2

Windows 系统总述

这一章首先讲述 Windows 系统的基本结构。作为一个典型的现代操作系统，Windows 有着广泛的用户群体，并且自诞生以来就一直备受关注。在讲述了 Windows 基本结构以后，本章将简要地介绍 WRK（Windows Research Kernel），这是 Microsoft 提供的一套可以编译和运行的 Windows 内核源代码，本书后面章节的绝大多数讲解都将参考 WRK 中的源代码。

本章也将介绍 Windows 系统中的基本概念以及 Windows 内核中的一些公共管理设施，这些知识不仅有助于读者全面认识 Windows 操作系统，而且也便于本书后面的章节直接引用 Windows 内核中的概念和管理机制。最后，本章还将介绍 Windows 的引导过程。从系统启动一直到内核能够正常工作，再到用户登录到系统中，Windows 系统中的各个组件都要完成相应的初始化任务。

2.1 现代操作系统的基本结构

操作系统本身属于软件的范畴，但是它需要紧密地跟硬件打交道，它为上层应用软件或应用系统提供了一层抽象，专门负责硬件资源的管理和分配。应用软件不需要直接跟硬件打交道，它们利用操作系统提供的功能来实现各种应用任务，如果它们要访问硬件，则必须通过操作系统提供的抽象接口来完成。图 2.1 显示了现代操作系统的一般性框架结构。

图 2.1 中的模型可能会有一些变化形式，比如，有些专用机器的系统并没有提供内核扩展性能，所有的硬件驱动模块都链接在系统内核中。但通用机器的系统倾向于提供可动态加载的驱动程序或专门的扩展接口，Windows 和 Linux 就是这类系统的典型代表。另外，在系统服务层之上，应用软件通过一层接口来调用系统提供的服务，而应用程序之间则保

持相对隔离，它们相互间的通信需要通过系统来完成。操作系统提供了一些基本的 IPC（Inter-Process Communication，进程间通信）原语来支持上层应用程序之间的交互操作。系统内核负责管理这些应用程序，把有限的计算资源分配给它们，使它们的任务得以完成。例如，计算机的处理器（即 CPU）、内存和外存（如硬盘）由系统内核统一管理和分配，因而多个应用软件可以同时运行在一个系统中，它们既可能毫不相关，也可能相互依赖，操作系统会协调它们的运行过程。

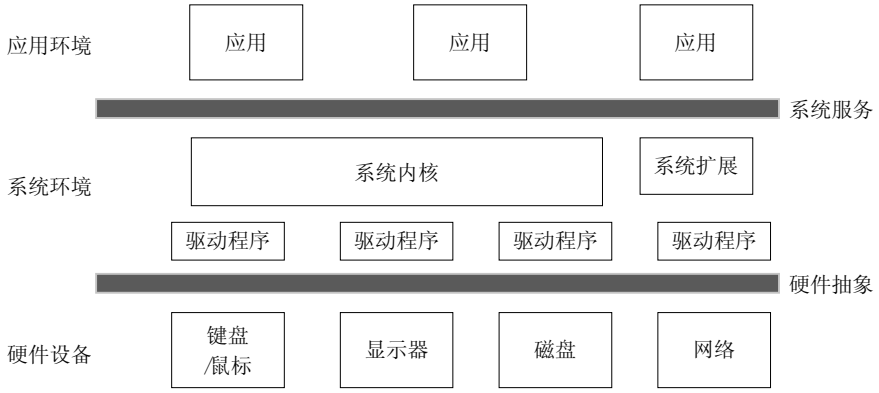


图 2.1 现代操作系统的基本结构

硬件设备，像键盘、显示器、磁盘、打印机和网络等，则通过各自的驱动程序，以一致的方式交由操作系统来处理。系统内核接受应用程序的请求，与硬件设备进行通信；另一方面，硬件设备向计算机发送信号，驱动程序收到信号后，与系统内核一起把信号传递给恰当的应用程序。对于通用的操作系统，为众多外部设备提供支持是系统执行环境的一个重要方面。为了灵活、方便起见，驱动程序往往是可替换或可升级的，它们构成了系统执行环境的一个重要组成部分，在代码量方面甚至超过了系统内核本身。

在现代计算机系统中，仅仅简单地支持外部设备往往还不够，设备的即插即用（plug-and-play）和电源管理越显重要。这一方面要求系统总线能够检测到设备的插入和拔除，另一方面也要求操作系统能够动态地加载或移除驱动程序，同时保持系统状态的完整性。电源管理不仅会影响到操作系统自身的状态管理，也需要获得驱动程序和硬件设备的支持，所以，电源管理自然成了设备驱动程序接口的一部分。

2.2 Windows 系统结构

上一章已经提到，Windows 内核（由于是从 Windows NT 发展起来的，也称为 NT 内核）从一开始就有良好的设计，其结构具备很好的可扩展性和安全性。所以，Windows

内核在 20 年的发展历程中一直能够很好地适应硬件的发展，在 Windows 操作系统的各个版本中并没有根本性的变化。这一节将介绍 Windows 操作系统的基本框架，这些内容完全适用于 Windows XP/Server 2003 及以后的版本。

图 2.2 显示了 Windows 基本结构。Windows 采用了双模式（dual mode）结构来保护操作系统本身，以避免被应用程序的错误所波及。操作系统核心运行在内核模式（kernel mode）下，应用程序的代码运行在用户模式（user mode）下。每当应用程序需要用到系统内核或内核的扩展模块（内核驱动程序）所提供的服务时，应用程序通过硬件指令从用户模式切换到内核模式中；当系统内核完成了所请求的服务以后，控制权又回到用户模式代码。

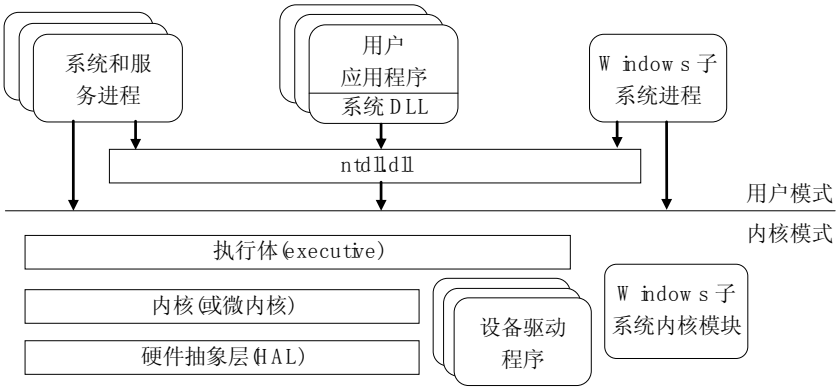


图 2.2 Windows 系统结构图

在 Windows 中，用户代码和内核代码有各自的运行环境，而且它们可以访问的内存空间也并不相同。在 32 位系统中，内核代码可以访问当前进程的整个 4 GB 虚拟地址空间，而用户代码只能访问底端的 2 GB 虚拟地址（或 3 GB，如果打开了内核启动开关/3 GB 的话）。

Windows 子系统是 Windows 系统中一个不可缺少的组成部分，它与系统内核一起构成了用户应用程序的执行环境。Windows 的原始设计是一个支持多环境子系统的操作系统，除了 Windows 子系统作为它的原生环境子系统，它还支持 POSIX 和 OS/2 环境子系统，为 UNIX 类应用程序和 OS/2 应用程序提供一个仿真执行环境。随着 Windows 操作系统的发展，自 Windows XP 以后，只有 Windows 子系统随系统一起发行。Windows 子系统既有内核模式部分（图形和窗口管理），也有用户模式部分。用户模式部分包括一个单独的子系统进程和一组链接到各个应用进程中的系统 DLL。

Windows 操作系统还包括一组系统进程和服务进程，它们为操作系统提供了关键的服务，比如会话管理、用户登录和注销、身份验证，以及打印服务、事件日志和任务调度等。这些系统进程和服务进程也是整个操作系统运行环境的一部分。

2.2.1 Windows 内核结构

正如图 2.2 所示，Windows 内核分为三层，与硬件直接打交道的这一层称为硬件抽象层（Hardware Abstraction Layer，简称 HAL），这一层的用意是把所有与硬件相关联的代码逻辑隔离到一个专门的模块中，从而使上面的层次尽可能做到独立于硬件平台。HAL 之上是内核层，有时候也称为微内核（micro-kernel），这一层包含了基本的操作系统原语和功能，如线程和进程、线程调度、中断和异常的处理、同步对象和各种同步机制。在内核层之上则是执行体（executive）层，这一层的目的是提供一些可供上层应用程序或内核驱动程序直接调用的功能和语义。Windows 内核的执行体包含一个对象管理器，用于一致地管理执行体中的对象。执行体层和内核层位于同一个二进制模块中，即内核基本模块，其名称为 ntoskrnl.exe。

内核层和执行体层的分工是，内核层实现操作系统的基本机制，而所有的策略决定则留给执行体。执行体中的对象绝大多数封装了一个或者多个内核对象，并且通过某种方式（比如对象句柄）暴露给应用程序。这种设计体现了机制与策略分离的思想。图 2.3 显示了 Windows 内核的详细组成结构。

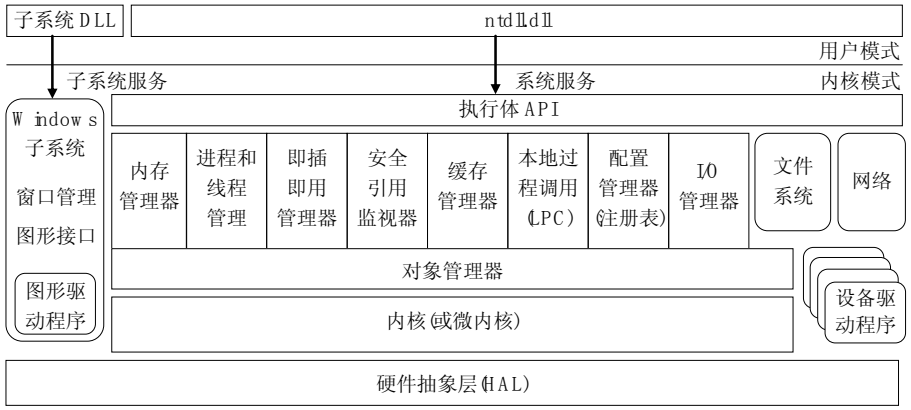


图 2.3 Windows 内核的组成结构

Windows 内核为用户模式代码提供了一组系统服务，供应用程序使用内核中的功能。应用程序通常并不直接调用这些系统服务，而是通过一组系统 DLL，最终通过 ntdll.dll 切换到内核模式下的执行体 API 函数中，以调用内核中的系统服务。Ntdll.dll 是连接用户模式代码和内核模式系统服务的桥梁。对于内核提供的每一个系统服务，该 DLL 都提供一个相应的存根函数，这些存根函数的名称以“Nt”作为前缀，例如 NtCreateProcess、NtOpenFile 和 NtSetTimer。另外，ntdll.dll 还提供了许多系统级的支持函数，比如映像加载器函数（以“Ldr”为前缀）、Windows 子系统进程通信函数（以“Csr”为前缀）、调试函数（以“Dbg”

为前缀）、系统事件函数（以“Etw”为前缀），以及一般的运行支持函数（以“Rtl”为前缀）和字符串支持函数等。

执行体 API 函数接收的参数来自于各种应用程序，因此，为了确保系统的健壮性，以及抵抗来自用户模式的恶意攻击，所有的执行体 API 函数必须保证参数的有效性。这意味着它们必须在恰当的时刻检查参数的值，若是指针的话，还必须保证调用者可以访问指针所指的内存。通常，执行体系统服务函数会在其开始处，对所接收的参数逐一探查它们的可访问性。例如，以下代码就演示了这一做法：

```
PreviousMode = KeGetPreviousMode();
if (PreviousMode != KernelMode) {
  try {
    ProbeForWrite(InputInformation,
        InputInformationLength,
        sizeof(ULONG));
    if (ARGUMENT_PRESENT(ReturnLength)) {
      ProbeForWriteUlong(ReturnLength);
    }
  } except(EXCEPTION_EXECUTE_HANDLER) {
    return GetExceptionCode();
  }
}
```

这里 InputInformation 和 ReturnLength 是该系统服务的直接参数，InputInformation 是个指针参数，它的可用长度由另一个参数 InputInformationLength 来指定，因此，这段代码通过 ProbeForWrite 来探查这一输入数据是否可写；另外，ReturnLength 是一个 ULONG 类型的输出参数，这段代码通过 ProbeForWriteUlong 来验证该参数是否可写。一旦探查函数发生访问违例，则说明这两个参数有问题，于是该系统服务就将直接返回违例异常代码。

正如前文所述，用户模式和内核模式代码所能访问的地址空间有所不同。在 32 位系统上，用户模式代码只能访问 2 GB 以下的虚拟内存地址空间，而内核模式代码可以访问当前进程整个 4 GB 虚拟地址范围。2 GB 以下称为进程地址空间，2 GB 以上称为系统地址空间。实际上，在两者之间有一块特殊的 64 KB 地址空间，位于 0x7fff0000—0x7fffffff，在两种模式下都不可访问。上述代码片段中的 ProbeForWrite<*Xxx*>函数首先检查目标内存地址是否越过了此特殊区域，若越过则访问违例；然后，试图将目标地址处的值赋回该地址，即触发一次该地址处的读和写操作，若该内存地址处当前线程不可写，则引发异常，从而使代码片段中的 except 子句截获控制。Windows 通过这种方法来捕捉到“用户模式代码传递一个系统空间地址”或者“传递一个无效内存地址”的情形，从而确保执行体函数接收到的参数已被检验过。

然而，执行体 API 函数并不总是要检验参数的有效性，如果在调用该 API 函数以前的模式是内核模式，那么，它不需要检验参数的有效性。执行体不会用坏的参数来调用它

自己的服务，只有当执行体 API 函数接收到一个或多个来自用户模式的参数时，它才使用 Probe 函数族检查参数的有效性。每个线程都维护着一个状态值，用以说明它以前的处理器模式。当从用户模式切换到内核模式时，该值将被设置为 UserMode，从而满足上述代码中的 if 条件。

2.2.2 Windows 内核中的关键组件

Windows 操作系统虽然算不上真正意义上的微内核结构，但是它的内核部分有良好的设计以及清晰的模块结构，如前面图 2.3 所示。现在我们来逐一介绍内核部分的各个关键组件，不过 Windows 子系统部分将留到下一小节单独讲述。

HAL（硬件抽象层）

HAL 的设计目的是将硬件的差别隐藏起来，从而为操作系统的上层提供一个抽象的、一致的硬件资源模型，以使 Windows 更容易被移植到不同的硬件平台上。理想的情形是，只要硬件厂商能够提供一个 HAL，Windows 就能够在相应的硬件平台上运行。因此，HAL 使得上层的模块无须考虑硬件的差异，它们通过 HAL 而不是直接访问硬件。

在 Windows 中，HAL 是一个独立的动态链接库。尽管 Windows 随带了多个主流机器的 HAL，但是在系统安装的时候只有一个会被选中，并拷贝和改名为 hal.dll。HAL 提供了一些例程供其他内核模块或设备驱动程序调用，这使得一个驱动程序可以支持同样的设备在各种硬件平台上运行。HAL 不仅涵盖了处理器的体系结构，也涉及了中断控制器、单处理器或多处理器等硬件条件。表 2.1 列出了在 Intel x86 机器上 Windows Server 2003 系统中随带的 HAL。

表 2.1 Windows Server 2003 的 HAL 列表（Intel x86 处理器）

HAL 文件	所支持的硬件系统
Hal.dll	³ y PC
Halacpi.dll	ACPI :‰ " ä (W Ç PC
Halapic.dll	APIC :‰ ¶ © Q / n Å % v PC
Halaacpi.dll	APIC ACPI PC
Halmps.dll	• ‰ 8 v PC
Halmacpi.dll	• ‰ 8 v ACPI PC

内核（或微内核）

这是大内核中的小内核，将其称为微内核更可以说明它在整个内核模式代码中的地

位。它是内核模块 ntoskrnl.exe 中的下层部分（上层部分为执行体），最接近于 HAL 层，负责线程调度和中断、异常的处理。对于多处理器系统，它还负责同步处理器之间的行为，以优化系统的性能。这一层的核心任务是，让系统中的所有处理器尽可能地忙和高效。内核层可在多个处理器上并发执行，它的代码以 C 语言为主，也包含一部分汇编代码。

Windows 的内核实现了抢占式线程调度机制，按照优先级顺序将线程分配到处理器上，并且允许高优先级的线程中断或抢占低优先级的线程。每个处理器上的线程切换也是由内核来完成，它按照调度规则让处理器放弃当前线程，选择下一个要执行的线程。每个线程有一个基本优先级值（base priority），这是由程序在创建线程时指定的；每个线程还有一个动态优先级值，这是在线程执行过程中根据各种条件在基本优先级基础上由内核来调整的，目的是让系统更快地响应用户的动作，以及在系统服务和其他低优先级进程之间平衡处理器资源的分配。

Windows 的内核按照面向对象的思想来设计，它管理两种类型的对象：分发器对象（dispatcher object）和控制对象。分发器对象实现了各种同步功能，这些对象的状态会影响线程的调度。Windows 内核实现的分发器对象包括事件（event）、突变体（mutant）、信号量（semaphore）、进程（process）、线程（thread）、队列（queue）、门（gate）和定时器（timer）。控制对象被用于控制内核的操作，但是不影响线程的调度，它包括异步过程调用（APC）、延迟过程调用（DPC），以及中断对象等。

内核层位于 HAL 之上，但鉴于内核所提供功能与硬件体系结构的紧密关联性，它不可避免地需要引入一些与体系结构相关的代码，例如，在切换线程时，保存和恢复线程的执行环境取决于处理器体系结构。不过，如何选择下一个线程，这是与体系结构无关的。内核有义务将 Windows 所支持的各种硬件体系结构进行抽象，使得体系结构的差异对 Windows 代码的影响尽可能地小，并且有些功能可以通过 HAL 来完成，毕竟 HAL 才是真正的硬件抽象层。例如自旋锁和中断的功能是在 HAL 中实现的，内核只需简单地使用 HAL 的导出函数即可。

执行体

执行体是内核模块 ntoskrnl.exe 的上层部分，它包含 5 种类型的函数：

- 被导出的、可在用户模式下调用的函数。对这些函数的调用接口位于 ntdll.dll 模块中。应用程序通过 Windows API 来间接地调用这些函数。
- 虽已被导出并且可在用户模式下调用，但无法通过任何一个 Windows API 来调用的函数。这样的例子包括 LPC（Local Procedure Call，本地过程调用）函数、各种查询

函数（如 NtQueryInformation<*Xxx*>），以及一些专用的函数，比如 NtCreatePagingFile 等。对这些函数的调用需要直接链接 ntdll.dll 来完成。

- 只能在内核模式下调用的导出函数，并且在 Windows DDK 中有关于这些函数的文档。这些函数可以被设备驱动程序调用。
- 供执行体组件之间相互调用，但未被文档化的函数。这包括执行体内部使用的一组支持函数。
- 属于一个组件的内部函数。

