L4 eXperimental Kernel

Reference Manual

Version X.2

分析文档

刘伟浩

2017.12.31

关于手册

手册理解

这个L4参考手册是所有L4 API和ABI的定义文档。 阅读本参考手册需要读者对L4的基本概念和硬件体系结构有深入了解。本手册的重点是精确的定义，而不是解释和说明。

此 L4 参考手册定义了所有32位和64位计算机的通用 API。因此, 通用参考手册是独立于特定处理器体系结构。它还辅以处理器特定的 ABI 规范。

在这篇文档中, 我们区分逻辑接口, 通用二进制接口、通用编程接口、便捷编程接口和特定于处理器的二进制接口。

* **逻辑接口**。逻辑接口定义所有概念和逻辑对象, 如系统调用操作、逻辑数据对象、数据类型及其语义。总之, 它们构成了逻辑 L4 API。
* **通用二进制接口**。大多数数据类型和一般数据对象的二进制表示是独立于特定处理器定义的 (尽管有两个不同的版本, 一个针对32位一个针对64位处理器)。两个版本一起形成 L4 的一般二进制接口。

逻辑接口加上通用二进制接口可以被看作是硬件的一个完整的规范独立的 L4 微内核接口。但是, 出于易用性和标准化的原因, 所提到的两个基本接口由另外两个接口类来补充:

* **通用编程接口**。通用编程接口定义逻辑接口的对象和通用二进制接口作为伪 c++ 类。与常规 c 语言绑定的语言大部分与 c++ 相同。对于 c 语言导致函数命名冲突的情况,函数名在方括号中给出。目前, 只指定 API 的 c 和 c++ 版本。其他语言接口的具体语法将被保留。稍后, 所有语言绑定都将包括在泛型编程接口.
* **便捷编程接口**。此接口不是严格意义上的 L4 微内核规范的一部分。它的所有数据类型和程序都可以使用通用编程接口实现。严格的说, 这是一个微内核之上的接口, 使最常见的操作对程序员来说更容易使用。重要的是要明白, 这个接口的目标是方便和易用性, 而不是完整性。它们提供的操作包括大约95% 的微内核功能。对于余下的 5%, 程序员必须使用基本 (不那么方便) 的通用编程接口来实现。显然, 便捷编程接口不是强制性的。因此, 从极简的角度来看, 不需要将它包含在通用的 L4 规范中。

然而, 由于标准化的原因, 因而软的可移植性洁具, 每一个完整的 L4 语言绑定必须包括整个便捷编程接口。

虽然便捷编程接口完全可以在通用编程接口之上实现, 即处理器独立的, 但是便捷编程接口的实现者也可以实现它的硬件依赖, 从而纳入任何优化, 成为可能针对特定的处理器而定制的二进制接口。

手册说明

* **基本数据类型**。基本数据类型是 word64，word32，word16，分别代表数据大小是 64、32、16位，并且与处理器无关；
* **特权线程**。某些系统调用只能由特权线程执行。任何与内核在启动时创建的初始线程属于同一地址空间的线程, 被视为特权线程。
* **位域**。位字段长度表示为下标（i/j），其中 i 是针对32位处理器，j 是针对64位处理器。如果仅仅只有下标 i 则表示32位和64位处理器有相同的位域。字节偏移是以 正负i/正负j 来分别表示32位处理器和64位处理器。如果所指定的字节，所有位字段都是只加32位，那么对于64位机剩下的32位，则是未定义或者是被忽略的。
* **符号“ ~ ”** 。输出参数或位字段可以是未定义的，对应的未定义参数或字段由 ~ 标记。它表示输出是没有被定义的值, 也就是说, 它们可能有任何值, 也甚至可能无法访问。任何依赖于未定义的参数或位字段的算法都视为不正确。
* **符号“ - ”** 。输入参数或位字段可以被指定为忽略, 由 - 表示。此类参数或字段可以保留任何值, 而不会影响被调用的服务。- 还可以定义可用于其他信息的位域。例如, fpage 外延包含一些被忽略的位, 它们用于某些系统调用中的访问控制位。
* **符号“ Ξ ”** 。在特定于处理器的接口中, 寄存器有时定义为不变。这时候就用 Ξ 表示。
* **向上兼容性**

1. 输出参数和位字段

当前被定义为 ~ 未定义的参数或者位字段可以被指定为已定义的。这些新定义的字段将只提供额外附加信息。如果系统调用与当前API中指定的方法是一样的，那么就可以忽略这些新定义的东西。

