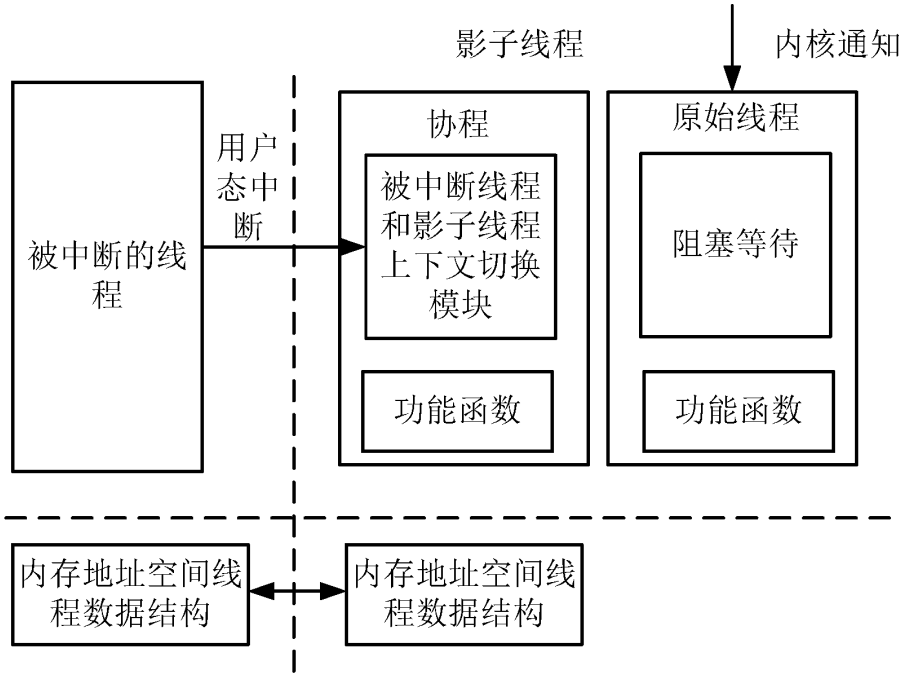
影子线程
内核通知
被中断的线程
用户态中断
协程
被中断线程和影子线程上下文切换模块
功能函数
原始线程
阻塞等待
功能函数
内存地址空间线程数据结构
内存地址空间线程数据结构