以上提到的组件是指执行体内部的组件，从大的方面来看，执行体包含以下组件（参考图 2.3）：

- 进程和线程管理器。负责创建进程和线程，以及终止进程和线程。在 Windows 中，对于进程和线程的底层支持是在内核层提供的，执行体在内核层的进程和线程对象的基础上，又提供了一些语义和功能。
- 内存管理器。此组件实现了虚拟内存管理，既负责系统地址空间的内存管理，又为每个进程提供了一个私有的地址空间，并且也支持进程之间内存共享。内存管理器也为缓存管理器提供了底层支持。
- 安全引用监视器（SRM，Security Reference Monitor）。该组件强制在本地计算机上实施安全策略，它守护着操作系统的资源，执行对象的保护和审计。
- I/O 管理器。它实现了与设备无关的输入和输出功能，负责将 I/O 请求分发给正确的设备驱动程序以便进一步处理。
- 缓存管理器。它为文件系统提供了统一的数据缓存支持，允许文件系统驱动程序将磁盘上的数据映射到内存中，并通过内存管理器来协调物理内存的分配。
- 配置管理器。它负责系统注册表的实现和管理。
- 即插即用管理器。它负责列举设备，并为每个列举到的设备确定哪些驱动程序是必需的，然后加载并初始化这些驱动程序。当它检测到系统中的设备变化（增加或移除设备）时，负责发送恰当的事件通知。
- 电源管理器。它负责协调电源事件，向设备驱动程序发送电源 I/O 通知。当系统电源状态变化时，通知设备驱动程序处理设备的电源状态。即插即用设备的管理和电源的管理也可以看做是 I/O 管理器的扩展功能。

此外，执行体还包含 4 组主要的支持函数，供以上这些执行体组件调用。差不多有 1/3 的支持函数可以在 Windows DDK 中找到相应的文档，因为设备驱动程序也要调用它们。这 4 类支持函数如下所列：

- 对象管理器。它负责创建、管理和删除 Windows 执行体对象，以及用于表达操作系统资源的抽象数据类型，比如进程、线程和各种同步对象。
- LPC 设施。LPC 设施负责在同一台机器上的客户进程和服务器进程之间传递消息。LPC 是 RPC（Remote Procedure Call，远程过程调用，关于网络上客户进程和服务器进程之间通信的工业标准）的一个优化版本。
- 一组运行时库函数。其功能广泛，涵盖字符串处理、算术运算、数据类型转换以及安全结构处理等。
- 执行体支持例程。例如系统内存分配（换页内存池和非换页内存池）、互锁的内存访问，以及对两种特殊类型同步对象（资源和互斥体）的支持。

设备驱动程序

在内核中除了内核模块 ntoskrnl.exe 和 HAL 以外，其他的模块几乎都以设备驱动程序的形式存在。Windows 操作系统中的设备驱动程序，并不一定对应于物理设备；驱动程序既可以创建虚拟设备，也可以完全与设备无关，而仅仅是内核的扩展模块。从软件结构角度而言，我们可以认为设备驱动程序是 Windows 内核的一种扩展机制，系统通过设备驱动程序来支持新的物理设备或者扩展功能。

设备驱动程序是可以动态加载到系统中的模块，其文件扩展名为.sys，其格式是标准的 PE 文件格式。驱动程序中的代码运行在内核模式下，尽管它们可以直接操纵硬件，但理想的情况是，调用 HAL 中的函数与硬件打交道，因此，驱动程序往往用 C/C++语言来编写，从而可以方便地在 Windows 所支持的体系结构之间进行源代码层次上的移植。

PE [Ê ã

PE Portable Executable [PE-SPEC] ¾ }Windows NT • ™ z t Ù K ¢ 5 ¶ - c Ÿ t Á ë 32 * ´ , Ä ‘ ¶ û 3 Ñ L ´ — • ™ d ã : q ¶ - r , ³ ¾ ò z Windows NT ¶ } • 5 ‰ 8 v x86 c MIPS c Alpha h n û â ½ ˜ , r < [h Windows NT ° - ½ •) % ¶ û 3 Ñ L ´ d Windows Ÿ º " £ } ' [Intel ‰ 8 v ìPE 3 Ñ L ´ ö â ž ¢ 5 G Ì e Ú ¯ n ¶ ô º ÿ ¶ û 3 Ñ L ´ Ä

Windows NT • â ´ , ÄWindows 9x , y ™ ° PE 3 Ñ L ´ Ù ® PE ö ¾ ¢ 5 ¶ - ¶ û 3 Ñ L ´ d

PE L ´ ô º t COFF Common Object File Format ã ¾ UNIX AT&T UNIX System V / ä & M í •) % , ³ 3 Ñ L ´ Ÿ ³ d 0 • COFF , ³ 3 Ñ G Ì t ¢ Q ó Ú ß ¯ ' » • a.out L ´) t ó • ì Q ö ¢ Ô « % ' " 3 Ñ / m section ô h « Ö « % m ` K ™) g « % M ¥ [¾ C++ 4] N ' ø Ü $ 8 Ë ð o d Ù ® $ ¢ Q ð COFF ´ , Ä , e ‹ [g • g r s c) û t ô º ' " AT&T ' • } COFF n „ h G Ì t ELF Extensible Linking Format ELF , • „ œ · R 5 UNIX + ´ , Ä g ó Linux ä FreeBSD "IBM } AIX / ° XCOFF " — Microsoft • } COFF L ´ Ÿ ³ n „ h G Ì t PE L ´ d } Windows < [h ¶ û 3 Ñ ô º ` .exe c , ³ 3 Ñ ô º ` .obj c N _] Ï ô º ` .dll » ƒ • • Ú N Q ô º ` .sys • 5 3 Ñ + ø ° t PE 3 Ñ L ´ d ; , 64 * , Ä þ ÿ PE 3 Ñ L ´ ™ - ë t ¢ Q ô º Q ‡ K PE32+ m ° 64 * Â · " P ÿ 32 * PE L ´ K PE32 d ‡ à / A , ' • ƒ 32 * PE L ´ d

PE 3 Ñ n ‡ r g ó DOS È c PE È c m ¶ » ƒ m ô l " Í 2.4 N µ d DOS È É } ' ' ¾ t ¹ » • MS-DOS , Ä , B c / " t ¢ m Ý ò ¶ } MS-DOS , B • Õ æ { q This program cannot be run in DOS mode r " , " µ ð o d DOS È K ¾ 4 " PE ³ qPE\0\0 r , ¾ PE È æ Ó dPE È Ó f æ Ó ! COFF È ä ¶ * È s ¶ û ø ¾ 3 Ñ ¶ * È ™ ¾ ¡ d PE È æ Ó g Ã t ' ò • 3 Ñ ¢ Ô æ e ð o g ó m ô h c ø Ü ð o c ¶ û 3 Ñ n ä & Ç Æ ô c Ý ò m ä ô l m Ö Ì c Q ‡ ð o c ¼ ä p z ³ Ö Ì » ƒ ô l , Ã data directory ð o d PE È / ô l , Ã k 16 » ã Ô , Ã » µ t ¢ Q ¶ û 3 Ñ ý & ¶ c ý { ¶ c ‡ W ¶ c 7 G * ¶ d

} PE È K ¾ m ¶ section table m ¶ / $ ¢ » µ t m ` K c m ¥ * " ä Ö Ì » ƒ c P ¢ Ô ' m ð o d s ¶ û ø ¾ m ` K) g â 1 ¶ 8 Q ASCII " ø d m Q ô PE È / ¢ Q 7 G d } m ¶ K ¾ m ô l s $ ¢ Q m } 3 Ñ / ô l h ¶ Ÿ Ì m Ö Ì } ã 5 Æ ã • m K ô l à Œ d H " # z ³ $ ô l æ Ó M } 3 Ñ / g Ã å Ò ô l d – ¢ Q _ É ‹ $ ¾ m * " Ö PE È / G ¨ s j N » } m ô l Õ m 0 m · ¶ Ÿ Â ƒ d

ò Windows , Ä ¦ { ¢ Q ¶ û ø ¾ ¨ " ´ ¶ û ø ¾ / G n ‰ ¸ < „ ½ Š ¶ û ø ¾ Ü â â „ ¦ { þ c P * " d t þ ¶ û ø ¾ / Ý ò Õ ä

ôlÕ}-N*"» ö Ò PE 3ÑL´/ 7G*¶¶» µÝòmäôlm/
‡Ô*" ã¾-s*" ä '„7íG*dN» }¦{¶ ûø¾3Ñ¨
¢ê„¦{ •Éo³ 0 PE È/ G n â¢! •¡ ' û7G*´d
N,7G*´¾ ²E7G*m¶/ $¢Q7G*» Üò•ø¾/ Ýò —g
ôlä Öí•Éo³ —ÄPÿ G n ÿä d

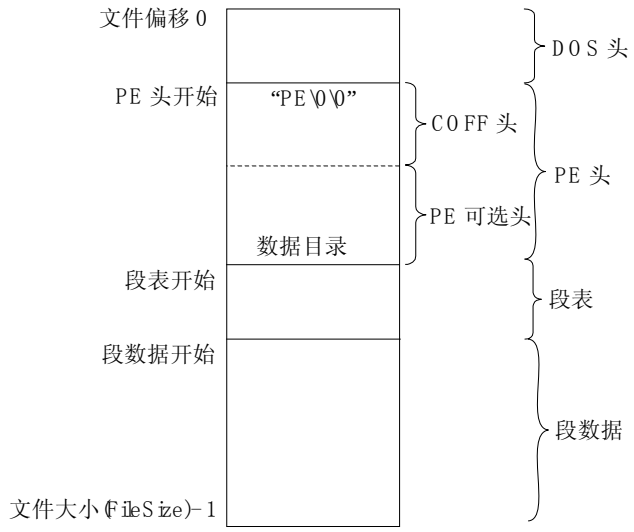


图 2.4 PE 文件的基本结构

'PE 3ÑL´·…ðo Èõ©PE 3ÑL´Ÿ³ [PE-SPEC] d–¢Q õ©‡
x¾Matt Pietrek ß f)3Ã [MSDN-PE1][MSDN-PE2] P}3Ã/¹¶Ýòä H• ut"å
e¢Q¶ û3Ñ góPE È eä7G* ± dP"b PEDUMP Q
WÝò ‡†™¾¢ÚóÚ 0}äõ©ëxd

–ó Visual C++ "b]n dumpbin ¶»yµ{¢Q PE 3Ñ R5ðo H"
•K¡µt Windows Server 2003 SP1 ,Ä/ 3Ñ notepad.exe Èðo!

```
C:\>dumpbin D:\Win2k3-Exe\notepad.exe /headers
Microsoft (R) COFF/PE Dumper Version 9.00.30729.01
Copyright (C) Microsoft Corporation. All rights reserved.


Dump of file notepad.exe

PE signature found

File Type: EXECUTABLE IMAGE

FILE HEADER VALUES
     14C machine (x86)
```

```
       3 number of sections
         42435B9A time date stamp Fri Mar 25 08:30:18 2005
       0 file pointer to symbol table
       0 number of symbols
      E0 size of optional header
      10F characteristics
         Relocations stripped
         Executable
         Line numbers stripped
         Symbols stripped
         32 bit word machine

OPTIONAL HEADER VALUES
…… ã : ˜ Û t ¶ * È æ Ó •

SECTION HEADER #1
 .text name
  7760 virtual size
  1000 virtual address (01001000 to 0100875F)
  7800 size of raw data
   400 file pointer to raw data (00000400 to 00007BFF)
     0 file pointer to relocation table
     0 file pointer to line numbers
     0 number of relocations
     0 number of line numbers
60000020 flags
     Code
     Execute Read

 Debug Directories

Time    Type  Size RVA     Pointer
-------- ------ ----- -------- --------
42435B9A cv    24   00001910 D10   Format: RSDS, {B4CD0BCE-C210-4
934-8161-DFC07F9870B0}, 1, notepad.pdb

…… ã : ˜ Û t       SECTION HEADER #2 ä SECTION HEADER #3 æ Ó •

 Summary

      2000 .data
      9000 .rsrc
      8000 .text
```

概括而言，设备驱动程序有以下三种基本类型：

- 即插即用驱动程序（也称为 WDM 驱动程序，见下文介绍）。这一类驱动程序通常是为了驱动硬件设备而由硬件厂商提供，它们与 Windows 的 I/O 管理器、即插即用（PnP）管理器和电源管理器一起工作。Windows 自身随带了大量即插即用驱动程序，用于支持各种常见的存储设备、视频适配器、网络适配器、输入设备等。
- 内核扩展驱动程序（也称为非即插即用驱动程序）。这一类驱动程序用于扩展内核的功能，或者提供访问内核模式代码和数据的一种途径。它们并没有集成到 PnP 管理

器和电源管理器的框架中。在引入即插即用管理机制以前开发的驱动程序都属于这一类型。现在仍然有大量的内核扩展驱动程序。

- 文件系统驱动程序。这一类驱动程序接收针对文件的请求，再进一步将请求转变成真正对于存储设备或网络设备的 I/O 请求，从而满足原始的文件请求。

Windows 的即插即用（PnP）管理器是 I/O 系统的一部分，它负责即插即用设备的内核支持，其职责是：自动检测设备的插入和移除；动态地分配硬件资源，例如中断、I/O 端口和 I/O 寄存器；指示 I/O 管理器为设备加载正确的驱动程序；向内核及应用程序提供有关设备插入和移除的通知机制。即插即用管理器根据总线和设备的功能分工，定义了一个驱动程序模型，让总线和设备的驱动程序协作完成设备的列举、插入和拔除等管理工作。支持这一模型的驱动程序称为 WDM（Windows Driver Model）驱动程序，共有三种类型：总线驱动程序、功能驱动程序和过滤驱动程序。总线驱动程序既负责管理总线上的设备（配合 PnP 管理器），也为总线上的设备提供了访问总线资源的方法。功能驱动程序负责管理具体的设备，向操作系统提供该设备的功能。过滤驱动程序的用途是监视一个设备的 I/O 请求及其处理过程，甚至增加或改变一个设备或驱动程序的行为。

在 WDM 中，每个硬件设备都有一个设备驱动程序栈（简称设备栈），其中包含一个总线驱动程序和一个功能驱动程序，以及零个或多个过滤驱动程序。PnP 管理器在设备列举过程中，依照总线与设备之间的关系，构建起一棵设备树，其中包含当前系统中所有被检测到的总线和设备。设备树的每一个节点都代表一个实际的设备，该设备的设备栈为其提供软件服务，操作系统（实际上是 I/O 管理器）通过设备栈来访问或操纵设备。

非即插即用驱动程序的用途多种多样，其中内核扩展是最自然的用法。例如，许多系统工具使用内核扩展类型的驱动程序来获得 Windows 内核中的各种系统信息，或者创建系统线程以便在系统进程环境中执行任务。另外，在 Windows 内核中，也有一些模块虽然以“.sys”作为文件扩展名，但它们其实并非设备驱动程序，而是单纯的内核扩展动态链接库，供其他的驱动程序或者内核模块调用。

有关 Windows 中 I/O 管理器、PnP 即插即用管理器、电源管理器以及设备驱动程序的进一步介绍，可参考第 6 章。

文件系统/存储管理

在现代操作系统中，文件系统是外部存储设备的标准接口，它为应用程序使用这些设备中的数据提供了统一的抽象，多个应用程序和系统本身可以共享使用这些设备。在 Windows 中，文件系统的接口部分由 I/O 管理器定义和实现，但文件系统的实现部分位于

专门的一类驱动程序中。当文件系统接收到 I/O 请求时，它会根据文件系统格式规范，将这些请求转变成更低层的对于外部存储设备的 I/O 请求，通过它们的设备驱动程序来完成原始的 I/O 请求。因此，文件系统的驱动程序定义了外部存储设备中数据的逻辑结构，使得这些数据可直接被操作系统和应用程序使用。

Windows 的原生文件系统是 NTFS（NT File System），其驱动程序为 ntfs.sys。NTFS 是专门为 Windows 设计的文件系统格式，它提供了安全性、可靠性、大容量支持、长文件名支持，以及可恢复性等一系列高级特性，目前广泛应用于 Windows 系统。另一个常用的文件系统格式是 FAT（File Allocation Table），这是从 DOS 时代发展起来的文件系统格式，格式规范相对比较简单，目前仍在使用，主要用于兼容老版本的操作系统，以及用于移动设备以便跨操作系统传送数据。

在 Windows 中，每个文件系统实例有它自己的设备栈，因而通过插入过滤驱动程序可以过滤文件 I/O 请求。Windows 支持两种形式的过滤驱动程序：一种直接插入到设备栈中，从而能够看到每一个经过设备栈的文件 I/O 请求；另一种基于 Windows 提供的过滤器管理器驱动程序（FltMgr）的 I/O 过滤框架，称为文件系统小过滤驱动程序，它们并不出现在文件系统设备栈中，而是以回调方式来响应 FltMgr 的事件。

文件系统的底层是对存储设备的管理。大容量存储设备以“分区（partition）”和“卷（volume）”来管理整个存储空间。分区是指存储设备上连续的存储区域（连续的扇区），而卷是指扇区的逻辑集合。一个卷内部的扇区可能来自一个分区，也可能来自多个分区，甚至来自不同的磁盘。文件系统则是卷内部的逻辑结构。因此，Windows 的存储管理形成了一个存储栈，最接近于应用程序的是文件系统，接下来是卷管理部分，最接近于存储设备的是分区管理和磁盘驱动程序。

磁盘设备是典型的即插即用设备，其设备栈和驱动程序符合 WDM 规范。PnP 管理器在设备列举过程中建立起每个磁盘设备的设备栈。设备栈的最底下是总线驱动程序，最上方是一个称为分区管理器的驱动程序，负责通知 PnP 管理器当前磁盘上有哪些分区，因而系统中的卷管理器可以接收到有关分区创建和删除的通知。这样，每个物理分区与卷管理器联系起来，卷管理器再将卷与文件系统关联起来，就形成了完整的存储栈。

有关 Windows 中文件系统和存储管理的进一步介绍，可参考第 7 章。

网络

网络虽然并非 Windows 操作系统中必不可少的组成部分，但实际上，它已经成为绝大多数 Windows 系统的标准配置。Windows 为应用程序提供了多种网络 API，允许应用软件

设计人员根据他们的需求适当选择。以下是 Windows 平台上主要的网络 API：

- Windows 套接字，简称 Winsock。它实现并扩展了 BSD 套接字标准。Winsock 2.0 版本支持一些新特性，比如异步网络 I/O、服务质量（QoS）规范、可扩展名字空间，以及多点消息传输等。
- WinInet。这是一个高层网络 API，它支持多个协议，包括 Gopher、FTP 和 HTTP。Microsoft Internet Explorer 使用 WinInet 来完成数据传输。
- 命名管道（named pipe）和邮件槽（mailslot）。用于不同进程之间进行通信。它们支持不同机器上的进程之间相互通信。命名管道支持连接方式的通信模型；邮件槽支持非连接方式的通信模型，客户进程可以发送广播消息。
- NetBIOS。这是一个早期的网络编程 API，Windows 支持 NetBIOS 是为了兼容老的应用程序。NetBIOS 支持有连接的通信和无连接的通信。
- RPC。这是网络编程的一个标准，往往是分布式系统基础设施的重要组件。RPC 建立在其他的网络 API 基础之上，比如命名管道和 Winsock。Windows 的 RPC 支持异步调用方式。

这些网络 API 都提供了用户模式的动态链接库（DLL），当应用程序通过这些 DLL 发出网络 I/O 请求时，它们必须将接收到的请求传递给内核模式下的相应驱动程序。通常，这些网络 API 要么通过专门的系统服务切换到内核模式，比如命名管道和邮件槽就有专门的系统服务；要么通过标准的系统服务接口，比如 NtReadFile、NtWriteFile 和 NtDeviceIoControlFile，由 I/O 管理器和对象管理器将网络请求转送至对应的驱动程序中。