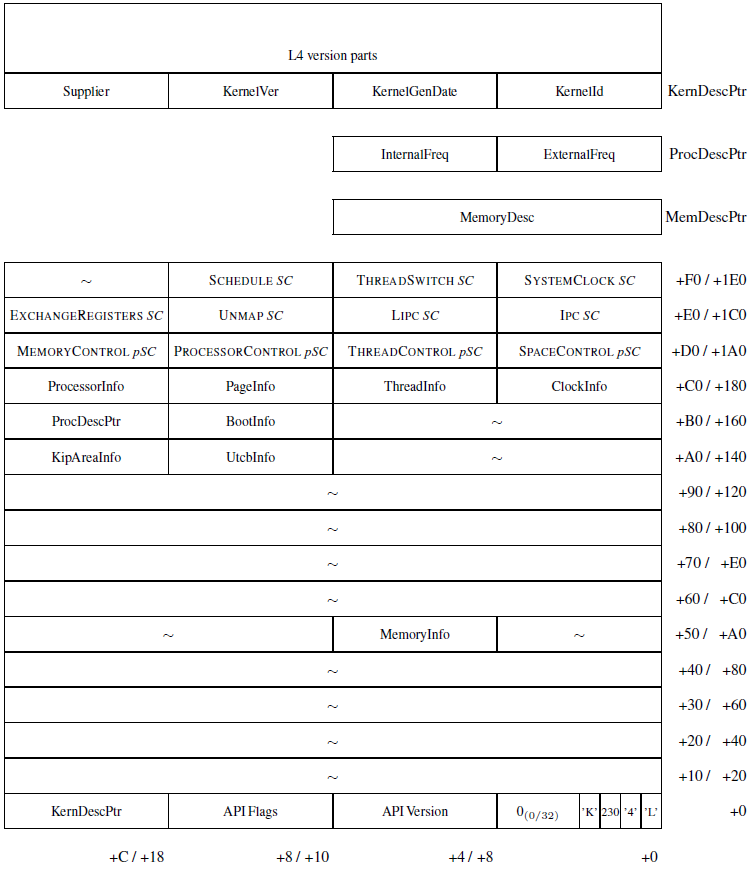
1. 输入参数与位字段

当前被定义为 - 忽略的字段可以指定为已定义的。但是这些字段的内容只与新定义的功能相关。如果这些API和指定用旧语义的系统调用一同使用，那么这些域将会被忽略。

第一章 基本内核接口

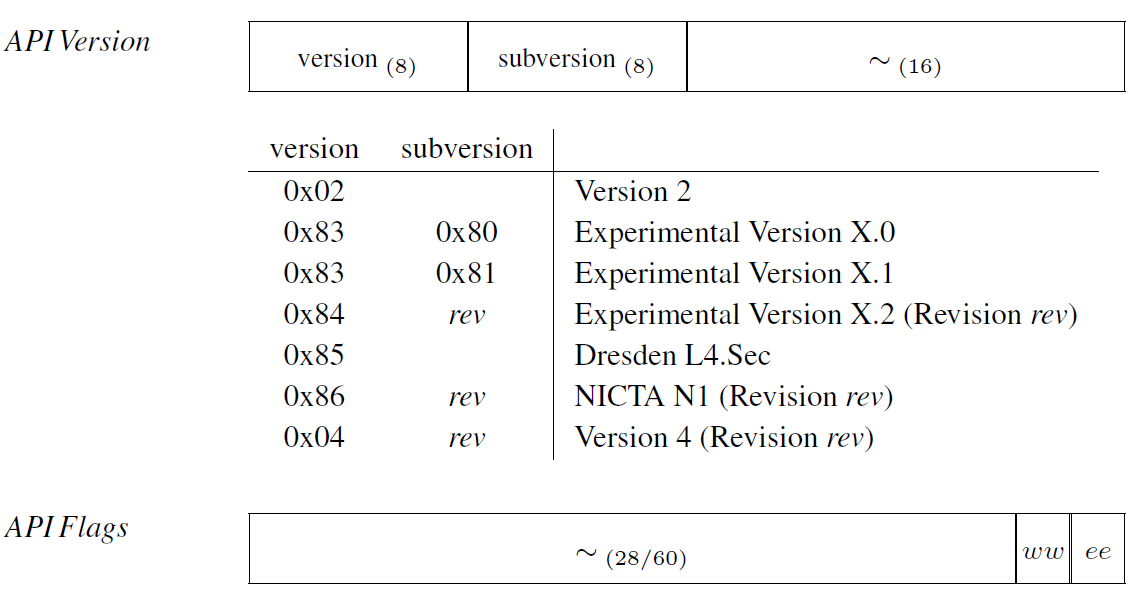
1.1内核接口页 [数据结构]

内核界面页包含 API 和内核版本数据、系统描述符包括内存描述符和系统调用链接。页的其余部分未定义。

该页面是一个微内核对象。是的在地址空间创建时, 通过微内核直接映射到每个地址空间。它不是由pager映射的, 不能映射或授予另一个地址空间, 也不能被取消映射。新地址空间的创建者可以指定需要映射内核接口页的位置。此地址将在该地址空间的生存期内保持不变。任何线程都可以通过KERNELINTERFACE这个系统调用获取内核接口页的地址。

如上图所示，右边的偏移是以字节为单位，一个字节不论32位还是64位机都是8位长度。每一行看做四等分，则每一份都是一个字，只是32位机的字是32位，64位机的字是64位。

**API描述部分**

其中

ee = 00 : 小端模式

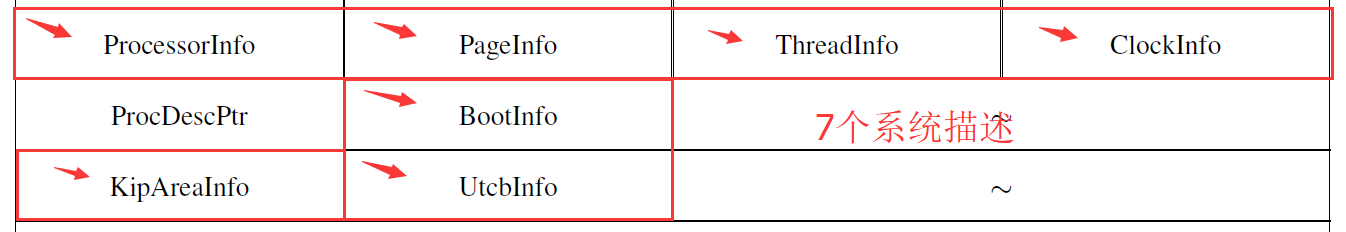
ee = 01 : 大端模式

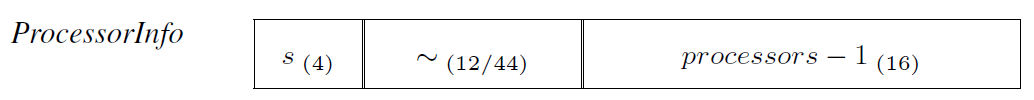
ww = 00 : 32位API

ww = 01 : 64位API

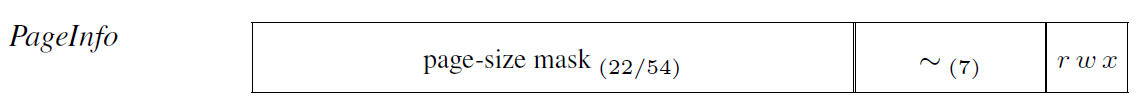
注意, 此字段不能直接用于区分大端模式和小端模式, 因为 ee 字段驻留在两个模式的不同字节中。此外, API 标志的偏移地址对于32位和64位模式是不同的。总之, 直接检查内核接口页不足以安全地区分32/64 位模式和小/大端模式。

通过KERNELINTERFACE系统调用来启用安全模式检测.安全模式检测可以在寄存器中传递 *APIFlags*。

**系统描述部分**

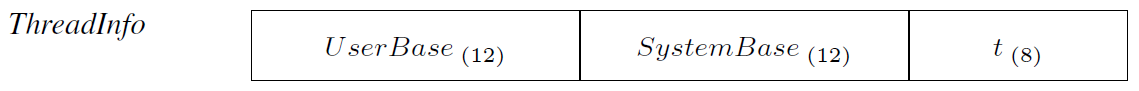
s 单个处理器描述占用的区域大小为2s。第一个处理器的描述字段的位置由 ProcDescPtr 表示。后续处理器的描述字段位于前一个之后。

processors 可用系统处理器的数量



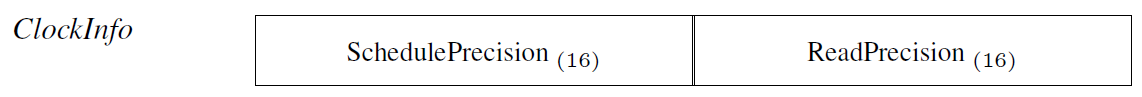
page-size mask 如果位 k-10 的page-size mask字段 (整个word的第 k 位) 设置为1，硬件和内核支持大小为2k的页。如果该位是0，硬件和/或内核不支持大小为2k的页。注意即使2k不是硬件支持的页面大小，大小为2k 的fpages也可以使用。有关支持的硬件页面大小的信息只是一个性能提示。

r w x 标识可以独立于其他访问权限设置的受支持的访问权限 (读取、写入、执行)。一个1位的信号可以在映射页上设置和重置该权限。处理器将隐式允许在任何映射页上读取和执行访问。



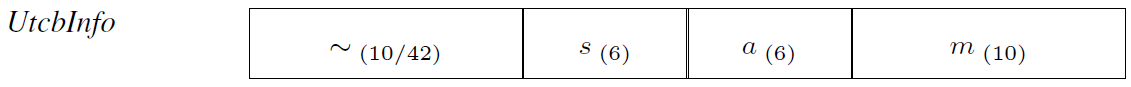
t 有效的线程号位数。"线程编号" 字段可能较大, 但仅位 0…t-1 对内核是有效的。较高的位必须都是0。

*UserBase* 用户线程可用的最低线程号 (请参见页14).前三线程号将分别用于初始线程σ0, σ1和root task(请参见页92)。这些初始线程的版本号将等于1。

*SystemBase* 用于系统线程的最低线程号 (请参见页14).此值下面的线程号表示硬件中断。

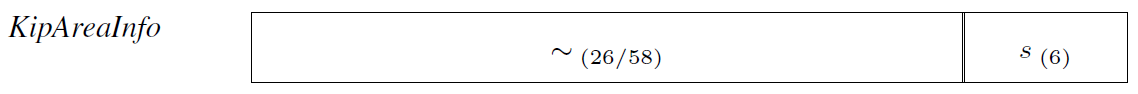
ReadPrecision 指定通过SYSTEMCLOCK系统调用读取系统时钟可以检测到的最小时间差不等于0。 基本上，这就是读取系统时钟时候的精度。

SchedulePrecision 指定基于唤醒时间的调度线程激活的最大抖动 (±):（假定没有更高或同等优先级的线程处于活动状态并启用计时器中断)。精度以时间段形式给出 (参见页30).