图 9

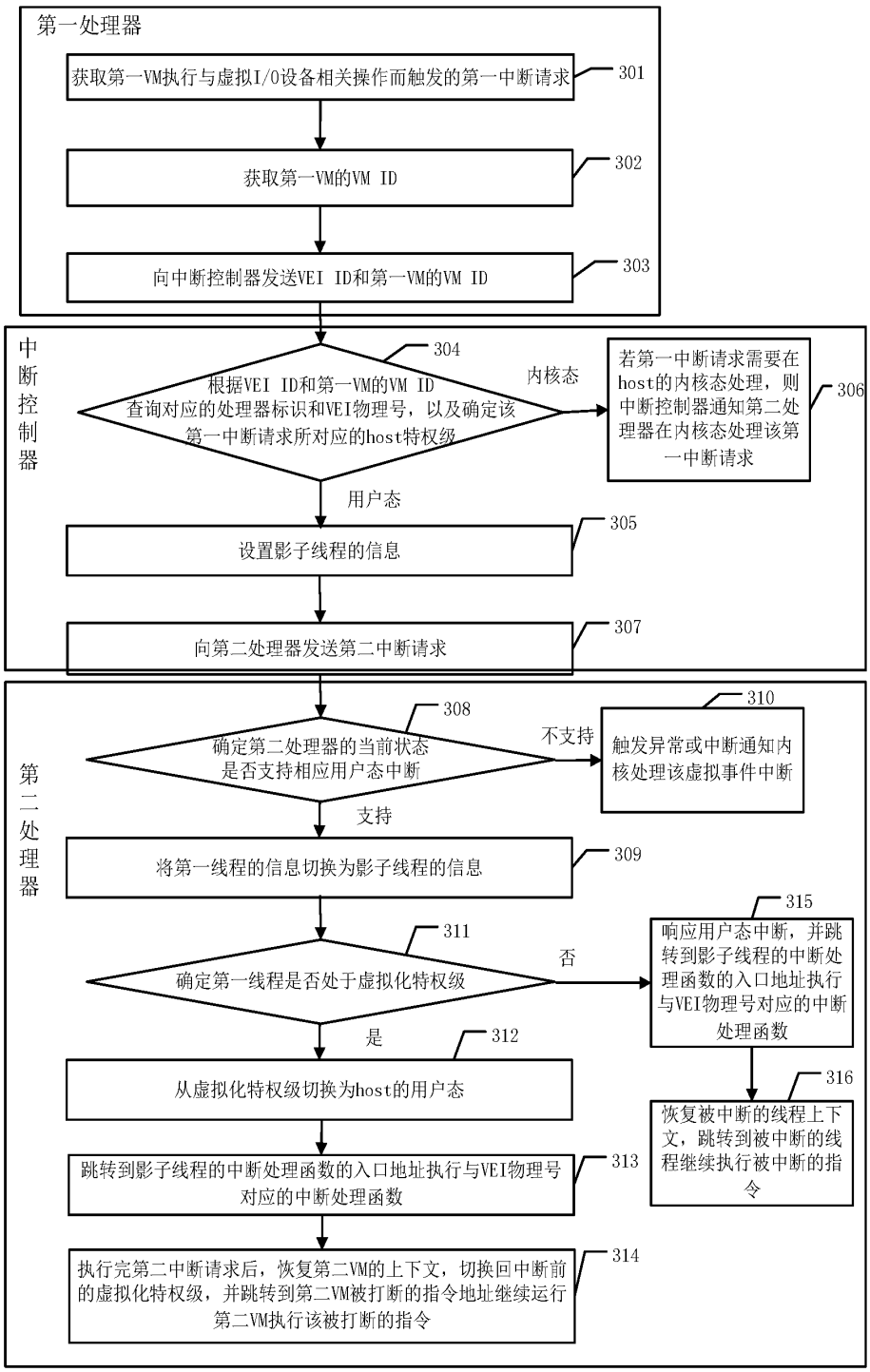
第一处理器
获取第一VM执行与虚拟I/O设备相关操作而触发的第一中断请求
301
获取第一VM的VM ID
302
向中断控制器发送VEI ID和第一VM的VM ID
303
中断控制器
304
根据VEI ID和第一VM的VM ID查询对应的处理器标识和VEI物理号，以及确定该第一中断请求所对应的host特权级
内核态
若第一中断请求需要在host的内核态处理，则中断控制器通知第二处理器在内核态处理该第一中断请求
306
用户态
设置影子线程的信息
305
向第二处理器发送第二中断请求
307
第二处理器
308
确定第二处理器的当前状态是否支持相应用户态中断
不支持
触发异常或中断通知内核处理该虚拟事件中断
310
支持
将第一线程的信息切换为影子线程的信息
309
311
确定第一线程是否处于虚拟化特权级
否
响应用户态中断，并跳转到影子线程的中断处理函数的入口地址执行与VEI物理号对应的中断处理函数
315
是
312
从虚拟化特权级切换为host的用户态
恢复被中断的线程上下文，跳转到被中断的线程继续执行被中断的指令
316
跳转到影子线程的中断处理函数的入口地址执行与VEI物理号对应的中断处理函数
313
执行完第二中断请求后，恢复第二VM的上下文，切换回中断前的虚拟化特权级，并跳转到第二VM被打断的指令地址继续运行第二VM执行该被打断的指令
314

图 10

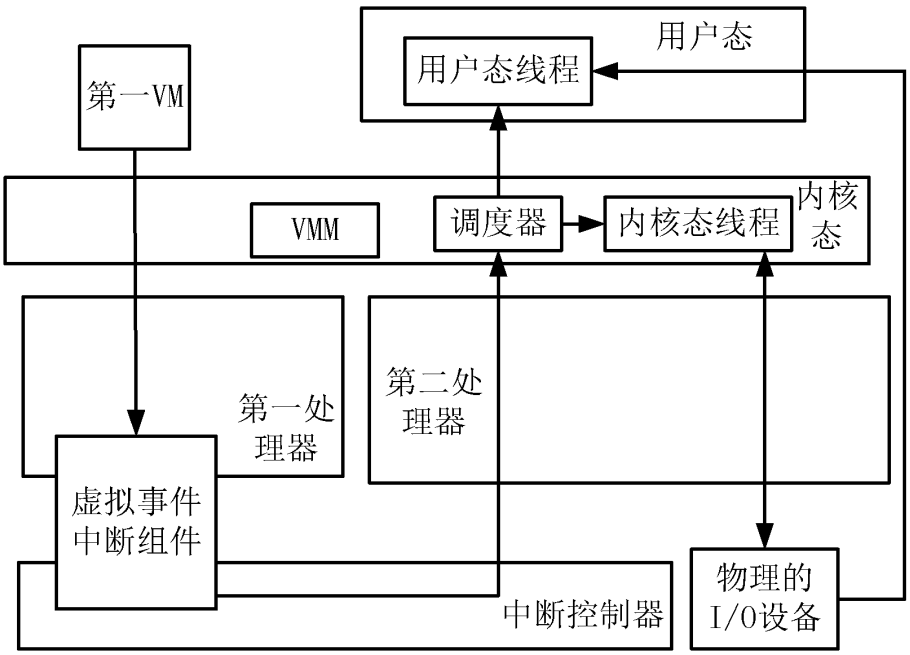
用户态
用户态线程
第一VM
VMM
调度器
内核态线程
内核态
第一处理器
第二处理器
虚拟事件中断组件
中断控制器
物理的I/O设备