Winsock 是 Windows 最重要的网络 API，它的用户模式部分不仅包含了一个 DLL（即 ws2_32.dll），还定义了一个可扩展的框架，允许第三方插入传输服务提供者和名字空间服务提供者，以支持更多的传输服务和名称解析或地址映射能力。Winsock 默认支持 TCP/IP、IPX/SPX、AppleTalk 和 ATM 等协议，它提供的传输服务和名字空间服务都通过内核模式驱动程序 afd.sys 实现网络通信。

在内核模式部分，网络 API 驱动程序（譬如 afd.sys）通过传输驱动程序接口（TDI，Transport Driver Interface）与协议驱动程序进行通信。TDI 实际上是一组预定义的 I/O 请求，它描述了各种网络请求，包括名称解析、建立连接、发送和接收数据等。网络 API 驱动程序是 TDI 客户，而传输协议驱动程序实现了 TDI 接口，称为 TDI 传输器。TDI 客户与 TDI 传输器之间是松耦合关系。一个 TDI 传输协议驱动程序可以被多个 TDI 客户使

用。例如，TCP/IP 驱动程序为 tcpip.sys，它既可以被 Winsock 驱动程序 afd.sys 使用，也可以被 netbt.sys 驱动程序使用。Windows 不仅实现了基本的 TCP/IP，还支持 NAT（网络地址转译）、IP 过滤以及 IPSec 规范等协议扩展，这些协议扩展也是内核驱动程序，它们通过私有的接口与 tcpip.sys 进行通信。

在 Windows 中，网络协议与网络适配器驱动程序是分开的，协议驱动程序独立于任何一个网络适配器，而真正发送和接收数据是通过网络适配器进行的。协议驱动程序通过统一的接口与适配器驱动程序进行通信，此接口是 NDIS（Network Driver Interface Specification）。符合 NDIS 的网络适配器驱动程序称为 NDIS 驱动程序，或 NDIS 小端口驱动程序（NDIS miniport driver）。Windows 提供了 NDIS 库，即 ndis.sys，作为协议驱动程序与 NDIS 驱动程序两者之间的桥梁。随 Windows XP 和 Windows Server 2003 一起发行的 NDIS 库是 NDIS 5.1；随 Windows Vista 一起发行的 NDIS 库是 NDIS 6。

NDIS 客户（即 TDI 传输器）利用 NDIS 库提供的功能，对将要发送给 NDIS 驱动程序的命令进行格式化，并发送给 NDIS 驱动程序；而 NDIS 驱动程序则利用 NDIS 库，接收请求和送回应答。NDIS 驱动程序并非标准的设备驱动程序，它们通过 NDIS 库与 NDIS 客户进行通信，I/O 管理器并不介入两者之间的通信过程。

有关 Windows 网络体系结构的进一步介绍，可参考 9.1 节。

2.2.3 Windows 子系统

按照 Windows NT 最初的设计，它支持三个环境子系统：OS/2、POSIX 和 Windows（或称为 Win32）。然而，Windows 子系统是必须要运行的，没有它 Windows 系统无法运行，而其他两个子系统则被配置成按需启动。而且，到了 Windows XP 以后，只有 Windows 子系统随 Windows 系统一起发行。这一节将介绍 Windows 子系统的概况，更详细的信息，请参考 9.2 节。

在Windows平台上，可执行映像文件的格式为PE文件格式[PE-SPEC]（参见上一小节中插入的关于PE文件格式的介绍），其头部域Subsystem指定了该应用程序将被运行在哪个环境子系统中。Microsoft Visual Studio的链接器（linker）支持/SUBSYSTEM命令选项，由它来指定子系统的类型。例如，该域为 2 说明这是一个Windows GUI应用程序，为 3 则是Windows控制台应用程序（Windows CUI）。

Windows 子系统中既有用户模式部分，也有内核模式部分。内核模式部分的核心是 win32k.sys，虽然它的形式是一个驱动程序，但实际上它并不处理 I/O 请求，相反地，它

向用户代码提供了大量的系统服务。从功能上讲，它包含两部分：窗口管理和图形设备接口（GDI）。其中窗口管理部分负责收集和分发消息，以及控制窗口显示和管理屏幕输出；图形设备接口部分包含各种形状绘制以及文本输出功能。

用户模式部分包括 Windows 子系统进程（csrss.exe）以及一组动态链接库（DLL）。Csrss.exe 进程主要负责控制台窗口的功能，以及创建或删除进程和线程等。子系统 DLL 则被直接链接到应用程序进程中，包括 kernel32.dll、user32.dll、gdi32.dll 和 advapi.dll 等，负责实现已文档化的 Windows API 函数。除了有些可以直接在用户模式中完成以外，很多 API 函数需要调用执行体 API 或 win32k.sys 模块提供的系统服务。

Win32k.sys 一方面向用户代码提供系统服务，另一方面也跟 Windows 内核紧密地融合在一起。它通过向内核注册一组出调（callout）函数，以便介入到内核的线程和进程管理等处理逻辑中，同时也可以接收电源事件。对于每个线程，一旦它调用了 win32k.sys 的任何一个系统服务，就变成了一个 GUI 线程，从而纳入到了 Windows 子系统的线程和进程管理范畴。Windows 内核的线程和进程数据结构为 Windows 子系统预留了一些域，从而 win32k.sys 可以方便地操纵它的线程和进程。

下面从窗口管理和图形设备接口两方面来介绍 Windows 子系统的核心功能和结构。

窗口管理

Windows 子系统的用户界面管理有一个层次结构，通常应用程序只是在一个默认的桌面上运行。图 2.5 显示了这一层次结构。每个子系统会话都有自己的会话空间，属于某一会话的资源将从该会话空间中分配。当用户登录到 Windows 中时，操作系统将为该用户建立一个会话；即使用户通过远程桌面或者终端服务连接到一个系统中，系统也会为该用户建立一个单独的会话。

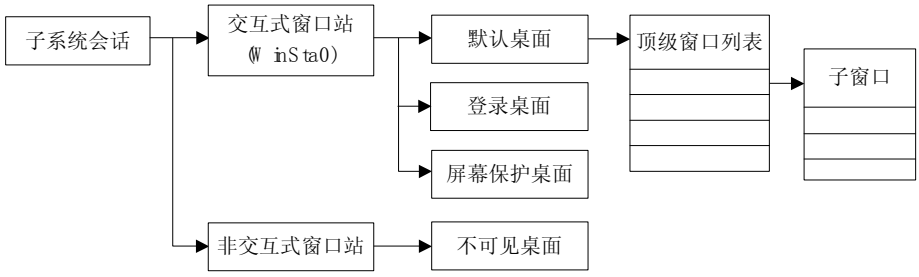


图 2.5 Windows 子系统窗口管理层次结构

在一个会话中，有一个交互式窗口站，可能还有非交互式窗口站。在交互式窗口站中

通常有三个桌面：登录桌面、默认桌面和屏幕保护桌面。通常我们运行的图形界面应用程序运行在默认桌面上。交互式窗口站有独立的剪贴板、键盘、鼠标、显示器等，在它的三个桌面中，任一时刻只有一个是激活的，输入输出设备归激活的桌面所有。

在每个桌面中，都有一个顶级窗口列表，这些窗口往往可以相互重叠，有系统菜单、最大化/最小化按钮和滚动条等。通常各个图形界面应用程序的主窗口属于当前桌面的顶级窗口。在 Windows 中，窗口可以有子窗口，子窗口占据父窗口的客户区域。因此，桌面上的窗口形成了一个层次结构。图 2.5 仅仅显示了顶级窗口的子窗口，实际上，一个窗口总是可以构建它自己的子窗口。

Windows 为常用的窗口定义了一些窗口类（window class），因而应用程序可以非常方便地创建这些窗口类的实例。应用程序如果要定义独特的窗口特性，可以生成一个窗口类，这个窗口类既可以是全新的，也可以是在系统已有窗口类的基础上定义得到。窗口类规定了其对象将如何响应各种消息，包括系统发送给它的消息和用户触发的消息。Windows 窗口的编程模型是消息驱动的，每个窗口对象根据其窗口类指定的窗口过程来响应各种消息。

Windows 子系统会话有一个 RIT（Raw Input Thread）线程，负责从输入设备读取原始的输入事件，然后生成消息，寄送到正确的线程消息队列中。每个包含用户界面元素的线程都应该及时地处理这些消息。通常的做法是在一个消息循环中，不停地获取消息，再分发给目标窗口，由目标窗口的窗口过程来响应。有关 Windows 子系统中的窗口管理和消息机制的更多信息，请参考 9.2.3 节。

图形设备接口

Windows 的图形引擎也是在 Windows 子系统中提供的，它有两方面的特点：首先，它提供了一套与设备无关的编程接口，即 GDI，这使得应用程序可以适应各种底层显示设备的差异；其次，应用程序与图形设备驱动程序之间的通信足够高效，从而即使在频繁输出和刷新图形元素的情况下，Windows 也能够为用户提供良好的视觉效果。

在技术上，Windows 子系统定义了一个稳定的图形体系结构，以便于第三方的图形设备硬件厂商可以方便地将他们的视频显示器和打印设备集成到 Windows 中。如图 2.6 所示，win32k.sys 通过 DDI（显示设备驱动程序接口）与显示驱动程序打交道，而显示驱动程序通过 ENG（图形引擎接口）调用 win32k.sys 中图形引擎的功能。

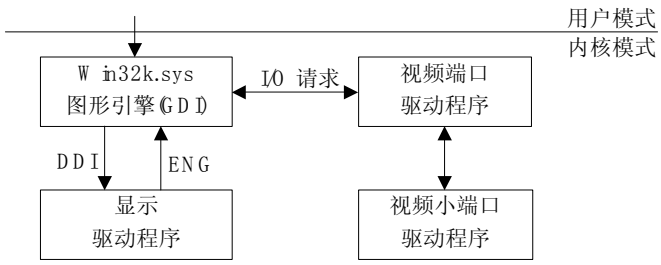


图 2.6 Windows 子系统的图形模块结构

Win32k.sys 的图形引擎实现了基于标准格式位图的图形绘制功能。显示驱动程序在初始化时向图形引擎报告它所支持的物理设备的特征描述。显示驱动程序既可以自己管理图形表面（surface），也可以直接使用图形引擎管理的图形表面。另外，显示驱动程序可以有选择地截取 GDI 的图形绘制操作，也可以将图形绘制操作转交给图形引擎。因此，显示驱动程序在实现功能方面有很大的灵活性。

如图 2.6 所示，显示驱动程序可以帮助图形引擎实现针对特定视频适配器的图形功能，视频小端口驱动程序更是针对视频适配器的硬件特性。两者的分工原则是：显示驱动程序执行一些对用户可见并且性能紧急的图形操作，譬如，它可以直接访问适配器的视频存储区或者寄存器；而视频小端口驱动程序执行一些不常见的图形操作，或者一些不能被中断打断或其他进程抢占的关键图形操作。

视频端口驱动程序由 Windows 操作系统提供，它实际上是一个动态链接库，用于帮助视频小端口驱动程序实现一些公共的、与图形处理有关的功能，以及为小端口驱动程序提供一个与系统内核和执行体打交道的环境。视频小端口驱动程序则负责直接的硬件资源管理和控制。

Windows 子系统的图形系统，除了支持 GDI，还提供了对 DirectX 的显示支持，包括 DirectDraw 和 Direct3D，因而允许像游戏、多媒体播放器等应用软件绕过 GDI 图形引擎，直接操纵显示器硬件，从而获得更快的显示速度，并且避免屏幕抖动。

有关 Windows 子系统图形功能部分的详细信息，请参考 9.2.4 节关于 Windows 显示驱动程序模型的描述，以及 9.2.5 节关于 Windows Vista 以后变化情况的简单介绍。

2.2.4 系统线程和系统进程

在 Windows 中，每个线程代表一个指令执行序列，同时也是一个调度单元；进程定义了一个执行环境，有自己独立的地址空间。每个线程都必定依附于一个进程。Windows

内核除了接受来自应用程序的系统服务调用，它自己也有一些线程用于各种用途。这些线程运行在一个特殊的进程环境中，称为 System 进程。为区分该进程与本节下文即将介绍的操作系统关键进程，本书将前者称为 System 进程，而将后者称为系统进程。System 进程的线程被称为系统线程，其中有一组系统辅助线程（system worker thread），它们代表操作系统或者其他的应用进程来完成一些特殊的工作。

设备驱动程序或执行体既可以在调用者进程中创建线程，也可以在 System 进程中创建线程。或者，也可以不创建任何一个线程，而是调用执行体函数 ExQueueWorkItem 或 I/O 管理器函数 IoQueueWorkItem，向系统辅助线程请求得到它们的服务。这两个函数负责把一个工作项目（WorkItem）放到一个队列中，而系统辅助线程将从此队列提取工作项目，并执行工作项目中指定的一个例程。因此，工作项目中的例程是在 System 进程的环境中执行的，它不能访问其他进程空间中的数据。

系统辅助线程实际上是一个线程池，Windows 在系统初始化时创建了一定数量的辅助线程，而且，随着辅助线程的负载的变化，执行体也会动态地创建一些辅助线程，以满足系统负载的变化需求。

除了系统辅助线程，内核中的许多组件也会创建系统线程来完成一些必要的工作，例如，内存管理器需要后台系统线程来监视和管理页面的换入和换出。另外，设备驱动程序也可以通过调用 PsCreateSystemThread 函数来创建系统线程，以便完成一些并非依附于调用者进程空间的任务，例如网络驱动程序和文件系统驱动程序可以利用系统线程来完成一些必要的后台处理。注意，通过 PsCreateSystemThread 函数来创建系统线程时也可以指定其他的进程作为系统线程的宿主进程，从而能够访问该进程地址空间中的数据，但默认的宿主进程是 System 进程。在本书后面章节的讲述中，我们会提到一些特定任务的系统线程，甚至可以了解到它们在什么情况下是如何被创建的。

从进程的角度来看，Windows 有一组系统进程对于整个系统的运行来说是必不可少的，包括本章前面介绍过的子系统进程 csrss.exe。当 Windows 操作系统引导起来，并且用户登录到系统中时，Windows 已经经过了一系列初始化过程，除了负责与用户交互的 Shell 进程，还启动了诸多系统进程用于实现各种不同的系统任务。总体而言，以下这些系统进程在 Windows 操作系统中扮演了重要的角色：

- 系统空闲进程（Idle）。该进程的 ID 为 0，其中每个处理器或核对应有一个线程。
- System 进程。在 Windows XP 和 Windows Server 2003 中该进程的 ID 为 4，它包含了内核模式系统线程。正如本节上文所述，系统辅助线程，以及执行体和驱动程序通过 PsCreateSystemThread 创建的线程，都在 System 进程中。

- 会话管理器（Session manager，smss.exe）。这是 Windows 系统中第一个创建的用户模式进程。Smss 在 Windows 启动过程中承担了一些重要的步骤，例如创建环境变量等，尤为重要的是，它启动了子系统进程 csrss.exe 和登录进程 winlogon.exe。另外，会话管理器也负责创建新的终端服务器会话（terminal server session），包括建立会话空间的数据结构，然后为新建的终端服务器会话加载子系统，启动 csrss.exe 和 winlogon.exe。

- 登录进程（winlogon.exe）。它负责处理交互用户的登录和注销。当用户按下 Ctrl+Alt+Del 组合键（称为安全注意序列[SAS，Secure Attention Sequence]）时，winlogon 就会接到登录请求，然后激发安全认证过程，并启动用户会话中的初始进程。在用户会话的任何时候，当用户按下了 SAS 组合键时，winlogon 都会提示一个安全对话框，其中通常包含“注销”、“启动任务管理器”、“锁定计算机”、“更改密码”、“关机”等选项。

- Windows 子系统进程（csrss.exe）。正如本章前文所提到的，Windows 子系统进程负责为用户提供一个子系统环境，包括提供控制台窗口的功能，以及创建或删除进程和线程。

- 本地安全权威子系统进程（lsass.exe）。它负责本地系统安全策略，例如允许哪些用户登录到本地系统中、口令策略、授予用户和用户组的特权，以及系统安全审计设置；同时也负责认证用户的身份，以及将安全审计消息发送到系统的事件日志（Event Log）中。

- Shell 进程（explorer.exe）。这是 Windows 的默认 Shell，它提供了系统与用户打交道的各种界面，包括开始菜单、任务栏、资源管理器窗口等几乎所有 Windows 用户都熟悉的界面。

- 服务控制管理器（services.exe）。它负责管理 Windows 的系统服务，这里的系统服务是指一些特殊的进程，它们通常并不与登录用户进行交互，因而被配置成可以在系统引导时自动启动起来，无须交互登录过程。Windows 中有很多功能组件是以服务的方式来实现的，比如事件日志、任务调度器和各种网络组件等。

2.3 关于 Windows 研究内核

Windows并非一个开放源代码的操作系统，但正如上一章所提，Microsoft开放了一份以Windows XP x64 和Windows Server 2003 SP1 为基础的内核源代码，它可以编译和运行，作

为教育科研机构的教学实践和研究的平台使用，称为WRK（Windows Research Kernel，Windows研究内核）[WRK]。除了这份源代码本身，WRK还提供了其他一些材料。这一节将介绍WRK所包含的内容、WRK源代码的说明，以及本书对于WRK中代码的引用。

2.3.1 WRK 包含了什么

WRK 的重要目标是辅助教学，让计算机专业的学生能够通过 Windows 内核的源代码来理解和掌握现代操作系统中的基本概念和各种机制。WRK 的可编译源代码于 2006 年 7 月面向全球大学的教职工开放，经过最近三年多的推广以及一些大学采用 WRK 作为操作系统教学和实验平台的经验积累，目前 WRK 已经逐渐形成了源代码、课程参考讲义、上机实验等全方位的教学系统平台。而且，也有一些大学在 Microsoft 的资助下，利用 WRK 从事操作系统的科学研究工作。

无论通过Internet在线下载[WRK]，或者申请免费光盘，您都可以获得以下相关内容：

- WRK 内核源代码，涉及进程、线程、内存管理、执行体、对象管理器、缓存管理器、本地过程调用（LPC）、注册表、I/O 管理器、安全引用监视器，以及线程调度、APC（异步过程调用）/DPC（延迟的过程调用）、中断以及异常处理等。随源代码一起提供的还有相应的编译工具，因此，无须额外的编译器即可将 WRK 编译成 Windows Server 2003 SP1 的可执行内核。
- NT 设计文档。这是一组早期的文档，尽管其内容已不完全适用于现在的 Windows 操作系统以及 WRK 中的代码，但是，通过阅读这些文档一方面可以清楚地理解 Windows NT 背后的原始设计思想，另一方面也可以看出 Windows 在这十多年中是如何发展和进化的。这些文档涵盖了 Windows 操作系统的方方面面，甚至包括文件系统设计大纲和内核的调试结构等。
- 软件 Virtual PC 2007，以及 Windows Server 2003 SP1 的虚拟机映像，此虚拟机系统已配置好 WRK 内核。利用此 Virtual PC 2007 和 WRK 系统映像，您可以方便地调试和跟踪 WRK 中的代码。
- 课程资源 CRK（Curriculum Resource Kit），包括一整套 Windows 操作系统讲义，共 15 个单元。每个单元又包含一些专题讲义、习题和上机练习题。对于以 Windows 为教学和实验平台的课程，这是一份非常有帮助的课件。CRK 中也包含了“Windows Internals”（第 4 版）的电子书，以及一组工具（windbg、kernrate 等）。
- ProjectOZ源代码。ProjectOZ是一个利用Windows内核的NTAPI建立起来的CPU、