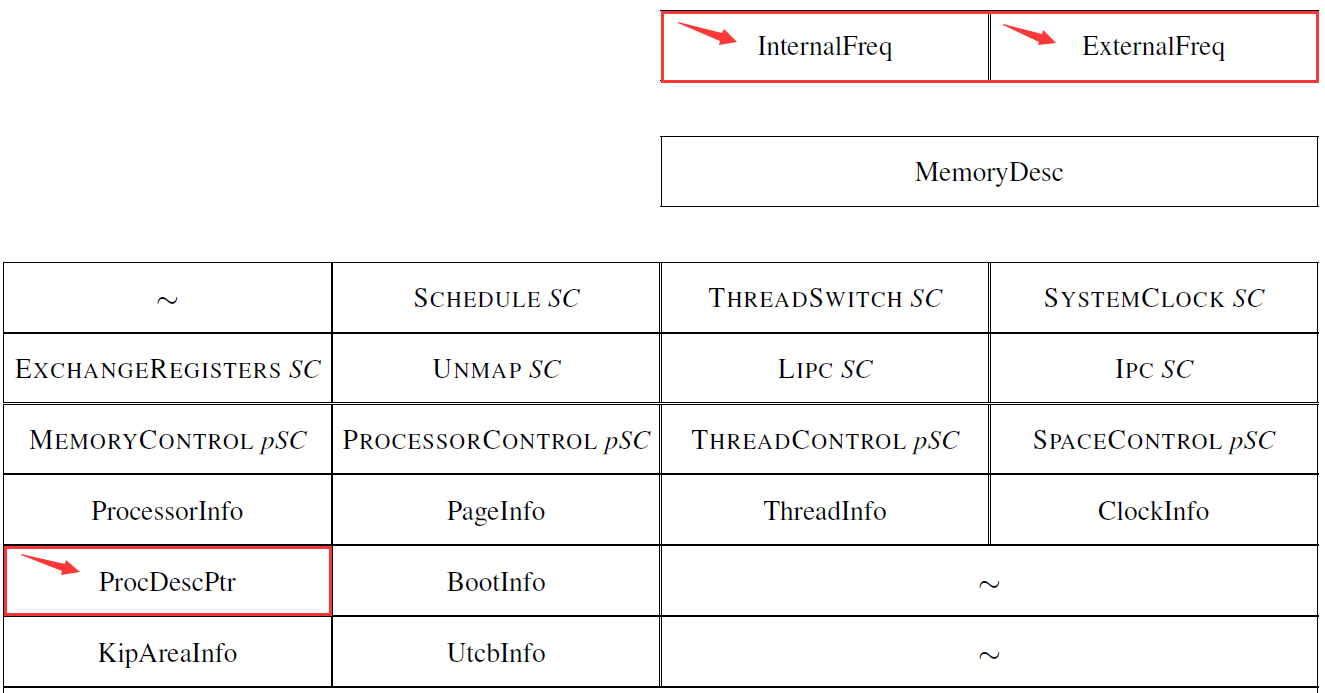
s 地址空间中的 UTCB 区域的最小大小是2s。UTCB 区域的大小限制了线程的总数量 k ,且满足式子2a mk ≤ 2s.

m UTCB大小的乘数。

a UTCB 位置必须与2a对齐。一个 UTCB 所需的总大小是2am 。

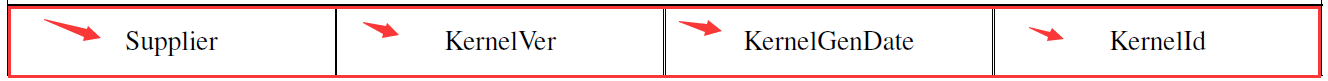
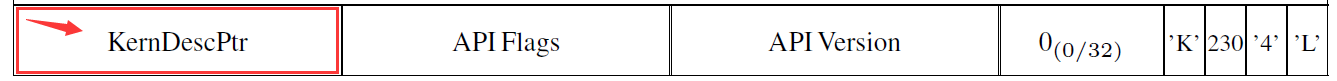
s 内核接口页的大小是2s

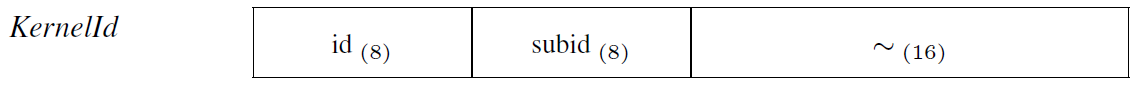
*Bootinfo* 在内核初始化之前, 引导加载程序可以将任意值写入内核配置页的 BootInfo 字段中 (请参见页92).初始化后的代码, 例如, 根服务器可以稍后从内核界面页读取该字段。它的值既不改变也不被内核解释。这是一个通过内核初始化传递系统信息的通用方法。

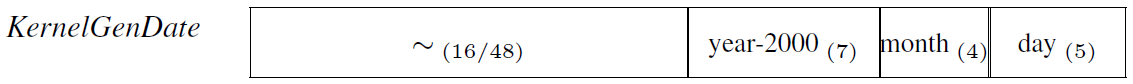
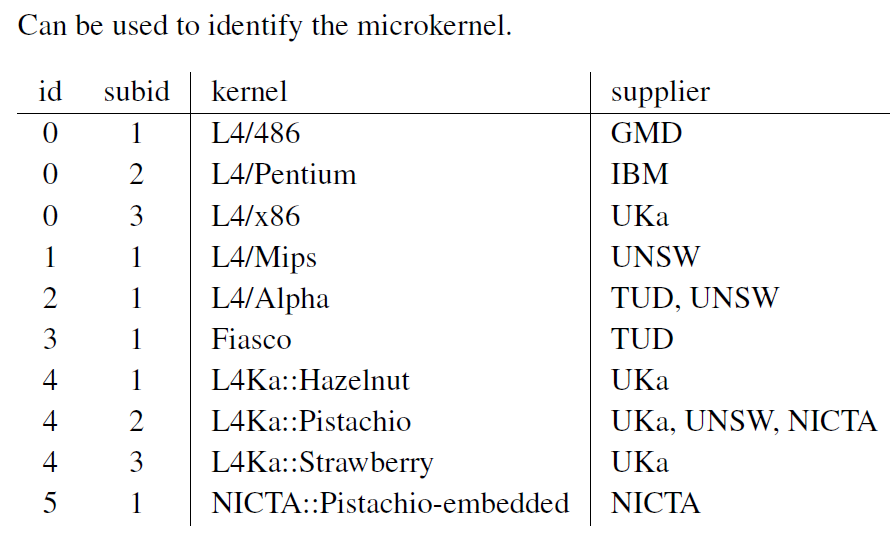
**处理器描述部分**

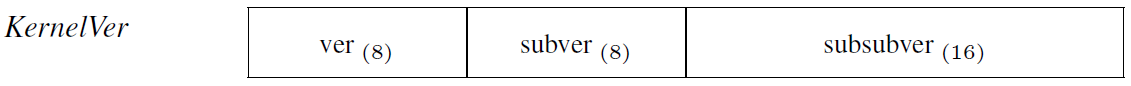
ProcDescPtr 指向一个数组, 其中包含每个系统处理器的说明。ProcessorInfo域包含数组的维度。ProcDescPtr作为相对于内核接口页的基址的地址提供。