图 11

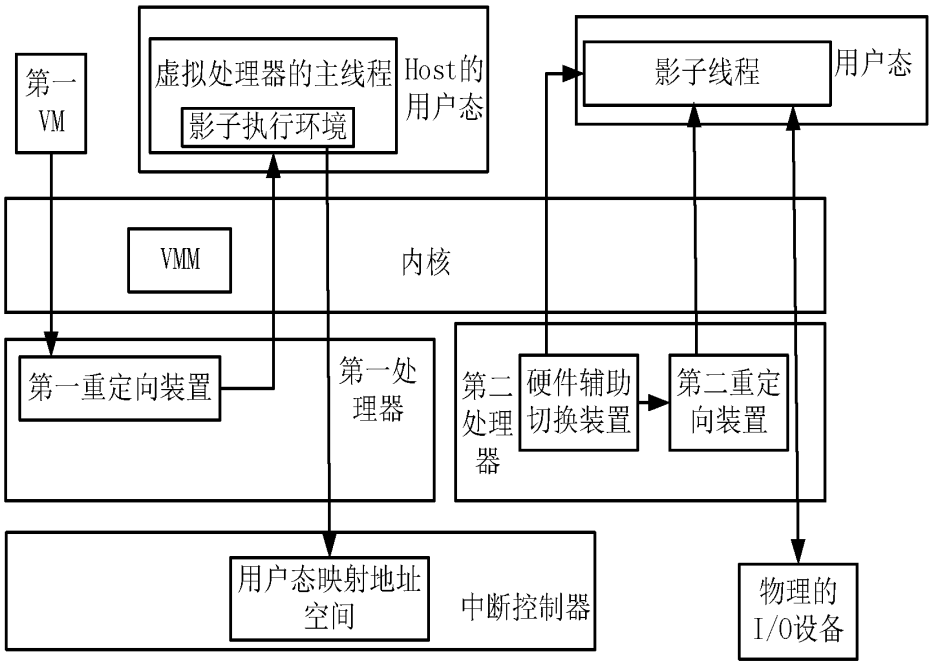
第一VM
虚拟处理器的主线程
影子执行环境
Host的用户态
影子线程
用户态
VMM
内核
第一重定向装置
第一处理器
第二处理器
硬件辅助切换装置
第二重定向装置
用户态映射地址空间
中断控制器
物理的I/O设备

图 12

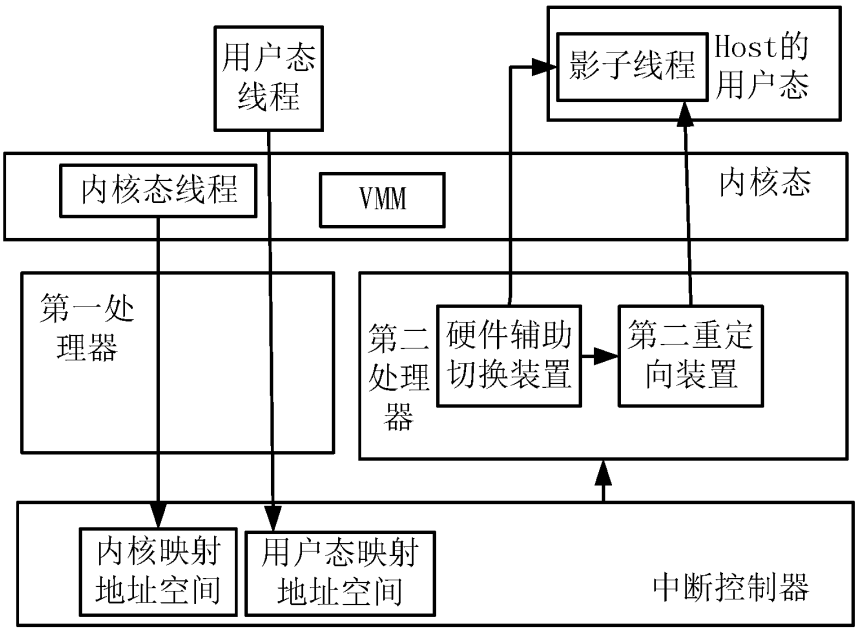
用户态
线程
影子线程
Host的
用户态
内核态线程
VMM
内核态
第一处
理器
第二
处理
器
硬件辅助
切换装置
第二重定
向装置
内核映射
地址空间
用户态映射
地址空间
中断控制器

图 13