MMU和陷阱机制的操作系统实验环境，其核心是CPU、MMU和陷阱机制的SPACE抽象[SPACE]。由于此实验平台的下面是一个真实的Windows操作系统在处理和操纵硬件，而不是一个模拟器，所以，学生们更有机会学习和感受操作系统算法和数据结构的复杂性。

- 相关的辅助材料和参考资料，包括WAP（Windows Academic Program，Windows学院计划）中的一些教学实践项目、“Windows Internals”两位作者的共 12 小时的视频材料，以及Singularity项目[Singrlarity]的一些文章和讲义。另外，还有一份介绍Windows Vista内核新特性的演讲稿。

然而，Microsoft 目前并非对所有人开放以上材料，而是以教学和科研为开放目标，仅限于大学的教职员工使用。请在使用 WRK 资料以前，首先阅读 WRK 许可条例，参见 http://www.microsoft.com/resources/sharedsource/licensing/basics/wrklicense.mspx

2.3.2 WRK 源代码说明

正如本章前面所讲，Windows 的内核模块文件是 ntoskrnl.exe，位于 Windows\System32 目录下，它包含了 Windows 体系结构中的执行体和内核（或微内核）部分。WRK 提供的源代码可以编译得到这一内核模块文件，在 WRK 编译环境下针对 Intel x86 处理器的默认生成文件名为 wrkx86.exe。Windows 的引导选项/kernel 可以指定不同于 ntoskrnl.exe 的内核模块文件。参见本书附录 A 关于编译、配置和调试 WRK 的详细介绍。表 2.2 列出了 WRK 源代码的目录结构及其对应的内核组件。

WRK 包含了编译 ntoskrnl.exe 内核模块所需要的绝大部分代码，未公开部分的代码主要包括即插即用设备管理、电源管理、设备驱动程序检验器和虚拟 DOS 机的实现。为了编译 WRK 源代码以得到实际可运行的内核模块，缺失的这部分被以二进制目标代码的形式包含在了 WRK 中，位于 base\ntos\BUILD\PREBUILT\i386（或 base\ntos\BUILD\PREBUILT\amd64）目录。该目录还包含了其他一些需要静态链接的目标文件。尽管如此，WRK 对于学习和理解 Windows 的工作机理仍然是一份极佳的资源。

WRK 的代码是从当时最新的 Windows 产品代码中摘出来的，可以编译并运行于 Windows Server 2003 SP1（x86 处理器版本）和 Windows XP SP2（AMD64 版本）系统中，其内核版本为 5.2。WRK 代码与产品代码几乎一致，主要的变化在于去掉了对服务器的支持，比如与 Intel IA64 有关的代码。

Windows 源代码一致性较好，非常易读。代码本身的逻辑以及各标识符基本上是自

解释性的，重要函数的头部都有详细的注释说明，重要的代码片段也有专门的注释。总体上，代码组织较为清晰，如表 2.2 所示。内核模块内部的每个组件都提供了一些接口函数供其他组件调用，也有一些函数供该组件内部使用。表 2.3 列出了一些常用的标识性前缀。有一些组件内部函数也有规律可循：前缀第一个字母后面跟一个 i，或者在前缀后面跟一个 p，这里 i 代表 internal，即内部的；p 代表 private，即私有的。例如，Ki 和 Mi 分别代表微内核和内存管理器的内部函数，而 Halp、Psp、Iop 分别代表 HAL、进程和线程管理组件、I/O 管理器的内部函数。掌握这些命名规律，有助于快速地理解一个函数的归属。

表 2.2 WRK 目录结构和相应的组件说明

目 录	组件说明
public	R Q ¦ Ñ k º ° g Ã 3 Ñ g ó DDK c SDK c HAL ä • â ‘ † ¢ Ô È 3 Ñ
base\ntos	Windows • â f Ö V , Ã
base\ntos\cache	/ É • 8 v W 3 Ñ
base\ntos\config	_ ¶ ¬ £ Ý ò
base\ntos\dbgk	8 Ë • , Ä • â f ´ æ Ó
base\ntos\ex	û ˜ Æ ô • â p c ½ ä c G ¨ v
base\ntos\fsrtl	3 Ñ , Ä n û Ï
base\ntos\fstub	3 Ñ , Ä ä ý Ç
base\ntos\io	I/O • 8 v â g ó ‡ ‡ • 8 v ä (W • 8 v æ Ó
base\ntos\ke	• â g ó ¬ Q 8 g v c CPU • 8 » ƒ ½ ä 4 Ì
base\ntos\lpc	‡ ¶ Q 8 LPC o % ¬ £
base\ntos\mm	• É • 8 v
base\ntos\ob	• â s À • 8 v
base\ntos\perf	• â ÿ Ÿ š Ã _ Ÿ
base\ntos\ps	) Q ä ¬ Q
base\ntos\se	æ ä ³ Ê v
base\ntos\wmi	Windows • 8 Ÿ ³ WMI Windows Management Instrumentation
base\ntos\inc	' Á NTOS æ Ó g Ã 3 Ñ
base\ntos\raw	RAW 3 Ñ , Ä Ú N Q ¬ £ Ý ò
base\ntos\rtl	• â n û ¨ Ï [
base\ntos\init	• â s N æ Ó Ý ò
base\ntos\VDM	¥ DOS o d — Ý ò
base\ntos\VERIFIER	Ú N Q ¿ r v È 3 Ñ

表 2.3 WRK 源代码中各组件接口函数的前缀

函数前缀	所属的组件或函数说明
Cc	/ É • 8 v
Cm	" • 8 v ‡ _ ¶
Dbg/Kd	8 Ë [Æ ô
Ex	û ~ Æ ô
FsRtl	3 Ñ , Ä Ú N Q n û Ï Æ ô
Fstub	3 Ñ , Ä ä ý Ç Æ ô
Hal	HAL " b Ç Æ ô
Io	I/O • 8 v
Ke	• â Æ ô
Lpc	‡ ¶ Q 8 LPC Æ ô
Mm	• É • 8 v
Nt	Windows , Ä û `
Ob	s À • 8 v
Perf	š Ã Æ ô
Po	(W • 8 v
Pp	‡ ‡ • 8 v
Ps	) Q/ ¬ Q
Raw	RAW 3 Ñ , Ä Æ ô
Rtl	• â n û Ï Æ ô
Se	æ Æ ô
Vf	Ú N Q ¿ r v Æ ô
Wmi	Windows • 8 Ÿ ³
Zw	0 Nt • w ½ ` ¢ Š Æ ô ~ à t õ ô r ä G c P æ € - ½ d ¶ » » Nt • w ` K Æ ô ì s f ´ 8 à » Zw • w ` K Æ ô ì s • â f ´ 8 à

2.3.3 本书对 WRK 源代码的引用

本书后面的章节将介绍 Windows 内核中的重要组件，包括进程和线程的管理、内存管理器、同步和并发机制、I/O 管理器，以及存储管理和系统服务等。在讲解这些内容时，将以 WRK 的源代码为主要参照，在必要的地方会列出相应的数据结构或者函数原型，以说明 Windows 中一些关键机制的实现原理。除了 C 语言的代码，有些底层逻辑也可能以 Intel x86 汇编指令的形式列示出来。

在后面的章节引用代码时，为使代码清晰、可读，所摘录的代码会进行简单整理，仅显示原始代码中对应于 Intel x86 编译条件下的部分，注释部分也会做相应处理，目的是使读者能更好地理解相应的逻辑。WRK 的许可条例规定，对代码片段的引用每次不能超过 50 行，但 Windows 有些重要数据结构，例如线程和进程数据结构，超过了 50 行。为此，本书第 3 章采取的做法是，将大的数据结构分成几部分，然后逐部分介绍其成员。

然而，为了保持本书的篇幅不至于过于庞大，笔者将尽可能地避免列出代码，而通过解释关键的逻辑，或者勾画出函数内部或函数之间的控制流图，以说明一些关键机制的实现过程。在讲解一个重要函数的实现时，针对有些关键的步骤，本书可能会指出所对应的代码行。因此，如果读者对照 WRK 来理解这样的函数，建议使用一个可显示行号的编辑器来辅助阅读，这样有助于利用本书帮助阅读源代码。

阅读源代码是掌握实现细节的重要途径，但由于 Windows 内核极其复杂，简单地阅读源代码很容易迷失思路。笔者的观点是，代码本身可能没有那么重要，重要的是 Windows 系统是如何实现一些关键机制的，以及一些关键的控制函数是什么，它们做了哪些重要的操作。这在某种程度上比洞悉每一个实现细节更为重要。本书的一个目标是，帮助读者理清 Windows 各种底层机制的思路和实现机理，而不是简单地把有关的实现细节摸索并展示一遍。根据笔者的经验，建立一个 WRK 调试环境将非常有帮助，这可以让某些控制流更加容易理解。本书附录 A 介绍了 WRK 调试环境的配置办法。

正因为如此，即使读者不能访问 WRK 的代码，也仍然可以阅读本书，譬如，从本书的描述中可以知道 Windows 是如何实现各种系统机制的。配合本书中提到的关键函数的名称以及一些重要步骤的实现逻辑，您可以查阅这些函数的文档，甚至在调试器中跟踪和检查这些函数的实现细节。另一方面，正如本书前言中所讲，即使读者的实验平台并非 Windows Server 2003 SP1 版本，本书的绝大部分内容仍然适用于自 Windows 2000 以来，直至 Windows 7 的系统，因此，抓住 Windows 内核的实现原理比剖析一份源代码更有意义。WRK 仅仅是 Windows 内核实现的一份参照。

Windows Y ,1u)Ú

ü)„ ·Au1k '2Ï4§ X ÈØ)Ú < .,X4± û î D ¹ 0?U qC* b , | <,XG! Ü È<Q' Ø)Ú < D• 3 Ý , | D B,X6Ñ o È Ã ¹ ý*ü7¾D•,X , |6Ñ o 9 ¿Eó ` ä Ô oAu1k Ï u È È Í b/á , á Ô&•,X1k"© È í ™NO?U ó } b Ø)Ú < ê,X , |6Ñ o ÄLc- Au1k Ø )Ú <,XAu1k6Ñ o á • ¤P¬ È W À6Ñ ó Ø)Ú,X D BG£ 3 üN²Eó rKS Ä´!8 È , |1u)Ú ¡ 02Ï4³,X ÔNMG¡?U Ï u Ä üAu1k , | '2Ï È Y ,,È y « Ø)Ú < { `1u)Ú È GAu1k ,X Û ¸ Ã ¹,È y ¡4‰ Y ,) ,X D B È ¹ È Y ,1u)Ú ¡ 02Ï4³ L8 ZE¯/ß `4“/ß1u)Ú ¹ ê Ô G¡?U,X ÔF¼ Ú Ä 0´ å À ÚA|AŽ Windows ,X Y ,1u)Ú Ä

¡ 02Ï4³ T T î4§ Ü Õ,X.@ Ê '2Ï4§ X 9EÝ ½,Ì h,X Y ,1u)Ú Ä b Y ,1u)Ú,X ì w î,È y E ¡ 2Ï4³ D•,X û6Ñ È ¹ È Y ,1u)Ú4˜ Ê,X Š4§ XEî ü \ û/ß z Þ + Ø)Ú <,X.@ Ê(M û 9 ‡ n,X ÄA@ V ÈWindows Õ,X # .@ Ê '2Ï4§ X Intel ,X Ø)Ú < È ´5à W,X Y ,1u)Ú á ÃFS ! « Intel Ø)Ú <.@ Ê(M û,X E ¡ Ä5à º Ô •M6 È ü îE¯/ß)ƒ W È Z Õ!£ þE¯/ß Ý(À0Ÿ,X 0NKÈ È¹ žE¯/ß 0NKÈ `2Ï4³ 0N KÈ KÈ,XLh/• ± x È Windows ü Ø)Ú < Ï ,X Î. Þ Èœ h*ü Z ûG£,X Y ,1u)Ú T 9$µC‡ Ø/¡LÔ" Ä' î þE¯/ß,X Y ,LÔ" `CYE› rL Ã*ü,X(=)Ú Y , Ê È WindowsE¬ ™ NO Ý G>5E- oE¯/ß,X Y ,LÔ" È J ó } b êF¼ , |6Ñ o 9E' W À,X?U" Ä

üE- Ô0´ È å À ÚOj VEÄ Ô ß)„ ·Au1k Þ ?U,X Y ,1u)Ú • `1k"© È â ' Ÿ4¡ Windows,X Y ,1u)Ú Ä y- Ú ÿA†EÄ Windows Y ,1u)Ú,X 5 þ ?U •M6 Ö2Ï 4³ Y ,1u)Ú ÃE¯/ß Y ,1u)Ú ÃNIM6 x 6 Ã(=)Ú Y ,1u)Ú ` ¹ 0Lš1u)Ú Ä Ô â Ÿ4¡ Ô þ Y ,,¥?š ¹ K MemMon Ä

Y ,1u)Ú VEÄ

ü)„ ·Au1k 2Ï4³ È Y , Ä memoryÅ Û Ø)Ú < Ã ¹,È yA“KÂ È ! b Ø)Ú < ê,X , | < Ä ü.@ Ê Þ È Ø)Ú <EîE› Ô4˜ 4“E² y E- o , | < Þ ÈE-4˜ 4“ X ä Z Y , 4“ Ä5à üEC Ê Þ È Ø)Ú <,XAŒ î Û ¸ AŒ*ü Y ,) ,X 0 Û ¸,X ¡ 0 D È ¢5à,È y ¡ 4‰E- o Y ,) ÄE-G ¤ Z Y , È ü Intel x86 '2Ï4§ X È Y , Ý Ý/¡2O _ Ö

x (=)Ú Ä G Y , , | <,X2ö é È Ø)Ú < ¡4‰ Y ,8ƒ(Ê ÈŒîE› 4“1u6î t Þ+ µ Ë 9AÏ ê m,Ì h,X Y ,) Ä ü Intel x86 '2Ï4§ X Þ È(=)Ú Ô þ 32 ! ê 36 !,X ´0ú Ë H D Ä

x <. ³ Ä Ý Ê í/Ä 4“ û Å Ä ü 32 !2Ï4³ Þ È<. ³ 0NKÈ Ã ¹E’ 4 GB û ã È 3 AÈ È H þ0NKÈ Ã ¹ Ý 2^{32}=4 294 967 296þ +8V) Ä Intel x868ƒ(Y Ý çK¼,X+ CÃBóB÷ ^ Ô þ<. ³ E@A¥ ä(=)Ú Ä

x F Ee ÄF Ee Ù ÿ øF¼ Ú Ö!‰ Äsegment Å ` #/Ï Äoffset Å Ä!‰F¼ Ú Û n Z ü H þ 0NKÈ ,X Ô þ Î ¹ ž!‰0NKÈ,X û ã È'' E¬ Ý!‰,X Ô o J ª 2 û Äâ Ï ,Ì G,X !‰,X Î ` û ã Ä #/ÏF¼ Ú Û n Z Ô þF Ee ,Ì Í b!‰ Î ,X #/ÏG£ Ä !8 #/ÏG£ á6ÑCYE›!‰,XE•+ Ä´!8 ÈF Ee ,X rL !‰ Î t Þ #/ÏG£ Ä Intel x868ƒ(3 Ý çK¼,X+ CÃ ^F Ee E@A¥ ä Ô þ<. ³ ê(=)Ú Ä

^ Ô þ A• Ø)Ú < ÈA} WA“KÂ,Ì Í h,X(=)Ú Y ,) ÈE- ÔE›/ß ¡ 02Ï4³ ` Ø )Ú <,Ì f # 0 9 ` ä,X Ä Ø)Ú < Ô4œLÔ?U,X Ô þ(=)Ú È ¹ È W ™NO ^EC Ê Û ¸ ,X E@A¥ ä(=)Ú È üE@A¥E›/ß Ã6Ñ î#] ž Ô o D B4§ X È*î7Ç#] ž I/O ¡ 0 ÄüE- Ô0´ È å À Ú î,ß Windows V) ý*ü Intel x86,X Ï (M û 9 Ý r ‘ Y ,1u)Ú Ä

º ê È ¢ ¡ 02Ï4³,X?¦ z 9,ß È Ô •M6 È WLÔ?U Ý 1u)Ú Ý,X(=)Ú Y , È S k ' Ô þE¯/ßLÔ?U Y , Ê È6Ñ ó ÚG!C‡ ó,X Y ,) 4-E- ÔE¯/ß ×º Ô •M6 È7 V Þ Ô0´ A† È E¯/ß ·>< Ô þ,Ì Í(À0Ÿ,X Ï u ÈW Ý Ô þF Ee Þ(À0Ÿ,X 0NKÈ Äá àE¯/ß,X 0NKÈ h A¹ ,Ì fLh/•,X Ä 3 AÈ È ü Ô þE¯/ß *ü A 9A“KÂ,X Y ,) È â ü º Ô þE¯ /ß *ü A A“KÂ,X á à,X(=)Ú Y , ÄE- . Ã ¹FS ! Ô þE¯/ß Ý ã ê ´ ã ‰ 9 º Ô þE¯/ß,X 0NKÈ ÄE-/¡ ûBü/Ä 0NKÈ,XLh/• û ÈW S k!£ þE¯/ß Ý7¾ Å,X/• Ý 0NKÈ Ä

<Q')„ ·Au1k G! Û,X(=)Ú Y ,C^ 9C^ î È!¨ V)„ ü,X PCEî G! Ý 1 GB~16 GB Y , È È'2Ï4³ E¯/ß DG£ r t ¹ â ÈE- oE¯/ß LÔ?U,X Y , DG£ T TCYE› Z <,X (=)Ú Y , È üE-/¡ ™ ‰ ß È ¡ 02Ï4³ ™NO Ü)Ú] f Y ,,X S*ü È S k Y ,2û5 Ê È ¶ á