ExternalFreq/InternalFreq 外部总线/内部处理器频率，单位kHz。

**内核描述部分**

*KernDescPtr* 指向包含4个内核版本字的区域（后面有说明）, 该区域后跟一些0终止的明文字符串。第一个明文字符串标识当前内核, 后跟进一步可选的内核特定版本信息。其余的明文字符串标识依赖内核功能的结构 (见附录3).零长度字符串 (即字符串仅包含一个字符0) 将终止功能说明的列表。KernelDescPtr 给出的是相对于内核接口页基址的地址。

 用于识别微内核。

 内核生成日期。

可用于识别微内核的版本。注意, 此内核版本不一定与 API 版本相关。

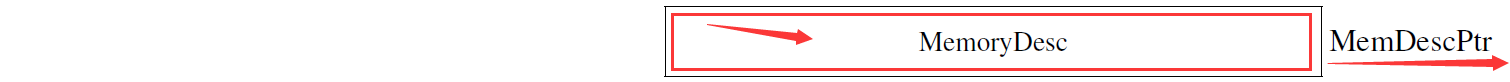
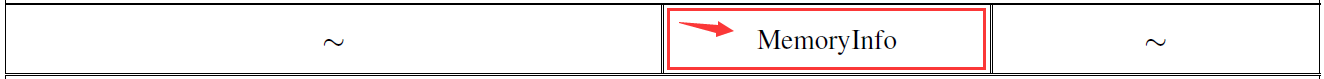
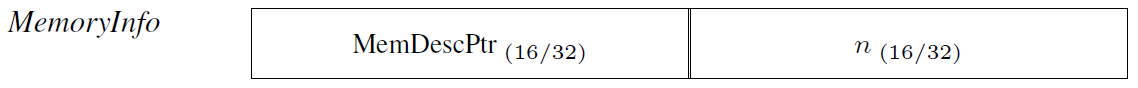
*Supplier* 以"供应商" 字段的四个最小有效字节指定标识内核供应商的字符串:

**系统调用链接**

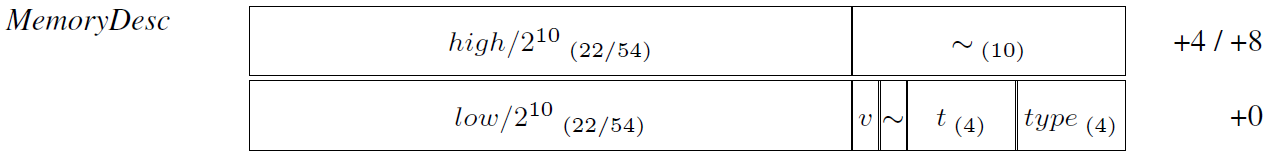
*SC* 一般系统调用。

*pSC* 特权系统调。例如, 只能由特权线程执行的系统调用

系统调用链接指定应用程序如何调用当前微内核的系统调用。系统调用链接的解释是 ABI 特定的, 但通常会根据内核接口页的基址来寻址,在那个地址内核提供了系统调用存根的位置。

**内存描述部分**

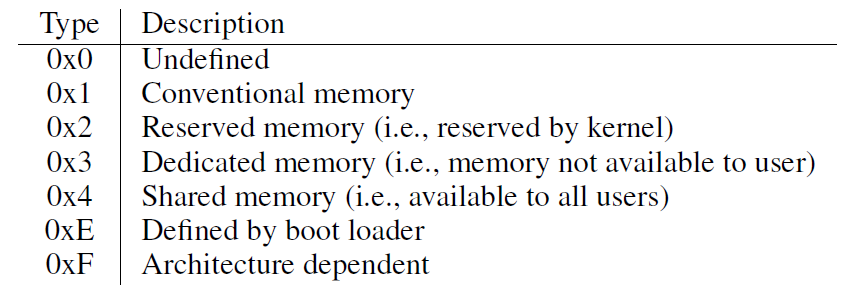
MemDescPtr 第一个内存描述符的位置(作为相对于内核接口页基址的偏移量)。后续内存描述符紧跟在第一个后面。对于指定重叠内存区域的存储描述符, 后面的描述符优先于较早的的。

n 内存描述符的数量。

high 内存区域中最后一个字节的地址。后十位地址位都是硬件置1。

low 内存区域中第一个字节的地址。后十位地址位都是硬件置0。

v 指示内存描述符是指物理内存 (v = 0) 还是虚拟内存 (v = 1)。

Type 标识内存描述符的类型：

*t,type=0xE*

内存描述符的类型依赖于引导程序。t 字段指定精确的语义。有关更多信息, 请参阅引导加载程序规范。

*t,type=0xF*

内存描述符的类型与体系结构相关。t 字段指定精确的语义。有关更多信息, 请参阅体系结构特定部件。

*t,type≠0xE, t,type≠0xE*

内存描述符的类型完全由type字段定义。t 字段的内容未定义。

1.2 KernelInterface [slow 系统调用]

该系统调用没有输入参数，返回的API version和API flags以及KernelId通过引用给形参赋值，函数的返回值是kernel interface page的基址。

函数形式**void\* KernelInterface（Word& ApiVersion，ApiFlags，KernelId）**

|  |  |
| --- | --- |
| 输入参数 | 输出 |
| 无 | void\* kernel interface page  Word ApiVersion  Word ApiFlags  Word KernelId |

各个形参的具体细节参看1.1节内容；便捷编程接口参看英文原版。

提供*kernel interface page, API version*和*API flags*的基址。后两个值是内核接口页中相应字段的副本。API 信息通过此系统调用使用寄存器传递(a) 以使在未来版本中的内核界面页面结构变化时候不受限制, (b) 能够确保内核的字节模式 (小/大) 和字宽 (32/64)的安全检测。

在第二页描述了kernel interface page。该页面是一个微内核对象。它通过微内核直接映射到地址空间创建时的每个地址空间。它不是由pager映射的, 不能映射或授予另一个地址空间, 也不能不要被取消映射。新地址空间的创建者可以指定必须映射内核接口页的地址。此地址将在该地址空间的生存期内保持不变。

任何线程都可以通过此系统调用确定内核接口页的地址。由于系统调用可能很慢, 因此极力建议将地址存储在静态变量中以供进一步使用。

对一个系统，还可以在所有地址空间中使用唯一一个内核接口页地址。然后, 在不使用当前系统调用的情况下, 可以通过固定绝对地址访问内核接口页。

除其他事项外, 该页还描述当前的 API、ABI 和微内核版本, 以便服务器或应用程序可以找出它是否以及如何在当前的微内核上运行。由于内核接口页还包含针对大多数其他系统调用的 API 和 ABI 特定的数据, 因此在使用其他系统调用之前通常需要该页的基址。

为了使版本检测能独立于 API 和 ABI,当前的系统调用在所有 L4 版本中都能正常工作。systemcall 的代码将永远不会更改, 并且在兼容处理器上将是相同的。(如果处理器向上兼容多个不兼容的处理器，内核应该为这个函数提供多个 systemcall 代码。)

针对KERNELINTERFACE系统调用衍生出来的其余内核接口，请查看英文原手册正文第 8 页。

1.3 虚拟寄存器 [虚拟寄存器]

虚拟寄存器由微内核实现。它们提供了一个快速接口, 用于在微内核和用户线程之间交换数据。虚拟寄存器是一个每个线程都拥有的静态对象。根据不同的特定的处理器类型, 它们可以映射到硬件寄存器或内存位置。也可以混合使用，即一部分虚拟寄存器映射到硬件寄存器，另一部分虚拟寄存器映射到内存上。 ABI 的虚拟寄存器访问取决于特定的处理器类型和虚拟寄存器类型, 更多硬件详细信息参看英文原版手册的附录。