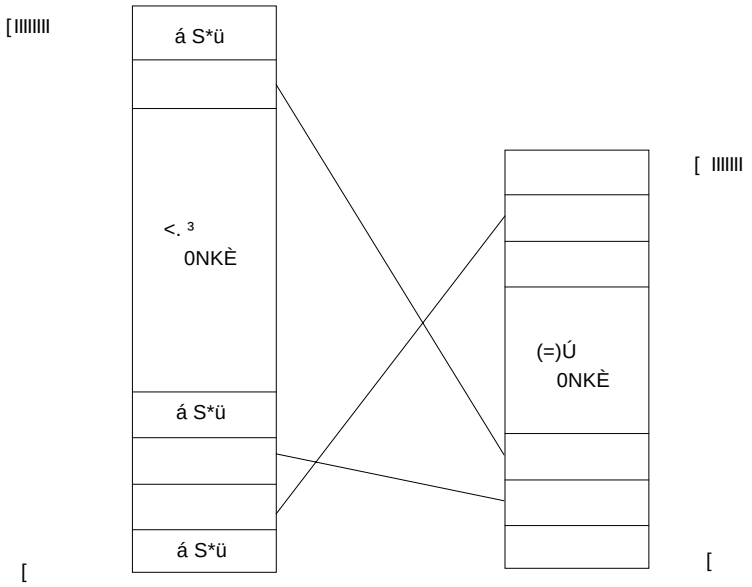
î"¶ ž2Ï4³ D•,X0 n û È à Ê 3 á î ùG¡ E ¡2Ï4³,X û6Ñ Ä ü)„ · ¡ 02Ï4³ È' ¥*ó E-/¡ ™ ‰ Ê È Ô8 ,X ."© ^ á2û ù,XE¯/ß ,X D B ê ··Õ , ê , ÄEî .@,¬ Å È ¢5à ^ W À 4*ü,X(=)Ú Y ,7R Î 94-2û ù,XE¯/ß S*ü È ê5Ù x4-2Ï4³ S*ü Ä ¹ â È' Y ,2û5 ,X(Š ‰4ç?· Ê È2Ï4³ a ^ ê , ,XE¯/ß D B ê ··Õ>™ ² Æ4£0NKÆ ß 9,X Y ,) È ¢5à SE- oE¯/ß Ý î4»4ÁE¤> ÄE- ø þE›/ß/Ä Y , 6 Î ` 6 9 Ä´ " Ý,X î E¯/ß ¡ 02Ï4³FÑ ÕE-/¡ Y ,1u)Ú Ä

y ß 9 ø ã8V Ú Ú ÿ Ÿ4¡NI ã Y ,1u)Ú `!‰ ã Y ,1u)Ú È E- ø/¡ # ,X Y ,1u)Ú • ã È J è Intel x86 Ø)Ú <FÑ Õ Ä ¢ Ï ?¦ z5à?Ô ÈNI ã1u)Ú,X — V) ^<. ³ E@ A¥ ä(=)Ú ×5à!‰ ã1u)Ú,X — í V) ^ !‰+ #/Ï 6 ã,XF Ee E@A¥ ä(=)Ú ÄE-G È E@A¥,X + 8ƒ(.@ Ê ¤ o,X È E@A¥ *ü ,X D B4§ X í Ã6Ñ + ¡ 0 2Ï4³ 91u)Ú,X Ä!8 â È å À ÚA|AŽ Ô o *ü,X Y ,1u)Ú1k"© È' â Ÿ4¡ Windows Y ,1u)Ú,X '4§ X È ¹ ž Windows Y ,1u)Ú < Ù ÿ,X Ô o4˜ Ê Ä

NI ã Y ,1u)Ú

ü V ž,XAu1k '2Ï4§ X È Y , Î) +8V È G 8 þ `E¯ ! Ä£ þ Û å Ô þ +8V È t 1 ¹ â Û å ß Ô þ +8V Ä(=)Ú Y ,,X4ê È G ! [A† ,X(=)Ú È Î n,X È ¹ È ¹,È yA}E¯/ß S*ü(=)Ú 9A“KÂ Y , Ú S kE¯/ß,X | Õ ÚG!L' ¹ Ý r ‘ È´ Y , ) âE¯/ß ÚEîE›(=)Ú 2û š 6(2Ï ü ÔCK Z È¢5à Y ,,X ² ` a Ú G! Ú «L$ b(M n,XE¯/ß `(=)Ú Ä Z '. E-/¡ G6( G2Ï È1T ),X ñCÃ È A}E¯/ß S*ü <. ³ È5à<. ³ `(=)Ú KÈEîE› Ô þ ô Ø>< 9 ` äE@A¥ Ä 8V Ú?U Ÿ4¡,X Intel x86 ,XNI ã Y ,1u)Ú!7 E- Ô/¡ • Ä

üNI ã Y ,1u)Ú È<. ³ 0NKÈ ÝNI Äpage Å 91u)Ú,X È Í h b(=)Ú Y , 3 ÝNI 91u)Ú È(=)Ú Y , ,XNIM6 Ý Ê í/Ä NI û Äpage frame Å È J û ã â<. ³0NKÈ ,XNIM6 ,Ì à Ä´!8 È ô Ø G2Ï ü Y ,NIM6,X Î. ÞE¯> ,X Ä ü<. ³ 0NKÈ E²4Á,XNIM6 Í h b ü(=)Ú Y , ,XNIM6 Ã ¹ á ™E²4Á ÈJ è È Eî E› ã — 4È x Q<. ³ 0NKÈ,XNIM6 â(=)Ú Y ,NIM6 KÈ,X ô Ø G2Ï È(=)ÚNIM6 Ã ¹>• | Õ ÚG!4-(M n,X<. ³NIM6 È¢5à ¾ Ý ' ,ó!7 Ý ™?U,X Ê í ! ^(=)ÚNIM6 ÚG!4-<. ³NIM6 È©0³(=)ÚNIM6,Ì Í 9AÈ /Ô5 C $d ÄV Ò 4.1 / È(=)Ú 0NKÈÄ J 8× È ª ‡ b2Ï4³ (=)Ú Y ,,X DG£ È Ò A’ 1 GB (=)Ú Y , Å Ý ÔF¼ ÚNIM6>• ô Ø Z º {,X<. ³ 0NKÈ Ä ü 32 ! G Ä Þ È J 8× È 0x0~0xffffffff Å Ä



Ò 4.1 <. ³NIM6 `(=)ÚNIM6 KÈ,X ô Ø

"¼ ã È ü Ô þ2Ï4³ È(=)Ú 0NKÈ ¾ Ý Ô þ È <. ³ 0NKÈ Ã ¹ Ý î þ Ä!£ þ<. ³ 0NKÈFÑ ™NO Ý Ô þ ô Ø G2Ï È5à è È<. ³ 0NKÈ Ý,Ì ' ÔF¼ ÚNIM6 J"u Ý Í h ,X(=)ÚNIM6 Ä ü Ò 4.1 ÛA„ á S*ü ,XNIM6 Å Ä rL Þ È!£ þ<. ³ 0NKÈ T T ¾ 6Ñ ô Ø \ å ÔF¼ Ú(=)ÚNIM6 Ä¡E› 9 È£ þ(=)ÚNIM6 T T ¾>• ô Ø Ô þ<. ³ 0NKÈ Ä V p Ý Ô þ(=)ÚNIM6>• ô Ø7Ç ø þ ê ø þ ¹ Þ,X<. ³ 0NKÈ ÈFw ÈE- o 0NKÈ Ú E •!8NIM6 È¹ ü Ô þ<. ³ 0NKÈ m Z!8NIM6 ,X D B È í ü J ª,X<. ³ 0N KÈ Ú Ã ¹,ß E- ,X ¬ ê Ä

Ý ZNIM6 æ Ú,X ¹ â È å À Ã ¹ ÇB5 È!£ þ<. ³ 32 ! µ C È J ÔF¼ Ú ! µ C Û n Z Ô þ(=)ÚNIM6 È J -,X ! µ C í Û n ZNI Y,X #/ÏG£ Ä 3 AÈ È<. ³ Ú ä Z øF¼ Ú ÖNI2ö é+NI Y #/Ï È J4§ X V Ò 4.1 / ÄNI2ö é ÛA¹<. ³ ü ô Ø G2Ï ,X2ö é4ê Ë ÈNI Y #/Ï í Û n ZA¹ üNIM6 YF¼,X K ' !5B Ä

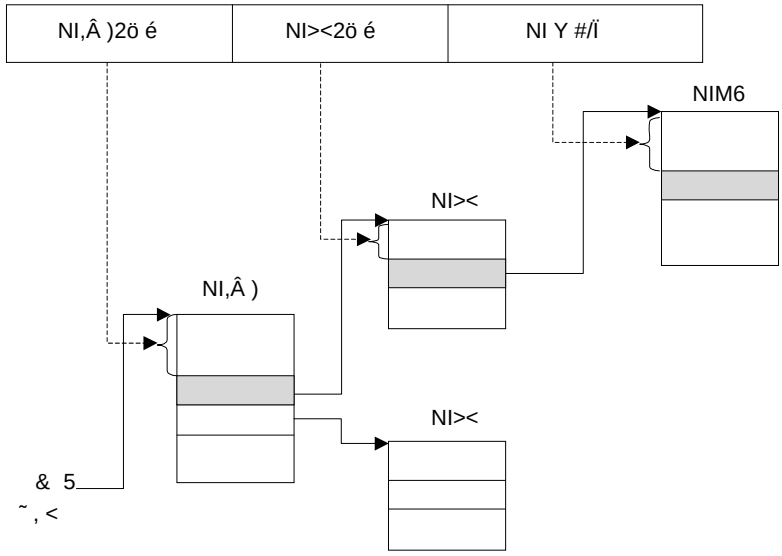
Ò 4.2 ÝNI æ Ú â,X<. ³ 4§ X

ßM6 å À ¹Intel x86 _ 9 Ÿ4¡ ¢<. ³ Y ,NIM6 (=)Ú Y ,NIM6,X ô Ø ÄOj È Ï 2Ï4³ ™NO.B nNIM6,X û ã È Û š,X û ã 4 KB È G 2^{12} +8V È ¹ È32 ! ,X Ô â

Windows *Y s)Ú â r)„*

12 ! NI Y #/Ï È5à ! 20 ! í NI2ö éF¼ Ú È*ü b R Ô þ rL ,X(=)ÚNIM6 Ä ´!8 È ü E- ,X2Ï4³ Þ ÈNIM6 ô Ø>< Ô þ 2^{20}=1 048 576Ä G 1 M Å û ã,X>< Ä V p,È y*ü Ô þ1T),X4“ û>< 9><E'E- Ô ô Ø><,XA± ÈLÔ?U4 MB Y , È ´ >< !£ ÔNMFÑ?U><E' Ô þ(=)Ú NIM6 È G S5×<% NIM6CK Ÿ ,X âM6 12 ! 0 ÈFw 3LÔ?U2.5 MB × V p a5×<% (=)Ú Y , ÔP¬ ´ ! Ã6Ñ 0 È íE¬ Ã ¹ Ý Ô n/ß z,X _4ý ÈE- ª ‡ b ' !2Ï4³ (=)Ú Y ,,X DG£ ÈA@ V1 GB Y ,,XA± È í(=)Ú Y , ,X ÔP¬ 2 ! 0 ÄE-G å À Ñ+9E- o?U2ô È A' ô Ø>< ,X!£ ÔNMFÑ Û n Z Ô þ 32 !(=)Ú Y , Ä

º Ô •M6 È ü!8 1 M û ã,X ô Ø>< È Ý,Ì ' DG£,X><NM J r J"u Ý*ü È ¹ È E-F¼ Ú><NM ÚG! , |0NKÈ #>C ÄIntel x86›*ü Z Ú4{NI><,X • ã 91u)ÚE- Ô ô Ø G2Ï Ä 32 !<. ³ ,XNI2ö éF¼ Ú œ>• Ú äNI,Â)2ö é Ä10 ! Å`NI><2ö é Ä10 ! ÅøF¼ Ú È ¹ È Ô þ 32 !<. ³ ,X rL X ä V Ò 4.3 Ô ÞE•,X<. ³ 4§ X / Ä !<. ³ Ö



Ò 4.3 Intel x86 ,X 32 !<. ³ ,X?· dE›/ß

Î bE- ,X<. ³ X ä È£ þ<. ³ 0NKÈ Í h Ý Ô þNI,Â) ÈJ Ù ÿ 2^{10}=1 024 þ,Â)NM ÄPDE ÈPage Directory EntryÅ ×!£ Ô þ,Â)NM Û å Ô ô Ù ÿ 1 024NM,XNI>< Ä ¹ ÈIntel x86 Ø)Ú < ü?· d Ô þ<. ³ Ê ÈOj B ÔP¬ 10 ! üNI,Â) n ! Ô þNI,Â)NM ÈW Û å Ô þNI>< Ä â B y ß 9,X 10 ! ÈüNI>< n ! Ô þNI><NMÄPTE È Page Table EntryÅ È!8NI><NM Û n Z,Â ÛNIM6,X(=)Ú Ä Ô â ü!8(=)Ú ,X Î. Þ t

ÞNI Y #/Ï È G k Ô4œ,X(=)Ú Ä ü Ò 4.3 / ,X ?· dE›/ß È r4“1• ·><NI ,Â) ÃNI>< `NIM6 KÈ,X Û/ G2Ï È5à<.4“1• í ·>< Z Ô þ<. ³ Ø þ4˜ äF¼ Ú üNI ,Â) ÃNI>< êNIM6 YF¼,X2ö é G2Ï Ä ê #/Ï Å Ä

ü ¹ Þ `4{NI><4§ X È CR3 ˜ , < Ù ÿ ZNI,Â ),X(=)Ú ÈNI,Â ),X û ã 4 096 þ +8V È!£ þ,Â )NM 4 þ +8V × à È!£ þNI><,X û ã 3 4 096 þ +8V È J !£ þNI ><NM 4 þ +8V Ä,Â )NM `NI><NM Û å Ô þ 32 ! È ¾ Ý ! 20 !,ó!7 Û å Ô þ(=)Ú È â 12 !*ü b Ø/¡ Û « µ C È!¨ VNIM6 ú Æ>•A“KÂE› Ã ú AŒ4ç ,1 Ä ü 0´ âM6 Ÿ4¡ Windows<. ³ Y ,1u)Ú Ê È å À aE¯ Ô!9A|AŽ PDE ` PTE,X4§ X Ä

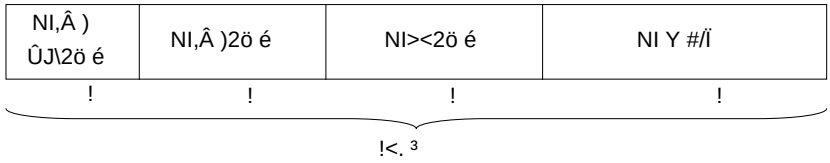
Í b Ô þ$µ,X<. ³ 0NKÈ È 4È x ô Ø G2Ï ELÔ?U 1 þNI,Â) ` 1 024 þNI>< È 40NKÈ 4 096+1 024ћ4 096 þ +8V ÈG 4 KB+4 MB û ã Æ-!¨1T ),X4“ ûNI><î Z 4 KB ÔJÔ È W ú 9,X Q Ø È'<. ³ 0NKÈ rL S*ü,X Y ,,X!¨ _EW ã Ê È\ îNI>< á ™ ü Y , X Î Î 9 È¢5à Ã ¹ U û 8V,ÕE- oNI><,X ÔJÔ ÄáE› È `4{NI><4§ X 3?U ¬ Î û6Ñ,X · Ë È ´ ü?· d Ô þ<. ³ Ê ÈLÔ?U ø õ ¹>< ¡ 0 Ä

ZFS ! ü î4{NI><?· dE›/ß î õ ¹><5à Ð7È û6Ñ ßL!,XKÂNl È Intel x86 Ø)Ú <4ç , Z E@A¥ µ C È G ¢<. ³ (=)Ú ,X ô Ø G2Ï ÄE- È' Ø)Ú <G¡ áA“KÂ à Ô þ Ê ´NO aE¯> E@A¥ Ä!84ç , Ô/¡ ! b Ø)Ú < YF¼,X G6(, |) L ë È3>•/Ä E@A¥ ¿ ¹4ç † ÄTLB ÈTranslation Look-aside Buffeћ Ä TLB Ù ÿ Z ÔE¥ S*üE›,X NIM6,X Y , ô Ø µ C È Ø)Ú < ¤ o Z çK¼,X+ CÃ 9 J ¥ AÏ ª J!¨EWTLB ,XNIM6 ô Ø NM Ä´!8 È Í bNe4 S*ü,X<. ³ È W À \ Ã6Ñ üTLB Ý Í h,X ô ØNM È´5à Ø)Ú < Ã ¹4± Í ¿Eó Ú<. ³ E@A¥ ä(=)Ú ×¡ ÈV p Ô þ<. ³ "u Ý Î)„ üTLB È Fw Ø)Ú < ™NOG›*ü ¹ Þ Ÿ4¡,X ø õ ¹><E›/ßÄ ã G- ?U ø õA“KÂ Y , Å!6Ñ ` ä E@ A¥ Ä üE-/¡ ™ ‰ ß ÈE- Ô õ Y ,A“KÂ î 6 Ô o È È4£E›E- õA“KÂ ¹ â È!8<. ³NIM6 â Í h(=)ÚNIM6 KÈ,X ô Ø G2Ï Ú>•A„) TLB È ¹ È ß õ aA“KÂ!8<. ³NIM6 Ê È Ø)Ú < Ã ¹ ¢TLB r)„ ¿EóE@A¥ ÈL8M2!8 ô ØNM Æ4£>•TLЋL8 Z Ä-è0J>< â È+ bAu1k /ß c,X Y ,A“KÂ Ý Ô n,X F¼ û È´!8 È G S Ø)Ú < ¾4È x Ô þ,Ì ÍEW ã,XTLB È/ß c ,XE¤> 36Ñ9‹ kEW :+,X û6Ñ ¤ [TLB-MISS] Ä

ü Intel x86 Ø)Ú < È TLB ` <+ .@ Ê 94È x,X È 6 ¹A±AÈ ÈEC Ê´"© ¡4‰ TLB ¹ “ t 9 Ã ±+- ê/ÏL8 J ,X ô ØNM Ä Ä J ª Ý o Ø)Ú < AŒEC ÊEîE› Ö 9 ¡4‰ TLB Ä Å' 5à È Ý Ô/¡ ™ ‰ Ã ¹ S TLB ,X ô ØNM ÈFw ' Ø)Ú < Û 6 CR3 ˜ , < ,X Ê í È s´ \1T) È Ô º CR3 ˜ , < Û 6 Z È ã G- ¢ Ô þ<. ³ 0NKÈ Û 6 Z º Ô þ<. ³ 0NKÈ È´!8 s 9Fw oNM"u Ý)Ú+ a ±+- Ä Ý Ô þ _ ê È V p ô ØNM,X PTE

,X < Û « ! Ä 32 ! PTE,X " 12 !FÑ Û « ! È J 1 8 ! Û â ZE- Ô þ < NME¬ F¼NM ÅÆ5B Þ Èí ü CR3 ˜ , < Û 6<. ³ 0NKÈ,XE›/ß È8 ô ØNM ¡' +- ü TLB Ä !8 ê È ü Intel x86 Pentium Pro â,X Ø)Ú < ÈEîE› invlpg Û ¸ Ã ¹ S) þ TLB NM Ä

¹ Þ Ÿ4¡ Z ü Intel x86 Ø)Ú < È Ô þ 32 !<. ³ V)>•E@A¥ Ô þ(=)Ú Ä º ê È Intel x86 Pentium Pro Ø)Ú <E¬ é 9 Z Ô/¡/Ä (=)Ú =) ÄPAE È Physical Address Extension Å,X Y , ô Ø õ ã È W Õ 36 !(=)Ú È <. ³ ¡' 32 ! Ä ´!8 È ü PAE õ ã ß È2Ï4³ Õ 64 GB(=)Ú Y , È J ô Ø • ã `NI><4§ X 3 Ý á à Ä<. ³ ,XE@A¥G›*ü Z Ý4{NI>< È V Ò 4.4 / Ä üNI,Â ) ! r t Z Ô þNI ,Â ) ÛJ\2ö é È5àNI,Â ) `NI>< ,X!£ ÔNMFÑ 64 ! È ¹ È4 KB û ã,XNI,Â) `NI >< ¾6Ñ , 512 NM È!7 Q Í h b<. ³ ,X 9 !2ö é ÄNI,Â ) ÛJ\>< Ù ÿ 4 NM È Ú ÿ Û å 4 þNI,Â ) Ô Ä+ bNI,Â ) `NI>< ,X!£ ÔNMFÑ ¬ ä Z 64 ! È ´!8 W À Ã ¹ £EÄ ÈKS,X(=)Ú Ä8¹1T) r t 4 !(=)Ú È G ¢ s 9,X 20 ! Ä"¼ ã ÈE¬ Ý 12 þ Û « ! Å =) 24 ! È í Ø)Ú < Ú AŒ2Ï4³ S*ü 64 GB(=)Ú Y , Ä Windows*ü 26 ! 9><E'(=)Ú È ´!8 Ã ¹ Õ 2^{26+12}=256 GB(=)Ú Y , Ä



Ò 4.4 Intel x86 PAE õ ã ß,X<. ³ 4˜ ä4§ X

1T5à?Ô ÈPAE õ ã J"u Ý r t<. ³ 0NKÈ,X û ã È AŒ2Ï4³ Õ È î,X(=)Ú Y , Ä Ô âNN " ¤ Ô ß È ü Intel x64 Ø)Ú < È Õ È î4{NI>< Ä _ V È64 ! Windows S*ü ¯4{NI>< È Ú Ô þ 48 !<. ³ E@A¥ ä Ô þ 40 !(=)Ú Ä ¢5à AŒ(=)Ú Y ,E' 1 TB ûãÅÄü WRK ,X ··Õ È å À Ã ¹,ß Windows Í b Intel x86 PAE õ ã ` 64 ! Ø)Ú < ,X Õ È È : ¾A|AŽ Windows Í b Intel x86,X 32 !(=)Ú Y ,,X Õ Ä

!‰ ã Y ,1u)Ú

L8 Z*ü<. ³ 9 r)„ Ý `&I# ,X Y ,1u)Ú ¹ ê È üAu1k ¥) Æ Þ È º Ô/¡G¡?U ,X Y ,1u)Ú • ã Ú(=)Ú Y , æ Ú ä8¹ F þ!‰ Äsegment Å È Ø)Ú < üA“KÂ Ô þ Y ,) Ê È EîE› !‰ Î + #/Ï ,X • ãAu1k Î rL ,X(=)Ú Ä!£ þ!‰FÑ Ã ¹ Ý7¾ Å,XA“KÂ 2 û È Ù ÀAÏ m 2 û Ã(M 4{ ÿ1 Ä _ V È ü Intel x86 Ø)Ú < È Ý çK¼,X!‰ ˜ , < È AŒ!£ 5 Û

¸ üA“KÂ Y , Ê Û n ü ¾ þ!‰ ÞE¯> Ä‰,X V É ü Intel 8086/8088r õ ã Æ4£ S*ü Z È ' Ê!‰,X*üEè =) 8× È ÈÚ2Ï4³,X Y , ¢ 64 KB =) 1 MB ÄØ)Ú < ,X ˜ , <Ä Ù À!‰ ˜ , < ÅFÑ 16 !,X È 4“ Ý 20 Ä ZA“KÂ H þ 8× È È Ø)Ú <,X ."© È Ú!‰ ˜ , < ,X º/Ï 4 ! a t Þ Ô þ 16 ! È 6 ä Z,Â Û Ä rL Þ ÈE- . Ã ¹E’ ,X Ô û (64 K-1) h 16+(64 K-1)=1 114 09Ä Z 80286 Ø)Ú <Ä24 ! Å È ü ± x õ ã ß È!‰ ¬ ä Z Ô þ2ö é È Û å!‰ £EÄ0ú>< ,X ¤ Ô þ!‰ £EÄ0ú È5à!‰ £EÄ0ú ! ,ó!7 Û n Z!‰,X Î Ã!‰KS z ¹ ž Ô o ± x 2 û Ä5à Z 80386 ¹ â È Ø)Ú < ,X ˜ , < !,ó!7E@/Ï Z 32 ! Ä 8V y ß 9 Ú Î b 32 !,X!‰ Ï õ ã 9A|AŽ!‰ ã Y ,1u)Ú Ä

ü Intel x86 ÈF Ee ,X!‰F¼ Ú/Ä !‰EÝ ½0ú Äsegment selectoÅ È Û n Z!‰,X2ö é ¹ ž?UA“KÂ,X(M 4{ ÿ Ä!‰ ˜ , < csÃssÃdsÃesÃfs ` gs çK¼*ü b Û n Ô þ ,X!‰ EÝ ½0ú Ä<Q' ¾ ÝE- A þ!‰ ˜ , < È EC Ê Ã ¹&I# S*ü W À 9 ` ä Ø/¡ s6Ñ Ä J Ý Ý þ!‰ ˜ , < Ý(M!^,X*üEè Ö

- x csÖ ··Õ!‰ ˜ , < È Û å Ô þ Ù ÿ Û ¸,X!‰ È G ··Õ!‰ Ä
- x ss Ö Ü!‰ ˜ , < È Û å Ô þ Ù ÿ ' !A×*ü Ü,X!‰ È G Ü!‰ Ä
- x dsÖ D B!‰ ˜ , < È Û å Ô þ Ù ÿ < `M- Õ D B,X!‰ È G D B!‰ Ä

<Q' ˜ , < ` D B ˜ , <FÑ 32 ! È !‰EÝ ½0ú ¾ Ý 16 ! È J ã V Ò 4.5 / Ä

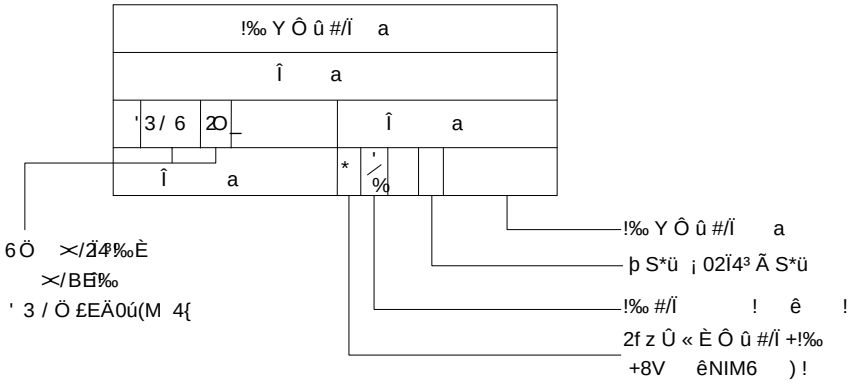
!‰2ö é	>< Û / !	' ! (M 4{

Ò 4.5 !‰EÝ ½0ú ã

ü!‰EÝ ½0ú È!‰2ö é Û n Z Ô þ!‰ ü!‰ £EÄ0ú>< ,X4ê Ë È W Ý13 ! ÈE- 3AÈ â Z Ô þ!‰ £EÄ0ú>< ¾ Ù ÿ$^13=8 192 þ!‰ ×>< Û/ !AÈ â Z!8!‰ ! b < !‰ £EÄ0ú>< ÄGDT ÈGlobal Descriptor TableÅE¬ F¼!‰ £EÄ0ú><ÄLDTÈLocal Descriptor TablÅ Ä ' !(M 4{ÄCPL ÈCurrent Privilege LeveÅÈ3/Ä AË" 5Ù(M 4{ È Ô þ ø !,X Ä0~3 ÅÈ ·>< ZAË" 5Ù,X ' !(M 4{ ÿ Ä(M 4{ CPU,XE¤> õ ã È0 ></ ÔP¬(M 4{ È3 ></ Ô "(M 4{ ÄWindows ` Linux ¾ S*üE- ø/¡(M 4{ È Ú ÿ/Ä Y õ ã Äkernel-mode Å ` *ü õ ã Äuser-mode Å Ä

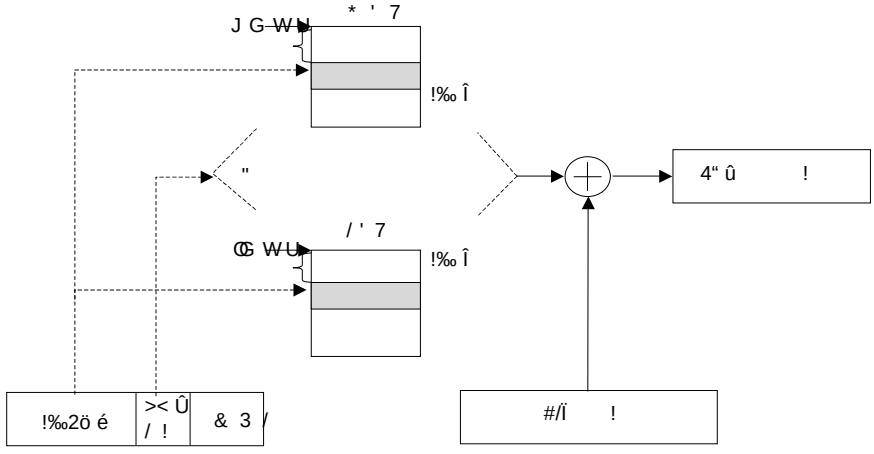
ü Ÿ4¡GDT `LDT ø ô>< ¹ ! Èå À 9,ß Ô,ß!‰ £EÄ0ú,X Y • Ä£ þ!‰ £EÄ0ú*ü 9 n Ô þ!‰ È J Ù À!‰,XCK Ÿ Ã Ý 8× È ` Ô o 2 û Ä Ò 4.64- Î Z!‰ £EÄ0ú,X4§ X Ä!‰ £EÄ0ú Û n Z32 ! Î È¹ ž 20 !!‰KS z Ä G!‰ Y Ô û #/Ï Å Ä 'G ! 0 Ê È

!8KS z) ! +8V ×G ! 1 Ê ÈBKS z) ! 4 096 +8V Ä ¹ È‰KS z ÃE' 2^{20} h4 096=4 GB È G H þ 32 !4“ û 0NKÈ Ä £EÄ0ú(M 4{ ÄDPL ÈDescriptor Privilege Level Å AŒA“KÂ!8!‰,X Ô "(M 4{ È!¨ V È DPL 0 ,X!‰ ¾ Ý 'CPL=0 Ê ! Ã ¹A“KÂ È5àDPL 3 ,X!‰ È Ã+ Ï)CPL ,X ·-ÕA“KÂ Ä2O _ ³ Ä E 4 ! Å Û n Z!‰,X2O _ È Ù À ·-Õ!‰ Ã D B !‰ ÃTSS‰ `LDT !‰ Ä



Ò 4.6 !‰ £EÄ0ú ã

y ß 9A|AŽ GDT ` LDT ÄNR á ñ È < £EÄ0ú>< GDT 2Ï4³ < 8× È Y Ý ,X Ô ô>< È W Ù ÿ Ô î 8 192 þ!‰ £EÄ0ú È ¹ È Ô ô ` <,X GDT ><LÔ?Ù 8 192 h8=64 KB Y ,0NKÈ ÄCPU Ý Ô þ ˜ , < gdtr Ù ÿ Z GDT ,X ÄL8 Z GDT ê È Ø)Ú < º Ý Ô þ LDT È W 3 à Ô î Ù ÿ 8 192 þ!‰ £EÄ0ú È Í h b LDT ,X ˜ , < ldtr È W Ù ÿ Z LDT ,X Ä)„ ü å À Ã ¹)Ú?· Intel x86E@A¥ Ô þF Ee ,XE›/ß È V Ò 4.7 / Ä



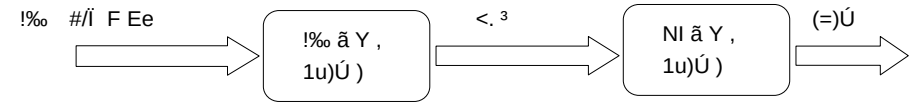
Ò 4.7 Intel x86 !‰+ #/Ï 6 ã,XF Ee ,X?· dE›/ß

Windows *Y s)Ú â r)„*

Ø)Ú < ü?· d Ô þ !‰+ #/Ï ,XF Ee Ê ÈOj B!‰ ˜ , < ,X>< Û/ !.B n hA¹ S*ü GDT Ä8¹>< Û/ ! 0 ÅE¬ LDT Ä>< Û/ ! 1 Å È' â ¢ gdtr ê ldtr k £EÄ0ú><,X È a t Þ!‰2ö éF¼ Ú , ¹ 8 È G k !‰ £EÄ0ú,X È' â B!‰ £EÄ0ú ,X ã È Ð Î 32 !!‰ Î È Ô â t Þ CPU Û ¸ ,X #/Ï È k Ô4œ,X4“ û Ä ü rL ;> Û ¸E›/ß È!£ þ!‰ ˜ , < YF¼FÑ Ý Ô þ 8 +8V,X4ç , Ä ê/Ä YF¼ ˜ , < Å È , Z Í h b!‰ ˜ , <,X!‰ £EÄ0ú È V p!‰ ˜ , <"u Ý ¬ È í ¹ Þ,X Au1kE›/ß Ã ¹ ,Õ+9 ¹ £EÄ0ú><,X!9Px È ¢5à,È y ü Ø)Ú < YF¼Au1k Î4“ û Ä

)„ ü å À Ã ¹ ÇB5 Ô ß È V) ý*ü ¹ Þ Ÿ4¡,X!‰ ã Y ,A“KÂ 9 r)„ ¡ 02Ï4³ ,X îE¯/ß 0NKÈ Ä ' È Ô/¡7¾' ,XA’Au ñ Ç È2Ï4³ < E •,X0NKÈ Ã ¹EîE› GDT 9] f `A“KÂ È!¨ V È ¡ 02Ï4³ D•,X ·-Õ ` D B 2Ï4³ < Ã?•,X È Ø þE¯/ß,X 0NKÈ á ÃFS ! ?U Ù ÿE-F¼ Ú Y , Ä!8 ê È Ø þE¯/ß/• Ý,X D B ` ·-Õ , ü LDT È´5à E¯/ß Û 6 Ê È ¾LÔ ¬ LDT >< È G Ã r)„E¯/ß/• Ý ,X Û 6 Ä ü)„ ·,X h*ü/ß c È!£ þE¯/ß T T Ù ÿ î þ `E¯ õ + È ¹ ž Ô o | Õ D B × Ø þ `E¯ õ + ¶ Ý ·-Õ È 3 Ý D B Ä!¨ V < ¬G£ `M- Õ ¬G£1 Å Ä ¹ È V p*ü!‰ 91u)Ú Y ,,XA± È!£ þ õ + FÑLÔ?U Ô þ!‰ È | Õ D B T TLÔ?U Ô þ ê î þ!‰ Ä!¨ V < Ú ` F¼ Ú È ¹ ž Ü1 Å Ä Í b4± û î D h*ü/ß c È 8 192 þ!‰ Ä Û LDT ,X!‰ ÅC‡ ó S*ü Z Ä Í b2Ï4³ < 0NKÈ È ¾ ?U ã —] f Q!‰,X S*ü È 8 192 þ!‰ Ä Û GDT ,X!‰ Å 36Ñ$µC‡!7 ,X Y , ÚG! Ä ý*ü E-/¡ •"© È ¶ Ã ¹ . E¯/ß KÈ,X0NKÈLh/• û È 3 Ã ¹ \ • “ üE¯/ß KÈ E • D B Ä

Ô âLÔ?UAÈ â,X È!‰ ã Y ,1u)Ú `NI ã Y ,1u)Ú J á Í0Ÿ,X È W À Ã ¼˜ ÜCK 9 ü à Ô þ2Ï4³ S*ü Ä_ r Þ È Intel x86 Ø)Ú <,X Y ,1u)Ú ) ÄMMU ÈMemory Management Unit Å4§ Ü ZE- ø/¡ Ï •"© Ä _ V È Ò 4.8 / Z Ô þF Ee >•?· d ä<. ³ È aE¯ Ô!9>•?· d ä(=)Ú ,X <E›/ß Ä ¡ 02Ï4³ Ã ¹ ÝEÝ ½ S*ü!‰ ã Y ,1u)Ú ) êNI ã Y ,1u)Ú ) 91u)ÚE¯/ß 0NKÈ `2Ï4³(=)Ú Y , ÄWindows ` Linux FÑEÝ ½ ZNI ã Y ,1u )Ú 0 ?U,X Y ,1u)Ú !‰ È à Ê 3 á ÃFS ! #] ž Z!‰ Äå À ü Windows ` Linux ,X Y ·-Õ FÑ Ã ¹,ß Ý G GDT `!‰ ¡ 0,X ·-Õ Ä



Ò 4.8 Intel x86 F Ee ,X ` H?· dE›/ß

Y ,1u)Ú1k"© Ÿ4¡

Y , Au1k 2Ï4³ L8 Z Ø)Ú < ¹ ê Ô G¡?U,XC $d Ëï) Ô þ/ß c,XE¤> FÑ/• á Ô

Windows *Y s)Ú â r)„*

Y ,C $d,X Ý S*ü Ä!M6 ø ã8V Ÿ4¡ Z.@ Ê Õ,X Y ,1u)Ú È ø J V) Ú<. ³
ê5ÙF Ee E@A¥ ä(=)Ú Y , Æ- Ô8V å À ÚOj A|AŽ ü Ô þ 0NKÈ YF¼ V) Ý
E¯> | Õ Y ,1u)Ú È â Ÿ4¡ *ü,XNIM6 Ó 61k"© È¹ ž üE¯/ß Y ,1u)Ú *ü
,X ¹ 0Lš V É `,Ì h,X1k"© Ä

A' ¡ 02Ï4³ ê5Ù Ô þE¯/ß Æ4£9‹ k Z Ô +E²4Á ,X Y , È2Ï4³ êE¯/ß ü ;> E›/ß
LÔ?U ý*üE- + Y , 9$µC‡ Ø/¡ Y ,AË" Ä+ b Y ,AË" , ü | Õ û ÈG!£ õAË" ,X Y ,
û ã Ã6Ñ á,Ì à È*î7Ç Â Ö \ û È J èE- o ã Y , +,X*ó Q < ó 3 á ,Ì à È ¹ È2Ï4³
LÔ?U ¤ o ÜEÖ,X1k"© 9 Ã6Ñ $µC‡E- o | Õ,X Y ,AË" Ä ü)„ ·Au1k 2Ï4³ È Ú
ÄheapÅ!7 E- Ô þ ¤ o | Õ Y , ÚG!6Ñ o,X Y , 'B5 Ä¡ 02Ï4³ S*ü Ú 9$µC‡ Ø/¡ |
Õ Y ,AË" È h*ü/ß cEîE› Ú9‹ k Y , Äå À *ü,X C/C++Î E¤> g ¤ o Z Ú Y ,1u)Ú
,X6Ñ o È ¹ ÈC/C++ /ß c ,X malloc/free ` new/deleteÃ ¹,È y ü Ú,X y · Þ ¹ 0 Ä

Bü5à?Ô È Y ,1u)Ú1k"© Ã ¹ Ú ø û2O Ö! Ò ÛA„"© `0NKÆJÒ><"© Ä ! Ò ÛA„"©
,X ñCÃ \1T) Ö A' ,X Y ÚG! Y ,,X û ã N +8V È1u)Ú Y ,,X2f z M +8V È J è
N=M hK È 3 AÈ È Y ,1u)Ú,X Î) M +8V È)„ ü E Ý K þ) LÔ?U | Õ1u)Ú Ä
ZA„)E- K þ Y ,) ,X S*ü ™ ‰ È! Ò ÛA„"© Ú S*ü Ô þ E Ý K !,X ! ÒÄbitmap ÅÈ
J !£ Ô !,X Ä0 ê5Ù 1 Å*ü 9AÈ âE- Ô ! Í h,X Y ,) ú0NKÆ Ä+ b ! Ò2'.B
A„) Z!£ Ô þ Y ,) ,X0NKÆ ê Æ>• S*ü,X ™ ‰ È ¹ È' Y ,1u)Ú < y Ô þ „,X
Y ,+ AË Ê È¾LÔ ? £ ! Ò È 6Ñ.B n ú Ý ÜEÖ,X0NKÆ Y , Ã ¹$µC‡!8AË" ÄJ ."© È
B AË" Y ,,X û ã ÈB nLÔ?U î å þE²4Á,X Y ,) 9$µC‡!8AË" È â ü ! Ò ?
£ ú , üE²4ÁE- î 0 ! È V R Z È í Ú W À Í h,X Y , ÚG!4- v È J è ÚE- o
!5B ä 1 Ä üGž Y , Ê È?U" v Û n YGž Y ,,XCK Ÿ ` û ã ÈE- Y ,1u)Ú <
Ã ¹Au1k Î!8 õ Y ,Gž Í h b ! Ò ¾ oE²4Á ! È J è Ú W À5B ä 0 Ä