一共有三种类型的虚拟寄存器：

* 线程控制寄存器（TCRs）
* 消息寄存器（MRs）
* 缓冲寄存器（BRs）

将非法值加载到虚拟寄存器、覆盖只读虚拟寄存器或访问在同一地址空间中的其他线程的虚拟寄存器是非法的(如果把虚拟寄存器映射到内存位置，这时候访问同一地址空间的中其他线程的虚拟寄存器是物理上可能的), 并且可能对当前地址空间的所有线程产生未定义的影响。然而, 因为虚拟寄存器不能跨地址空间访问, 它们从内核的角度来看是安全的：非法访问可以像任何其他编程 bug 一样只危害发端人的地址空间。

通常, 虚拟寄存器直接定位，而不能通过指针间接。

因此, 通用 API 不会提供任何的间接虚拟寄存器访问操作。然而，如果 ABI 允许, 处理器特定的代码生成器可能会使用间接访问技术。

针对虚拟寄存器的编程接口查看英文原手册正文第 11 页。

第二章 线程

2.1 ThreadId [数据类型]

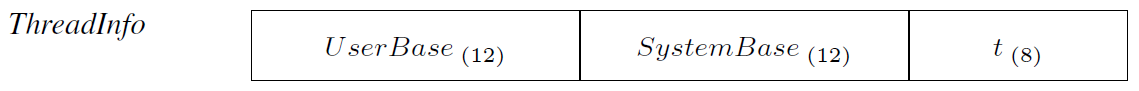
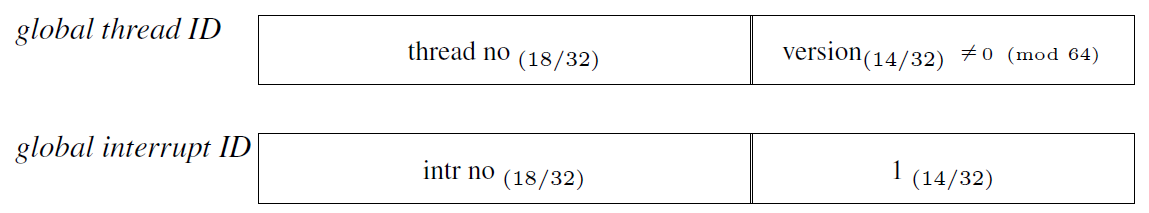
线程ID标识线程和硬件中断。线程 ID 可以是全局的或局部的。全局线程 ID在整个系统中是唯一的。它们独立于使用它们的地址空间来标识线程。每个地址空间都存在本地线程 ID；线程本地 ID 的范围仅作用于线程自己的地址空间。在不同地址空间, 相同的本地线程 ID 可以识别不同的和不相关的线程。

注意, 任何线程都有一个全局线程 ID。全局和本地线程 ID 都是以一个字节编码的。

**全局线程ID**

全局线程 ID 由一个字（32位机的字长是32位，64位机的字长是64位）组成,其中18 位 (32 位处理器) 或32位 (64 位处理器) 确定线程号，然后剩下的14位 (32 位处理器) 或32位 (64 位处理器) 可用于版本号。为了和局部ID区分开，表示版本号的字段的低6位中至少有一个必须是1。

用户线程编号可以在区间 [ UserBase，2t ) 内自由分配, 其中 t 表示线程 id 的上限。线程区间号 [ SystemBase，UserBase ) 是为L4内部线程保留的。硬件中断被视为硬件实现的线程。因此, 它们由线程 id 标识。它们对应的线程号在区间 [ 0, SystemBase ] 内。SystemBase、UserBase和 t 的值在内核接口页中。

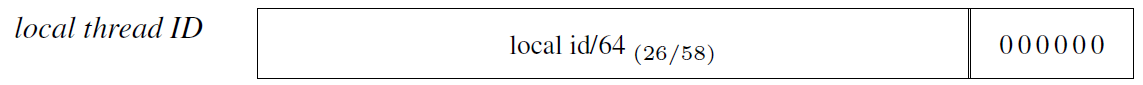


|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 0 | SystemBase | | UserBase | | 2t |
| 硬件中断 | | 内部线程 | | 用户线程 | |

全局线程 ID 具有一个版本字段, 其内容可以由那些可以创建和删除线程的线程自由设置。但是, 版本的低6位不能全部是 0, 即每一个版本值v都必须满足 v mod 64 ≠ 0。对于硬件中断，版本字段始终是1。

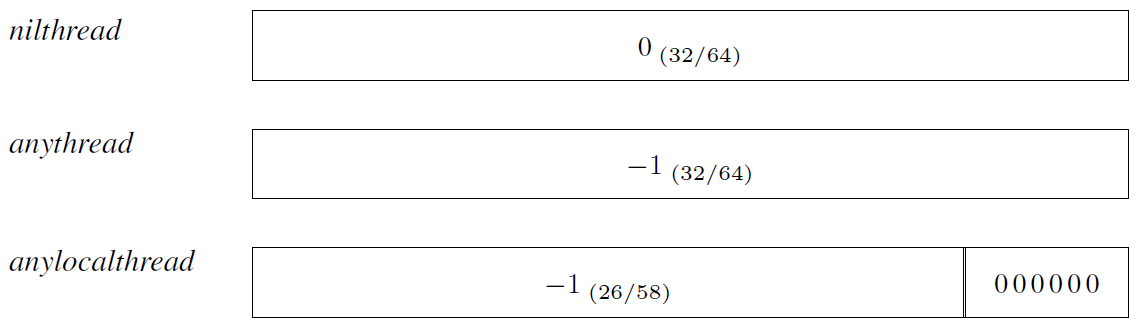
每当线程通过其全局线程 ID 访问时, 微内核就会检查版本字段。但是, 版本字段的语义不是由微内核定义的。操作系统的特性是自由使用这个字段用于任何用途。例如, 他们可以使用它来使线程 id 在时间上是唯一的。