! Ò ÛA„"©,X r)„!¨EW1T) È LÔ?UNq ê,X Y , ÔJÔ ÈEî $\frac{N}{M}$ È ¹ È ¾LÔ
EÖ ' EÝ ª M È Ã ¹ { E-F¼ ÚNq ê ÔJÔ Ä " È*ü AË" ,X Y , û ã á Ô n M +
8V,X á D È ´5à ü ÚG! Y , Ê Ý Ô n,X#>C Ä G 5à?Ô È!£ õ*ü AË" Ú Ð7È M/2 +8V
,X#>C Ä º ê È Y ,1u)Ú < ü ÚG! Y , ÊLÔ?U ? £E²4Á î þ 0 ! È!8 ¡ 0 J áP¬ Ä á
z O(K) Å ÈE- A¹1k"©,X Ô þ5 &• Ä

º ê Ô2O | Õ Y ,1u)Ú •"© S*üJÒ>< 9 £EÄ Æ ÚG!,X `0NKÆ,X Y , + È Ä 0NKÆJÒ><
"© Ä ü ñ Ÿ Ê È H þ Y , +>• ' . Ô þ û,X0NKÆ + t 9 0NKÆJÒ>< Ä ¹ â È ' Y ,1u)Ú
< y Ô þ Y , ÚG!AË" Ê È Ú ¢0NKÆJÒ>< R Ô þ ÜEÖ,X Ã6Ñ ¤ oC‡ ó Y ,,X0NKÆ
+ È J ¢A¹0NKÆ + Ú/• ÎC‡ ó î,X Y , È x4- v È = ß,X Y , Ä V pE¬ Ý,XA± Å ¡'

Ô þ0NKÆ + È5à Æ ÚG!,X Y , í t 9 Æ ÚG! Y ,JÒ>< Ä 'Gž Ô + Y , Ê È Y ,1u)Ú < Ú Æ ÚG!,X Y , + ¢ Æ ÚG!JÒ><E@/Ï 0NKÆJÒ>< ÈV p Ý Ã6Ñ,XA± Èâ,ÌF•,X Y , + Ü J ¹ " X ä È û,X0NKÆ + È ¢5à Ã6Ñ $µC‡ v ,X û Y ,AË" Ä üE- Ô2O •"© È ' Y ,1u)Ú < y Y ,AË" Ê È Ú Ý'; ¹ ß á à,X1*+9 9 ¹ REÖ ',X0NKÆ Y , + Ö

(a) Ô G!"© Äfirst-fit Å È ¢0NKÆJÒ>< R 1 Ô þ$µC‡ v AË" ,X0NKÆ + Ä

(b) Ô G G!"© Äbest-fit Å È ¢0NKÆJÒ>< R Ô yE¥ b v AË" û ã,X0NKÆ + Ä

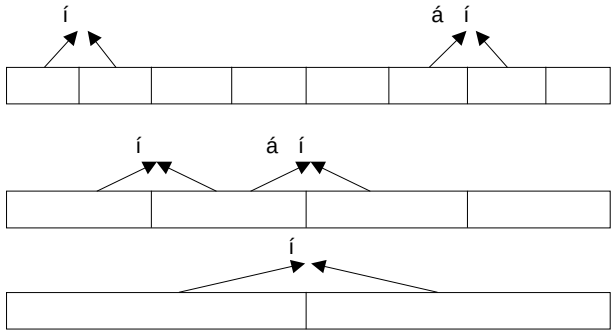
(c) Ô Â G!"© Äworst-fit Å È ¢0NKÆJÒ>< R Ô û,X0NKÆ + Ä

(d) ß Ô þ G!"© Änext-fit Å È ¢0NKÆJÒ><,X ' ! !5B T â ? £ È R 1 Ô þ$µC‡ v AË" ,X0NKÆ + Ä

L8 Z ¹ Þ Ÿ4¡,X ! Ò ÛA„"© `0NKÆJÒ><"© ¹ ê ÈE¬ Ý ø/¡ Y ,1u)Ú1k"© 3 k Ÿ4¡ Ô ß Öslab1k"© ` í 2Ï4³ Äbuddy system Å ÄSlab 1k"© rL Þ ¹ Þ Ÿ4¡,X ! Ò ÛA„"© ` 0NKÆJÒ><"©,X4§ Ü È WJ\ Í ¤ þKÜ ¹ ß,X Y , + S*ü ! Ò"© È Ý'; 2 ,X õ È‡£ ÔL Ý Ô + Y , ` Í h,X ! Ò × ü!8KÜ ¹ Þ Èslab 1k"© S*üJÒ>< 91u)Ú Y , ÄLinux ` Solaris 2Ï4³,X Y S*ü Z slab1k"© Ä

Slab1k"© Í b ã Y ,,X ÚG!M2 ¿EóP¬ È 3 Ý0NKÈ#>C È' AË" ,X Y , û ã Ÿ b 2 ,X ø þE²4Á õ KÈ Ê È ÚG!,X Y , + Ä û ã 2 ,X õ Å , üF¼ Ú0NKÈ#>C Ä #>C ,XF¼ Ú/Ä Y.b(Äinternal fragmentation Å È ´ W ! b Æ ÚG!,X Y , + YF¼ Ä Í h È V p.b(! b Æ ÚG!,X ø þ Y , + KÈ È í/Ä ê.b(Äexternal fragmentation ÅÄ_ V È!M6 Ÿ4¡,X0NKÆJÒ><"© ü4£E› Ô!‰ ÊKÈ,X | Õ Y , ÚG! `Gž ¹ â È T T îEô ä \ î ê.b(È´!8 È G S rL ,X0NKÆ Y ,E¬ Ý \ î È + b ê.b(,X s ´ È Í bEW û Y ,,X+ AË 3 T T ´"©$µC‡ Ä

?· ‡ ê.b(KÂNl,X Ô þ1k"© í 2Ï4³ Äbuddy system Å Ä ßM6 ¹ `E¯ í 2Ï4³ _ 9AÈ â W,X ?U ñ Ç ÄOj È A' Y ÚG!,X H + Y ,,X û ã 2 ,X õ È¨ VAÈ 2^m + 8V È!£ þ +8V,Ì Í b Î ,X #/ÏG£ 0 È1 È2 È È2 ^{m}-1 × º Ý Ô þ D4˜avail[m] È J !£ þ 2ôavail[i] A„) Z û ã 2^{i+1},X Y , +,X0NKÆJÒ>< ÄY ,,X ÚG! Ý'; 2 ,X õE¯> È 3 AÈ È ÚG!4- v ,X Y , + 2 ,X õ • È á1u v ú,ó!7LÔ?UE- î Y , Ä Í b Ï Ô û ã 2^i,X Y , + È A' J,Ì Í b Î ,X #/ÏG£ p È íA¹ Y , +,X í >• n È p,X1 i+1 ! ª>9-Õ t Þ Î ÈE- k ,X Û å,X à û ã,X Y , + Ä Ò 4.9 $è/ Z í Y , + `M2 í Y , + Ä



Ò 4.9 í 2Ï4³ ,X í Y , +

í 2Ï4³ ü ñ Ÿ Ê È H þ Y ÚG! Y , +FÑ 0NKÆ,X È ¹ Èavail[m-1] JÒ>< Û å!8 Y , + ÈA¹ D4˜ J ª Ý,XJÒ><FÑ 0N,X È' v + AË Ô + û ã k ,X Y , + Ê È í 2Ï 4³ ü Ý • ¶ogk º¸X avail[]JÒ>< ¹ R0NKÆ + È ¢1 Ô þ R ,XM20NJÒ>< R Î Ô þ Y , + È4£E› Ú>– ¬ ä ÜEÖ û ã È' âE¨ ²4- v Ä´!8 È í 2Ï4³,X Y , ÚG!E›/ß rL Þ û Y , + Ú>– ä ã Y , +,XE›/ß È Ú>– k ,X ã Y , + ÔF¼ Ú4- v È= ß,X Ö EÖ ',X 0NKÆJÒ>< È ¹ Û ß õ4»4Á ÚG!4- v Ä

ü Y , ² E›/ß ÈV p Y ² ,X Y , + âJÒ>< Æ Ý,X Ô + Y , f í È í W À Ã ¹ Ü J ä È û,X Y , + È ¢5àE@/Ï û Y , + Í h,X0NKÆJÒ>< Ä´!8 È Y , +,X Ü J ü f í ,X Y , + KÈE¯> È J è ¢ ã û È Ô,È á6Ñ Ü J !6 Ä

í 2Ï4³,X Y , ÚG! ` ² ,X ;> )[!¨EWP¬ ÄO(logn) Å È 3 ÝKÂNl Ö1 Ô È0N KÈ ý*ü)[,XKÂNl È+ b W Ý'; 2 ,X õ 9 ÚG! Y , + È ¹ È V p v Ý';+9 û b 2 ,X õ 9+ AË Y , È í0NKÈ#>C ,X)„B5 ÚEW ùG¡ ×1 ` È ê.b(KÂNl ¡' , ü È _ V È ø þ,ÌF•,XM2 í Y , + G S6Ñ$µC‡ v ,X Y ,?U" È í 2Ï4³ 3 á î ^ W ÀE²CK 9 ÚG!4- v Ä Ý Ô o E¯,X í 2Ï4³6Ñ4ç?·E- oKÂNl È)[Ã6Ñ á V `E¯ í 2Ï4³E- Q Ä G b í 2Ï4³,X ÈAº4š µ C ÈAï5Ù Ã ¹ –5×,Ì G [) [TAOCP-1] Ä

y ß 9 å ÀA|AŽ üNl ã Y ,1u)Ú2Ï4³ È '(=)Ú Y ,2û5 Ê ÈA¹ ¢ ¾ oE¯/ß EÝ ½ ¾ o NIM6 È ^ W À,X Y • m .•,¬ Þ È ¢5à7R ÎE- oNIM6 Í h,X(=)ÚNIM6 È ¹ "*ü b â4Á,X Y ,LÔ?U Ä+ b ü Ô þ rL ,X îE¯/ß Ã î Ï u2Ï4³ È ÝE¯/ß S*ü,XNIM6 D Ã6Ñ îCYE›2Ï 4³ ,XNIM6 DG£ È´!8 È ' Ô þE¯/ß å2Ï4³AË" È î,X(=)ÚNIM6 Ê È2Ï4³ ™NO Ý Ô +1k"© ê 1*+9 9 ±A•EÖ Ê $µC‡A¹E¯/ß,XLÔ?U Ä Í b ¡ 02Ï4³5à?Ô ÈE- rL Þ 3 üNIM62f z Þ,X(=)Ú Y ,1u)Ú È J ,X1k"© T T/Ä NIM6 Ó 61k"© ÄEî ¹ ß Ô o1k"© k5×<%,X [MOS] Ö

Ô ìNIM6 Ó 61k"© ÄThe Optimal Page Replacement Algorithm Å ÄE- Ô þ)ÚAŽ Þ

Ô ì,X1k"© ÈW?U" 6Ñ óNX# !£ þNIM6 ß õ S*ü,X ÊKÈ È¢5à.B nA¹NIM6E¬LÔ?U1 Y îKS ÊKÈ ! î,ó!7 S*ü È ¹ ÈüEÝ ½A¹ 6 Î ¾ oNIM6 Ê Èì 5×<%Fw o1 Y ÊKÈ ÔKS,XNIM6 Ä !81k"©,X Î s)Ú ÈC^ Ne4 S*ü,XNIM6 ÈC^ hA¹+- ü(=)Ú Y , ×,Ì Í5à?Ô È V p?U 6 Î 6 9,XA± È h Ã6ÑEÝ ½Fw o á î>•Ne4 S*ü,XNIM6 È ê5Ù ü ¤!‰ ÊKÈ Y á î>•Ne4 S*ü,XNIM6 Ä Ô4œE' ,X p £ åNIM6 6 9 6 Î,X õ D Ä ÈE- Ô1k"©,XKÂNl ÈNX # Ô þNIM6 ß õ>• S*ü,X ÊKÈ ü rL 2Ï4³ T T á Ã> ,X È8M2 ü . _ â Ú d Ä!8 È E-/¡1k"© Ã ¹ ' . Ô þ Î š 9 Í Æ Ý,X1k"© . û6ÑA˜ Ë ÈK ' ."© Èü Ô þ2Ï4³ A„) ß!£ õNIM6>•A“KÂ,X Z Æ+©EÍ D B È Ý ZE- o D B ¹ â È Ã ¹ ü õ ³)ƒ W È S*ü Ô ì NIM6 Ó 61k"© È k Ô å,X 6NI õ D È 0 >•A˜ 1k"©,X Ô þ)ÚAŽ Ô ì –'; Ä

ÔE¥ þ S*ü ÄNRU ÅNIM6 Ó 61k"©ÄThe Not Recently Used Page Replacement Algorithm Å ÄE- Ô1k"©,X ñCÃ È '2Ï4³LÔ?U(=)ÚNIM6 Ê È " ¹ Ý,XNIM6 È ì Ó 6 Fw o ÔE¥ Ä Aç ÔE¥ È Ô þ,Ì Í ÊKÈ È!¨ V È ÔE¥,X ´ þ ÊJs$È1(Å Ô,È"u Ý>•A“KÂ ê Â ,XNIM6 Ä Z Î0ŸCK ÔE¥ ú>•A“KÂ ê Â ,X –5× q B ÈEî !£ þNIM6LÔ?UA„) ß W >•A“KÂ,X ™ ‰ È ¢)[95×<% ÈE- T TLÔ?U.@ Ê,X Õ Ä Ý ø þ Û « ! K Ý(M ÿ,X ã Ö A“KÂ ! R ` Â ! M Ä ' Ô þNIM6>• ñ õ S*ü Ê È W,XA“KÂ ! R >•5B Þ È8¹NIM6>• Â È í Â ! M >•5B Þ Ä üE¯/ß,XE¤> E›/ß ÈR !>• n ó#ÙL8 ÈE- 2Ï4³ 6Ñ Ú ÔE¥ þ >•A“KÂE›,XNIM6 ` ÔE¥>•A“KÂE›,XNIM6 Ä'LÔ?U Ó 6NIM6 Ê ÈOj RFw o þ>•A“KÂE›,XNIM6 × V pE¬ á ó È í4»4Á R Æ>•A“KÂ þ>• Â E›,XNIM6 × V pE¬LÔ?U È î,XNIM6 È í ¾ Q RFw o Æ>•A“KÂ è Æ>• Â E›,XNIM6 ÄE- Ô1k"©,Ì Í1T) J è ç r)„ Èø J ü.@ Ê,X Õ ß Ã ¹ ÝEW Q,X û6Ñ È<Q' W á Ô ì,X È ü r*ü Ý ,X Ä

E¯ ÎNIM6 Ó 61k"© ÄThe First-In First-Out Page Replacement Algorithm Å ÄNR á ñ ÈE-/¡1k"©,X ñCÃ ^ Ý Æ ü Y , ,XNIM64˜4› ä Ô þKó ë Ä 3 Ã ¹ Ô þJÒ >< Å È!£ õ ' ÝNIM6 6 9 Y , ,X Ê í È #Ï t Kó ë,X ÿ × 'LÔ?UNIM6 6 Î Ê È,È y ¢Kó ë /ÏL8NIM6 ÆE- Ô1k"© CK 9 \ ÝF')Ú È^+- ü Y , ÊKÈ ÔKS,XNIM6 6 Î Y , È rL Þ È4£ ?UA“KÂ,XNIM6 3 á k á üKó ë # | È¢5à îEô ä á ™?U,X 6 Î ` 6 9 Ô JÔ Ä+ bE- ,X s ´ È ü rCÉ ÈE- Ô1k"© \ å>•)(À S*ü Ä

1 ` õ îNIM6 Ó 61k"© ÄThe Second Chance Page Replacement Algorithm Å Ä E- Í E¯ ÎNIM6 Ó 61k"©,X E¯ È \7¾' È Í b Ô5Õ,XNIM6 È GKó ë ,XNIM6 È V p W,XA“KÂ ! R 0 È íAÈ âE- þNIM6 á ™5Õ È5à è \ "u*ü Z È)Ú h 6 Î • × V p R ! M20 È íAÈ âA¹NIM6 ÔE¥>•A“KÂE› È ´!8 a4- W Ô õ î È ."© È ^ R !#ÙLÊ È' â ^ W/Ï Kó ë È Q £ W Ô þ „ 6 9,XNIM6 Ô Ä â2Ï4³ aE¯ Ô!9 " ¹Kó ë ,XNI

M6 Ä V pKó ë ,XNIM6 ÔE¥FÑ>•A“KÂE› ÈFw È W À Ú>• q õ ” ¹ ÔF! J#ÙL8 JA“KÂ ! È ' â ü ß õ a>• ” ¹ ,X Ê í>• q õ 6 Î Y , Ä

1 ` õ îNIM6 Ó 61k"© ü K ' r)„,X Ê í ÈÝ Ô/¡ ì ê •"© ÈW Ã ¹FS ! üKó ë Ne4 /Ï |NIM6 È5à ^NIM64˜4› ä)ƒ 6JÒ>< È â*ü Ô þ ÛJ\ Û å ÊKÈ Þ Ô ½ t 9,XNI M6 ÄE- .,X Q Ø È V p Ý Ô þNIM6>• ” ¹ ZA“KÂ ! ¹ â È J á ¢JÒ>< #ÙL8 È í ¾LÔ #ÙL8 JA“KÂ ! È J/Ï | ÛJ\ Û å ß Ô þNIM6 G Ã È´NO ÚNIM6 ¢JÒ>< /Ï JÒ>< Ä+ b E-/¡ ."© £ Ô þ ÊJs,X ÛJ\ üJsM6 Þ/Ï | Ô È˜!8A¹1k"© Ý Ê í 3>•/Ä ÊJsNIM6 Ó 61k"© ÄThe Clock Page Replacement Algorithm Å Ä J rBüC³1 ` õ îNIM6 Ó 61k"© ` <,Ì à È ¾ r)„ Þ á à5à Æ Ä

ÔE¥ Ô þ S*üÄLRU ÅNIM6 Ó 61k"©ÄThe Least Recently Used Page Replacement Algorithm Å ÄE- Ô1k"©,X ñCÃ È '2Ï4³ üEÝ ½ 6 Î Ô þNIM6,X Ê í È ì 5×<% ÔE¥ Ô þ S*ü,XFw þNIM6 Ä81k"© rL Þ Í Ô ìNIM6 Ó 61k"©,X Ô þ Au È J q B NIM6A“ KÂ,X F¼ û s)Ú Ä¶' ´"©,È y# G£NIM6 Ú 9>•A“KÂ,X ÊKÈ È á |*ü ÔE¥ Ô!‰ ÊKÈ YNIM6 >•A“KÂ,XNe)[9(ð# W Ú 9>•A“KÂ,X ™ ‰ È¢5à # } 0 ÎNIM6 Ó 6 ‡1* Ä8¹ ü ÔE¥ Ô!‰ Ê KÈ Y È ¤ oNIM6>•Ne4 A“KÂ È í ü Ú 9,X Ô!‰ ÊKÈ Y È W ÀE¬ Ã6Ñ î>•Ne4 A“KÂ Ä ¡ È8¹ ¤ oNIM6KS ÊKÈ þ>•A“KÂ È ï ü Ú 9 ÈW À U Ý Ã6Ñ ¡' KS ÊKÈ á î>•A“KÂ È ¹ È üEÝ ½NIM6,X Ê í ì 5×<%E- oNIM6 Ä