**本地线程ID**

本地线程 ID 标识同一地址空间内的线程。通过设置线程ID最低6位都是0来标识本地线程。

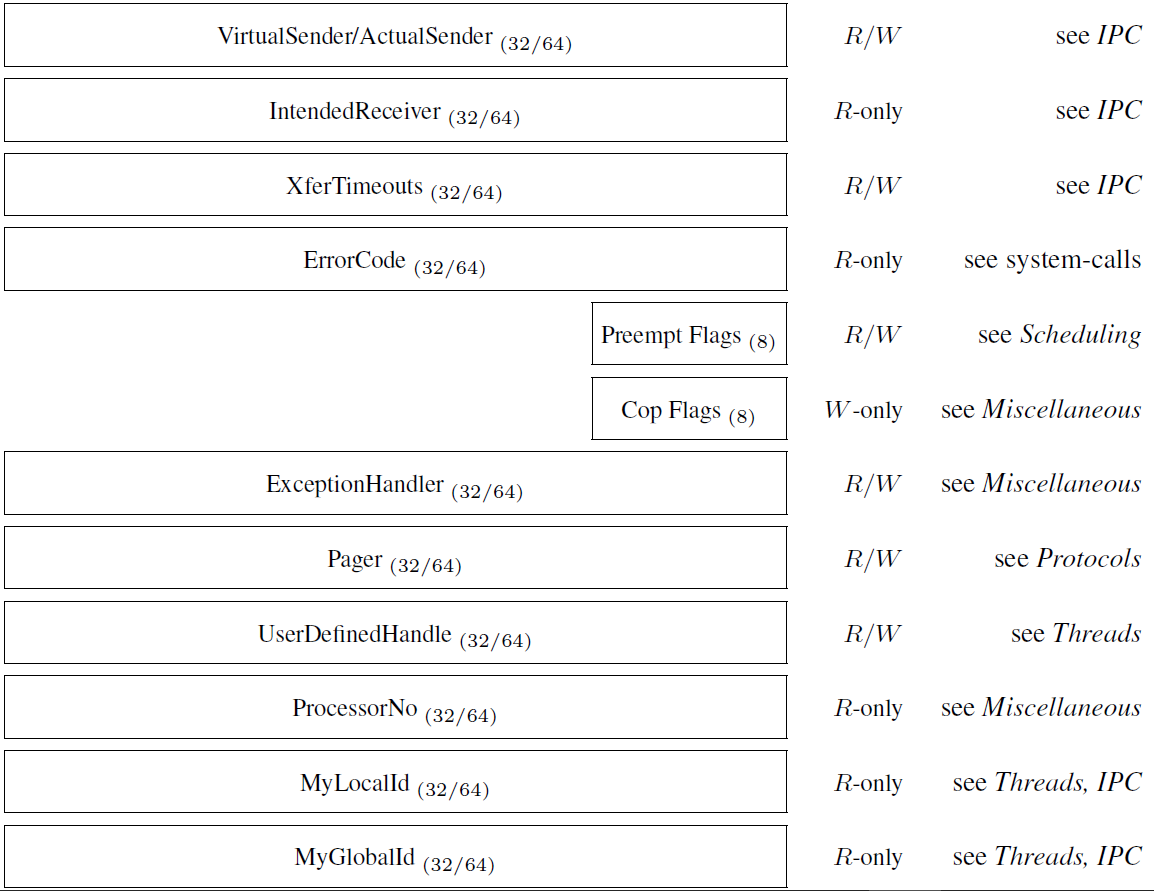
**特殊线程ID**

存在nilthread和两个通配符的特殊ID。线程ID：anythread，与任何给定线程ID匹配，包括所有的中断线程ID。线程ID：anylocalthread，匹配驻留在相同地址空间的所有线程。

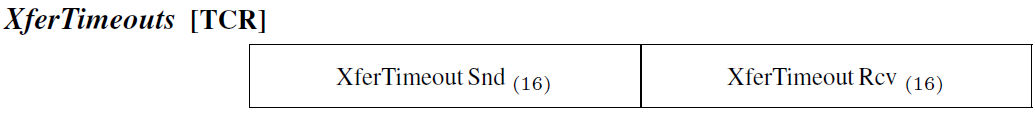
他们的格式如下：

针对线程ID的编程接口查看英文原手册正文第 15 页。

2.2 线程控制寄存器（TCRs） [虚拟寄存器]

TCRs是在用户线程和微内核之间交换相对静态控制信息的快速机制。TCRs是每个线程的静态非暂态寄存器。

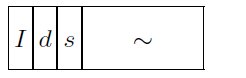
VirtualSender 当IPC阶段要发送的消息的消息头中的低16位控制位中的P字段等于1时候，表示该IPC是传输发送操作，而VirtualSender指定了发起者线程的ID。

IntendedReceiver 当一个IPC被标识为重定向IPC时候，该IPC被重定向到当前线程，并且IntendedReceiver这个字段用于指定应当接受消息的线程的ID。具体细节见IPC的msgtag部分。

在一个IPC中，一旦消息传输已经开始，传输消息的时间粗略地被发送者和接收者的XferTimeout的最小值所限制。 “粗略”意味着传输超时仅在发送者或接收者地址空间中的消息复制引起页面错误时才被检查。

每个线程有两个传输超时。一个用于发送阶段，一个用于接收阶段。具体细节见IPC部分。

ErrorCode



Preempt Flags

抢占标志，用于控制异步抢占。I标志位表示是否有异步抢占正在等待；s标志位控制异步抢占是否通知异常处理程序；d标志位控制抢占的发生方式，是所有抢占都立即响应还是基于优先级响应。具体细节见调度部分。

Cop Flags c0 ········ · · c7

协处理器标志，用于帮助内核优化某些硬件体系结构的线程切换。通过将ci位重置为0，一个线程告诉系统它不再需要协处理器i。 如果内核发现ci = 0，则得出结论：协处理器的寄存器和状态不必保存。 但是，内核确保协处理器不能用作不同地址空间之间的隐蔽通道。一旦一个线程复位了位ci，就必须将ci设置为1，然后才能在协处理器i上执行下一个操作。 否则，在使用协处理器寄存器和状态时可能会被任意修改。

请注意，ci位是只写的。 读取它们会导致一个未定义的值。 线程创建后，所有的ci位都被设置为1。有关Cop Flags的接口见6.2节。

ExceptionHandler 如果该字段不等于nilthread，指定异常处理程序线程。 当一个线程产生一个异常时，内核向线程的异常处理线程发送一个异常IPC消息，并等待来自包含指令指针的异常处理程序的响应，线程应该继续在MR1中执行；如果该字段等于nilthread，则线程没有指定异常处理程序，如果发生异常，则线程暂停，不再调度。

Pager 调页程序。也是一个进程，与其相关联的线程通信也是使用的MR寄存器。

MyGlobalId 线程的全局ID。

MyLocalId 线程的本地ID。

ProcessorNo 运行线程的处理器的编号。

UserDefineHandle 这个区域可以被用户线程随意设置和读取，比如用于存储线程号，存储附加线程控制块指针等等。

针对TCRs的编程接口查看英文原手册正文第 17 页。

2.3 ExchangeRegisters [系统调用]

函数形式 ThreadId ExchangeRegisters (ThreadId dest, Word control, sp, ip, flags, UserDefinedHandle, ThreadId pager, Word& old control, old sp, old ip, old flags, old UserDefinedHandle, ThreadId& old pager)

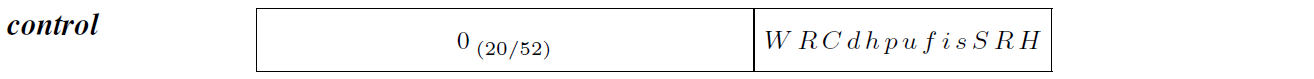
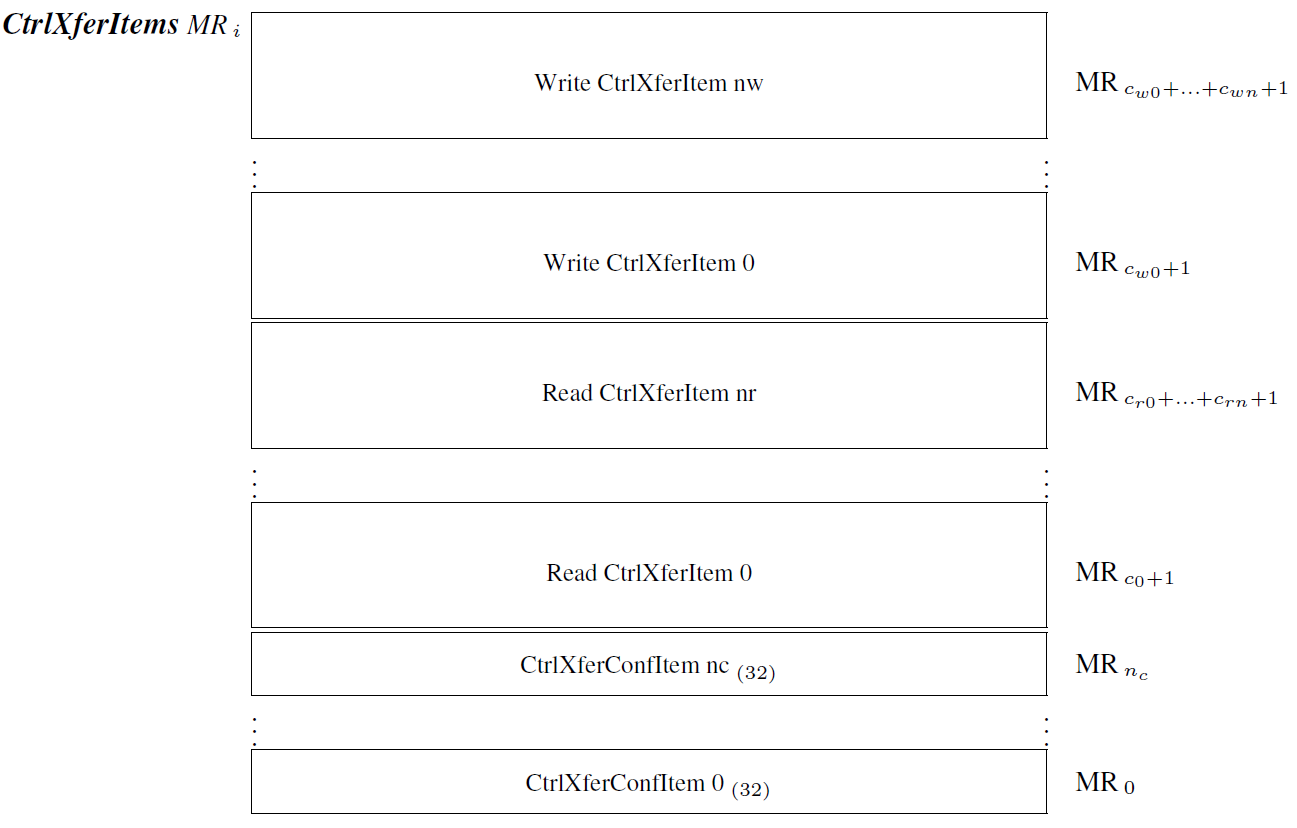
|  |  |
| --- | --- |
| 输入参数 | 输出 |
| ThreadId dest  Word control  Word SP  Word IP  Word FLAGS  ThreadId pager  Word UserDefinedHandle | ThreadId result  Word control  Word SP  Word IP  Word FLAGS  ThreadId pager  Word UserDefinedHandle |

该系统调用交换或读取线程的FLAGS，SP和IP硬件寄存器，以及调页程序和UserDefinedHandle TCR。而且，线程执行可以暂停或恢复。 目标线程必须是驻留在调用者地址空间中的活动线程。

任何IP，SP或FLAGS修改都会更改所寻址线程的相应用户级寄存器。一般来说，正在进行的内核活动不受影响。 但是，当前活动的IPC操作可以被取消或中止。有关详细信息，请参阅下面的SR位指定。

无论目标线程是以用户模式还是以内核模式执行，TCR中的调页程序（pager）字段和UserDefinedHandle字段的修改都会立即生效。

输入参数：

dest 被寻址线程的线程标识。这可能是本地或全局ID。但是，所指的线程必须驻留在当前地址空间中。在某些实现中使用本地线程ID可能会快得多。

W,R,C 就C标志位而言，针对内核生成消息，C标志位配置内核是否使用扩展控制传输协议。R和W标志允许使用控制传输项目直接读取和写入线程状态。所有控制转移项目（CtrlXferConfItem n）都被传递到调用线程的消息寄存器中。

 C = 1 调用者要求扩展状态在内核生成消息上发送。每一次错误发生，扩展状态位都要被指定，就像是控制传输配置项目CtrlXferConfItem一样。这些项目是从MR0开始。

fault 内核消息生成的错误的体系结构特定标识符。

idmask 指定发送消息时要包含的控制转移项目的位掩码。标识符是结构特定的。如果掩码中的位n被设置为1，则内核将把编号为n的CtrlXferItem附加到消息上。请注意，内核不保证为一个特定的CtrlXferItem选择单个寄存器不被允许; 相反，总是包含特定项目的全部内容。

C 每一个消息寄存器MRi中的最后一位C，是连续标志，除了最后一个CtrlXferItem外都被设置。

R = 1 调用者请求扩展状态从目标线程读取。 扩展状态作为一组控制传输项目在调用者的消息寄存器中传递。 如果C = 1，则要读取的第一个CtrlXferItem紧跟在最后一个CtrlXferConfItem之后。 如果C = 0，则读取项目从MR0开始。连续标志c被置位，除最后一个CtrlXferConfItem之外。注意，每次读取CtrlXferConfItem的时候，都必须提供足够的空间足以涵盖要读取的项目中的所有寄存器（即，如果项目的掩码指定要读取的寄存器有k个，则该项目的大小必须包含至少k个寄存器的字）。

W = 1 调用者请求扩展状态从目标线程写入。 扩展状态作为一组控制传输项目在调用者的消息寄存器中传递。 如果R = 1，则要写的第一个CtrlXferItem紧跟在最后一个读项目之后。否则如果C = 1，则第一个写项目紧跟在最后一个CtrlXferConfItem之后。否则如果C = 0，从MR0开始写。连续标志c被置位，除最后一个CtrlXferConfItem之外。

d 如果d = 0，返回结果是未定义；

如果d = 1，返回结果会提供调用该系统调用之前的各个参数所对应的值。

注意：不论d = 0还是1，与系统调用是否正确执行没有关系，d只决定是否返回旧值。

h p u f i s s表示SP寄存器；i表示IP寄存器；f表示FLAGS寄存器；u表示线程控制寄存器（TCR）的UserDefinedHandle字段；p表示TCR的调页函数（pager）字段；h指的是后文提到的H标志位。如果一个标志位被置1，那么他所对应的寄存器或者状态位就会被输入参数重写。否则的话忽略输入参数，并且所对应的寄存器或者是状态位不被修改。

SR 控制是否通过系统调用取消/中止所寻址的线程正在进行的IPC操作。

S = 0 所寻址的线程的，正在等待发送消息的IPC操作或者是正在发送消息的IPC操作会跟之前一样继续进行。SP、IP或标志修改将延迟到IPC操作终止。

S = 1 所寻址线程的正在等待发送消息的IPC操作会被取消；当前正在发送消息的IPC操作会被中止。

R = 0 所寻址的线程的，正在等待接收消息的IPC操作或者是正在接收消息的IPC操作会跟之前一样继续进行。SP、IP或标志修改将延迟到IPC操作终止。

R = 1 所寻址线程的正在等待接收消息的IPC操作会被取消；当前正在接收消息的IPC操作会被中止。

H 如果H = 1，则暂停/恢复线程；如果 H = 0，则忽略。

H = 0 如果线程没有停止，则没有影响。否则，线程执行将恢复。

H = 1 用户级线程执行被暂停。注意，正在进行的IPC和其他内核操作不受H的影响。

SP 如果输入参数control中的s标志位是1，那么当前用户级堆栈指针会被设置成该输入参数SP。如果s标志位是0，则忽略该参数。

IP 如果输入参数control中的i标志位是1，那么当前用户级指令寄存器指针会被设置成该输入参数IP。如果i标志位是0，则忽略该参数。

FLAGS 如果输入参数control中的f标志位是1，那么根据该参数来设置线程的用户级处理器标志。如果i标志位是0，则忽略该参数。FLAGS的语义取决于处理器类型。

UserDefinedHandle 如果输入参数control中的u标志位是1，那么根据该参数来设置线程TCR中的UserDefinedHandle字段。如果u标志位是0，则忽略该参数。

pager 如果输入参数control中的p标志位是1，那么根据该参数来设置线程TCR中的pager字段。如果p标志位是0，则忽略该参数。

输出参数：

result ≠ nilthread，并且输入参数dest是一个局部线程ID

被寻址的是全局线程ID，ExchangeRegisters系统调用成功。

result ≠ nilthread，并且输入参数dest是一个全局线程ID

被寻址的是局部线程ID，ExchangeRegisters系统调用成功。

result = nilthread

操作失败。TCR中的ErrorCode字段会表明出错原因。

ErrorCode

如果result = nilthread，则会被设置；否则如果result ≠ nilthread，则该字段未定义；

= 2，无效线程。dest参数指定了一个无效的线程ID、未活动的线程ID或者是指定了一个不在同一地址空间的线程。

该参数只有在输入参数的control参数d字段等于1的时候才是有效的，其他情况下都是未定义。

H 报告当ExchangeRegisters系统调用被调用的时候所寻址的线程是否是停止了。注意，这个输出参数control的H位是独立于输入参数control。

SR 报告当ExchangeRegisters系统调用被调用的时候所寻址的线程是否正在进行一个IPC操作。该字段的值为0表示所寻址线程没有在发送阶段或者是接收阶段。同样的，这个输出参数control的SR位是独立于输入参数control。

R = 1 当寻址线程位于IPC操作的接收阶段时，执行操作。如果输入参数control的R = 1，IPC操作被取消或中止。

S = 1 当寻址线程位于IPC操作的发送阶段时，执行操作。如果输入参数control的S = 1，IPC操作被取消或中止。

SP 如果输入参数control中的d字段等于1，则该参数的值是原来线程未调用ExchangeRegisters系统调用之前的SP寄存器的值，如果d等于0，输出参数SP的值未定义。

IP 如果输入参数control中的d字段等于1，则该参数的值是原来线程未调用ExchangeRegisters系统调用之前的IP寄存器的值，如果d等于0，输出参数IP的值未定义。

FLAGS 如果输入参数control中的d字段等于1，则该参数的值是原来线程未调用ExchangeRegisters系统调用之前的FLAGS寄存器的值，如果d等于0，输出参数FLAGS的值未定义。FLAGS的语义是处理器特定的。

UserDefinedHandle

如果输入参数control中的d字段等于1，则该参数的值是原来线程未调用ExchangeRegisters系统调用之前寻址线程TCR中UserDefinedHandle字段的值，如果d等于0，该参数的值未定义。

pager 如果输入参数control中的d字段等于1，则该参数的值是原来线程未调用ExchangeRegisters系统调用之前寻址线程TCR中pager字段的值，如果d等于0，该参数的值未定义。

针对ExchangeRegisters的编程接口查看英文原手册正文第 21 页。

2.4 ThreadControl [特权系统调用]

函数形式：Word ThreadControl (ThreadId dest, SpaceSpecifier, Scheduler, Pager, void\* UtcbLocation)

|  |  |
| --- | --- |
| 输入参数 | 输出 |
| ThreadId dest  ThreadId SpaceSpecifier  ThreadId scheduler  ThreadId pager  void\* UtcbLocation | Word result |

特权线程（例如根服务）可以通过此功能删除和创建线程。它还可以修改现有线程的全局线程ID（仅限版本字段）。

线程可以创建为活动或非活动的线程。非活动线程不运行，但可以由在相同地址空间中运行的活动线程激活。

主动创建的线程立即启动，方法是通过执行其调页程序的短接收操作。（一个活动线程必须有一个调页程序。）激活的线程期望从其调页程序获得启动消息（MsgTag和两个无类型的字）。一旦接收到启动消息，它将MR 1的值作为其新的IP，MR 2的值作为其新的SP，然后用这接收到的IP和SP在用户级开始执行线程。新的线程将在与调用了ThreadControl系统调用的处理器上运行。

中断线程被视为正常的线程。它们在系统启动时处于活动状态，不能删除或迁移到不同的地址空间（即，SpaceSpecifier必须等于中断线程ID）。当发生中断时，中断线程发送一个IPC到其调页程序，并等待空的中断结束确认消息（MR0 = 0）。中断线程永远不会引起页面错误。为了停用中断消息传送，调页程序被设置为中断线程自己的ID。

输入参数：

dest 寻址线程。必须是全局线程id。只有线程号才能有效地用于寻址线程。如果存在具有与dest指定线程号相同的线程，则其版本位将被dest id的版本位覆盖，并且任何正在进行的IPC操作都将被中止。否则，指定的版本位用于线程创建，即线程创建会生成一个id为dest的线程。

SpaceSpecifier≠nilthread，dest不存在

创建新的线程。SpaceSpecifier指定线程将驻留在哪个地址空间中。由于地址空间没有自己的ID，因此使用线程ID作为SpaceSpecifier。 其含义是：新线程应该在与线程SpaceSpecifier相同的地址空间中执行。

新地址空间中的第一个线程是使用SpaceSpecifier = dest创建的。 这个操作隐含地创建一个新的空的地址空间。注意，新地址空间是使用空的UTCB和KIP区域创建的。因此，在执行线程之前，必须通过SpaceControl操作来完成空间创建。

SpaceSpecifier≠nilthread，dest存在

只修改。被寻址的线程dest既不被删除也不被创建。可以修改寻址线程的版本字段，相关调度器，调页程序或相关地址空间。如，将线程迁移到新的地址空间。

SpaceSpecifier = nilthread，dest存在

删除。 被寻址的线程dest被删除。删除地址空间的最后一个线程也会隐式删除地址空间。

scheduler≠nilthread

定义允许调度被寻址线程的调度程序线程。注意，在被寻址线程开始执行时，调度程序线程必须存在。

Scheduler = nilthread

当前调度程序关联不被修改。ThreadControl在执行创建操作时，这种变体是非法的。

pager≠nilthread

dest所指线程的pager被设置为pager参数指定的线程。如果dest之前是非活动的，那么就激活它。

Pager = nilthread

当前的pager关联不被修改。

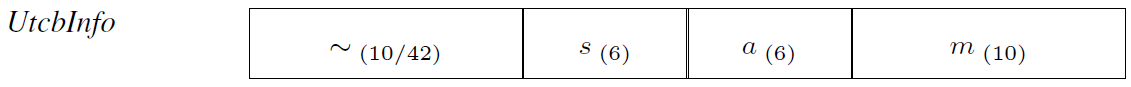
如果执行的是ThreadControl的创建线程操作，dest会被创建成一个非活动的线程。

UtcbLocation≠-1

线程UTCB的起始地址被设置为UtcbLocation。线程激活时，UTCB必须完全适合配置的地址空间的UTCB区域，并且必须根据内核接口页面的UtcbInfo字段正确对齐。确保多个线程的UTCB不重叠是应用程序的责任。更改已经激活的线程的UtcbLocation是非法的操作。注意，由于新创建的空间具有空的UTCB区域，因此无法在未使用SpaceControl正确配置的地址空间中激活线程。

UtcbLocation = -1

UTCB的位置不变。



s 地址空间中的 UTCB 区域的最小大小是2s。UTCB 区域的大小限制了线程的总数量 k ,且满足式子2a mk ≤ 2s.

m UTCB大小的乘数。

a UTCB 位置必须与2a对齐。一个 UTCB 所需的总大小是2am

输出参数：

result 如果操作成功，则结果为1，否则结果为0，并且TCR中的ErrorCode 指示失败原因。

ErrorCode

如果result = 1则是未定义，result = 0的时候才被设置。

= 1 没有特权。 当前线程没有执行操作的权限。

= 2 无法使用的线程。 dest参数指定了内核线程或不可用的中断线程。

= 3 无效的空间。 SpaceSpecifier参数指定了一个无效的线程ID，或者激活尚未初始化的空间中的线程。

= 4 无效的调度程序。 调度程序参数指定了无效的线程ID，或者设置为nilthrad来创建THREADCONTROL操作。

= 6 无效的UTCB位置。 UtcbLocation位于UTCB区域之外，或者尝试更改已经激活的线程的UtcbLocation。

= 8 内存不足。 内核无法分配执行操作所需的资源。

针对ThreadControl的编程接口查看英文原手册正文第 25 页。

第三章 调度