ÔE¥ Ô þ S*ü ÄLRU ÅNIM6 Ó 61k"© â !M6 Ÿ4¡,X ÔE¥ þ S*ü ÄNRU Å1k"© J á Ô Ä NRU 1k"© Î bNIM6,XA“KÂ ! ` Â ! 9 0 Î ‡ n È5à LRU 1k"© Î bNIM6 ÔE¥>•A“ KÂ,X ÊKÈKS-Á 9 0 ÎEÝ ½ Äü r)„ LRU 1k"© Ê È?U" 6Ñ ó n ! Ô "u Ý S*üE›,XNIM6 È E- Ã ¹EîE›4È x Ô þNIM6JÒ>< 9 r)„ È !£ õA“KÂ Ô þNIM6FÑ?U ^E- þNIM6/Ï JÒ><Oj È ></ W î î>•A“KÂE› Ä ´5à1k"©,X4È x ä EWP¬ ÈL' ¹.@ Ê r)„ Ä

Ô á4£ S*ü ÄNFU ÅNIM6 Ó 61k"©ÄThe Not Frequently Used Page Replacement Algorithm Å Ä!81k"©,X ñCÃ â LRU Ô7È È W ?U ¤ o Z Ô/¡EC Ê r)„ Ä J ."© È !£ þNIM64È x Ô þAu D < È ñ 0 Ä!£ õ ÊJs • Ê È2Ï4³ Í ÝNIM6 È ^ W À,XA“KÂ ! Ä0 ê5Ù 1 Å t Au D < Þ ÈE- È4£ >•A“KÂ,XNIM6 Ý î r t JAu D < È5à á A“KÂ,XNIM6 JAu D <,Ì ÍEW å k r t Ä E- þ1k"©,XKÂNl ü b ÈAu D < ¾ r á £ ÈE- ã G- NIM6,X Z Æ îKS E ¡NIM6 Ó 61k"©,X ‡1* Ä

Í NFU 1k"©,X Ô þ E¯1k"©/Ä NIM65Õ ê1k"©Äpage aging algorithm ÅÄW Í NFU . Z Â È S J È Q õ ³ LRU 1k"© Ä J ."© È ü ÊJs • Â NIM6Au D <,X Ê í È

J á 1T) Eæ rAu D < È5à ^Au D <,X Ç/Ï Ô ! È' â ^A“KÂ ! R t Au D <
,X Ô ºE• ! Þ È5à á Ô ÇE• ! Ä4£E›E- Â ¹ â È V p Ô þNIM64£E› Z Ô!‰Ne4 A“KÂ
,X ÊKÈE› â ÈW 6 6 á a>•A“KÂ Z Èí ´Ne4 A“KÂ5à ÍAu D <,X E ¡ ü4£E› ´ õ Ç/Ï !
¹ â ÈEä#ä#\L8 Z È ª5à · ,X ÔE¥A¹NIM6>•A“KÂ,X ™ ‰ Ä

5Õ ê1k"© ¾*ü ÝL$ þ ! 9 õ ³NIM6 ÔE¥>•A“KÂ,X ™ ‰ ÈW ¤ o,XAu D < JM22’.B,X Ê
KÈAu D È5à ¾ Ô þ,Ì Í,X ÔE¥>•A“KÂ,X –'; È J ì&• ü b È W6Ñ óEä#ä • • Z
Æ,X E ¡ È5àA} ÔE¥ Ô!‰ ÊKÈ,X>•A“KÂ ™ ‰ – â ‡1* Ä ü rCÉ ÈE- o,Ì Í E°,X Z
Æ Í b ‡1*,XG¡?U û J áP¬ È ¹ È5Õ ê1k"©!¨EW K Ý rL ã Ä

¹ Þ Ÿ4¡ Z ¡ 02Ï4³ ü Ó 6NIM6 Ê,X Ô o *ü1k"© `EÝ ½ q B Ä)„ ü å À 9,ß Ô,ß È
2Ï4³ üE¯/ß õ Þ V)1u)Ú ` { (=)Ú Y ,C $d,X ÄE- Í b îE¯/ß2Ï4³ ÝG¡?U,X ã È
´ 1u!£ þE¯/ßFÑ ÝM2 û,X<. ³ 0NKÈÄ!¨ V ü 32 ! Windows Þ Ý 2 GB ê 3 GB
/• Ý,X<. ³0NKÈ Å È W À6Ñ k ,X(=)Ú Y , T T ¾ ,Ì ÍEW å,X ÔF¼ Ú ÈE¯/ß KÈ rL
Þ ü] v ÝL$,X(=)Ú Y ,C $d Ä ¹ È¡ 02Ï4³ ™NO ã — G>5!£ þE¯/ß,XLÔ" ` ÚG!
4- W,X Y , Ä Z>5G£E¯/ß k ,X(=)Ú Y ,C $d ÈE-G Oj Ÿ4¡E¯/ß ¹ 0Lš,X V É Ä

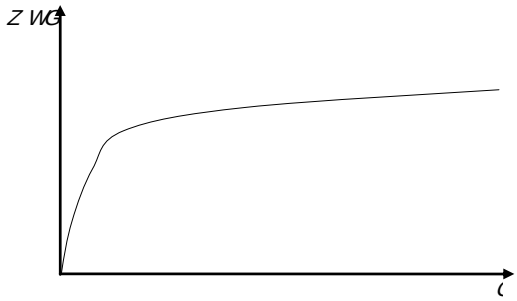
' Ô þE¯/ß>• ï Î J Ô ŸE¤> Ê ÈÔ ñ Ý,XNIM6FÑE¬ ü.•,¬ ÞÄ Ù ÀE¯/ß,X Ã ;>
[Ê Å ÈLc- { # á • !E¯ È < D B ` Ü,X 8× È>• á 0 A“KÂ È J è | Õ Y ,
,XLÔ" 3 Ô Ÿ Î)„ ÈA¹E¯/ßEä#ä9‹ kC^ 9C^ î,X(=)Ú Y ,NIM6 ÄÍ Y ,NIM6,XAË" `$µC‡
Eî ¹ • ê Ö ,X • ã 9 ` ä,X ÄLc- E¯/ß 4 Ý,X(=)Ú Y ,C^ 9C^ î ÈW,XE¤> C_ å
G$¥ È´ Í b(=)Ú Y ,,XLÔ" Ô Ÿ £ å Ä¡ 02Ï4³ BLÔ?U5à ÚG!(=)ÚNIM6,X ."©/Ä
ÝLÔ 6NI Ädemand paging Ä

4§ Ü !M6 Ÿ4¡,XNIM6 Ó 61*+9 È å À Ã ¹)Ú?· Ö¡ 02Ï4³ ü Y ,2û5 Ê Ú B Ô n,X
1k"© `?˜ í È åE¯/ß?U ²(=)ÚNIM6 Ä 3 AÈ ÈÉÝ ½ ¾ oNIM6>• Ó 6 Å ×5àE¯/ß í ü ™?U
,X Ê í å2Ï4³AË" È î,X(=)ÚNIM6 Ä ¡ 02Ï4³ üE- ø5Ù KÈ1u)Ú- ÝL$,X(=)Ú Y ,C
$d ÄFw È Í b Ô þE¯/ß5à?Ô È Ô •M6 È ' W 4*ü(=)Ú Y , þ î Ê È7¾' È Ý oNIM6 î
>• ¡ 02Ï4³ ² • ×º Ô •M6 È ' W,X ;> F EeLÔ?U È î(=)Ú Y , Ê È¡ 02Ï4³ Ã ¹ ^ '
!0NKÆ,X ê5Ù ² 9,XÄ ¶ Ã6Ñ ¢ J ªE¯/ß ² 9 È3 Ã6Ñ ¢ W7¾D• 4,X Y , ² 9 Å
(=)ÚNIM6 ÚG!4- W Ä ü Ï Ô4- n Ê ÈE¯/ß 4,X(=)Ú Y , .B n,X × ¢ Ô þE›/ß 9,ß È
W 4,X Y , DG£)„ Î | Õ ¬ ê,X(M û Ä¹ 0Lš õ _!7 + Ô þE¯/ß,X Y , S*ü ™ ‰
,X õ _ ÄE-G È ¹ 0Lš Ä working set Å Û Ô þE¯/ß ' !!7 ü S*ü,X(=)ÚNIM6,XLš Ü Ä

h*ü/ß c ü ¹ 0 Ê È Í b Y ,,XA“KÂEî)„ Î Ô n,X F¼ û È 3 AÈ È ü Ô!‰ Ê

KÈ Y È/ß c Í Y ,,XA“KÂ T TLš ü Ô n,X8× È Y ÄE- 3 ã G- ÈE¯/ß,X ¹ 0Lš,X ¬ ê,Ì Í5à?Ô 4ç 6,X ÄE¯/ß ¹ 0Lš ¬ êC^4ç 6 È í) ! ÊKÈ YNIM6 6 9 6 Î ¥*ó,X õ DC^ å È E- '' Ý ý bE¯/ß,XE¤> È W,X û6Ñ7¾' C^ Q ×º Ô •M6 ÈE¯/ß,X ¹ 0Lš 3 + ¡ 02Ï4³ 91u)Ú ` { ,X È ¹ 0LšC^ û È í W,X ¬ ê7¾' C^4ç 6 Ä´!8 È ¹ 0Lš1u)Ú 3 ¡ 02Ï4³ Y ,1u)Ú,X Ô þG¡?U •M6 Ä

ü ¹ 0Lš)ÚAŽ õ _ ÈE¯/ß,X ¹ 0Lš Ã ¹*ü Ô þ ` Ñ D w(t, ƒ9></ È J t ·>< ÊKÈ&• È G>< Ô!‰ ÊKÈKÈLh È 3/Ä ¹ 0Lš0k · Äw(t , ƒ></ t- Ga t ø þ ÊKÈ&• KÈE¯ /ß A“KÂ ,XNIM6Lš Ü È ' ÈLc- GX r û Èw(t , ƒ¾ Ã6Ñ r t5à á î £ ã È G w(t, ƒ GX)A×M2Eæ £ Ñ D Ä + b/ß c,X Y ,A“KÂ,X F¼ û s í È w(t, ƒGXEæ r ü GW ã Ê \ ¿ È' â î0 n ß 9 È J Æ4“ û7È V Ò 4.10 / Ä ' Gu Ô n/ß z Èw(t , ƒGÃ6Ñ œ î Ý Ô!‰ ¿Eó rKS È' â0 n ß 9 Ä ' GW û Ê ÈwÆ4“ ª ‡ b/ß c,X ;> F Ee Ä



Ò 4.10 ¹ 0Lš)ÚAŽ õ _

¹ 0Lš)ÚAŽ õ _ Ã ¹*ü 9 Û Ð ÍE¯/ßNIM6,X Ý 1u)Ú È_ V ÈüE¯/ß ñ Ÿ ;> óKÈ È E¯/ß,X ¹ 0Lš \ ¿ rKS È Ô n Ê í È ¹ 0Lš î0 n ß 9 Ä´!8 È Ô/¡ Ý ,X ì ê !‰ ÈA„) ß ¹ 0Lš0 n ß 9 ¹ â ¤ Ô Ê ,X ¹ 0Lš Y • Ä GE¯/ß ,X ¾ oNIM6>•A“ KÂ Z Å È ß õA¹E¯/ß | Ê È,È y E- oNIM6C \(=)Ú Y , È J è ¢.•,¬ tEQ,Ì h,X Y • ÈE- Ã ¹FS ! ¹ ÝLÔ 6NI,X • ãEä#ä ¢.•,¬AÏ ª [Ê Y • È ¢5à û û t ¿E¯/ß,X |Eó z Ä Windows S*ü ZE-/¡ ì ê !‰ È/Ä F EeNX ª < Ä Logical PrefetcheÅ Ä

Fw È V)4È xE¯/ß ¹ 0Lš µ C 6 Û Ô/¡1T “,X ."© ÈA„)!£ þNIM6 ÔE¥>•A“KÂ ,X ÊKÈ ÈE- È BNXA',X G È Ô º ' ! ÊKÈCYE› ZA¹NIM6 ÔE¥>•A“KÂ,X ÊKÈ a t Þ G È í ¢ ¹ 0Lš ôL8!8NIM6 Ä B ¹ 0Lš)ÚAŽ õ _ ÈNXA',X G Ä '' á6Ñ þ ã Å Í b ¹ 0Lš J"u Ý \ û,X E ¡ Ä5à è È ¹ 0Lš,XE- Ô4È x Ã ¹ âNIM65Õ ê1k"© Ý 4§ ÜCK 9 È ü rCÉ E- áL' . È _ V,È y BNIM6,X5Õ ê/ß z 9 ‡ n ú ¢ ¹ 0Lš /ÏL8 Ô þNIM6 Ä

Ý ZE¯/ß ¹ 0Lš,X µ C ¹ â È å À Ã ¹*üE- o µ C 9 E¯NIM6 Ó 61k"© Ä _ V È ü ! M6 Ÿ4¡,X ÊJsNIM6 Ó 61k"© È V p ÛJ\ Û,XNIM6,XA“KÂ ! 0 È í ã G- A¹NIM6 Ã ¹>• Ó 6 È)„ ü Ý Z ¹ 0Lš µ C ¹ â ÈLÔE¯ Ô!9 ” ¹!8NIM6 ú 2 b ' !E¯/ß,X ¹ 0Lš È V p È í á>• Ó 6 È1k"©4»4Á T ! ¹ R J ª,XNIM6 ÄE- Ô E¯1k"©/Ä WSClock [WSCLOCK] Ä

8 J OYE,1Œ)Ú(VTEÄ

¹ Þ Ÿ4¡ Z)„ ·Au1k '2Ï4§ X Õ,X ø/¡<. ³ Y ,1u)Ú ¹ ž ¡ 02Ï4³ ü1u)Ú Y , Ê#] ž,X1k"© ` V É ÈE- Ô8V å À 9,ß Ô,ß Windows Y ,X Y ,1u)Ú < V) Ý 1u)Ú2Ï4³,X(=)Ú Y , ¹ ž!£ þE¯/ß ,X<. ³ Y , Ä

Oj ÈWindows G›*ü ZNI ã Y ,1u)Ú • È ü Intel x86 Ø)Ú < Þ ÈWindows á S*ü !‰ 91u)Ú<. ³ Y , È È Intel x86 Ø)Ú < üA“KÂ Y , Ê ™NO?UEîE›!‰ £EÄ0ú ÈE- ã G- Windows Ú Ý,X!‰ £EÄ0úFÑ XEô ä Z ¢ Î 0 Ô Ÿ È è!‰,X û ãA’5B 0x80000000 Ã 0xc0000000 ê 0xffffffff È K ' ª ‡ b!‰,X*üEè `2Ï4³A’5B Ä ¹ ÈWindows 2Ï4³ ,X · -Õ È Ù À ¡ 02Ï4³ D•,X ··Õ ` h*ü/ß c ··Õ È M6 Í,X 0NKÈFÑ 4“ û 0NKÈ ÄE- /¡ ."©,Ì ' b #; Z Ø)Ú < ,XF Ee V É È!‰ ¾>•*ü bA“KÂ { ` Y , ± x Ä

!7 V å À ü1 2 0´ A† ÈWindows S*ü Z ø/¡(M 4{ ÿ Ö 0 ` 3 È J (M 4{ 0 /Ä Y õ ã È(M 4{ 3 /Ä *ü õ ã Ä' Ø)Ú < ;> Y õ ã ··Õ Ê ÈW À Ø b2Ï4³ 0NKÈ È ! b 0x80000000~0xffffffff È Ý,XE¯/ß E •!80NKÈ ×' Ø)Ú < ;> *ü õ ã ··Õ Ê ÈW À Ø bE¯/ß 0NKÈ È ! b 0x00000000~0x7fffffff ÈE-F¼ Ú0NKÈ E¯/ß/• Ý,X Ä*ü õ ã ··Õ ¾ 6ÑA“KÂE¯/ß7¾D•,X D B È5à Y õ ã ··Õ á ™ Ã ¹A“KÂ ' !E¯/ß,X D B È 3 Ã ¹A“KÂ2Ï4³ 0NKÈ ,X D B Ä Ý,XE¯/ß È Ô ºE¯ 9 Y õ ã È í E • à ,X2Ï4³ 0NKÈ Ä

J õ È ü Windows ,X!£ þ 0NKÈ È<. ³ ,X ÚG! ` ² FÑ ™NO Ý'; ù ,X?˜ íE¯> Ä Windows?˜ n È h*ü/ß c ü S*ü Y , ¹ ! ™NO + AË È ¹ È ¡ 02Ï4³ YF¼ Ã ¹ B h*ü/ß c,X+ AË `Gž ¡ 0 94È x Q H þ<. ³ 0NKÈ,X Y , ÚG! ™ ‰ Ä5à è È Windows 3G›*ü Z ÝLÔ ÚG!,X1*+9 È 3 AÈ È ¾ Ý ' Ô!‰<. ³ Y ,,ó!7>• S*ü,X Ê í È 2Ï4³ ! î W ÚG!NI>< `(=)ÚNIM6 Ä£ þE¯/ß,X<. ³ 0NKÈ,X ÚG! ™ ‰EîE› Ô4˜<. ³ £EÄ0ú ÄVAD ÈVirtual Address DescriptoråA„ ) ß 9 ÈE- o £EÄ0ú X ä Z Ô É G>5 ` • å È ¹ “ b ¿Eó n ! Ô þ Û n<. ³ ,X £EÄ0ú Þ Ä

ü Windows Y ,1u)Ú < ÈL8 Z<. ³ 0NKÈ,X1u)Ú È º ÔG¡?U6 B÷ 1u)Ú(=)ÚNI M6 È¹ ž r)„E¯/ßNIM6,X 6 9 ` 6 ÎE›/ß Ä ü Windows ÈNI û4ê Ë D B g ÄPage Frame

Number DatabasÈ1T/Ä PFN D B g Å £EÄ Z(=)Ú Y , Ø þNIM6,X(Š Õ Ä PFN D B g rL Þ Ô þ4§ X D4˜ È!£ þNIM6 Í h Ý Ô þ PFN NM ÈA„) ZA¹NIM6,X S*ü ™ ‰ È Ù À W,X (Š Õ Ã Í hNI><NM,X 1 µ C Ä!8 ê È ¡ 02Ï4³E¬4È x Z Ô4˜JÒ>< È Ú ÿ Ú,Ì à2O _,X NIM6JÒ yCK 9 È!¨ V È Ý0NKÆ,XNIM6FÑ ¦ 9 Ô þ0NKÆJÒ>< È ¹ È ¡ 02Ï4³ Ã ¹ ¿ Eó ¢A¹JÒ>< 9‹ k Ô þ0NKÆ,X(=)ÚNIM6 ÄNIM6 3 îLc- J(Š Õ,X ¬ ê È¹ ž>•E¯/ß,X S *ü ™ ‰ È5à ü á à,XJÒ>< # | È ê5Ù á 2 b Ï) Ô þJÒ>< Ä Windows,XNIM6 Ó 61k"© 3 !7 üE- o D B4§ X,X Î. Þ r)„,X Ä

<Q' Intel x86 n Z<. ³ â(=)Ú KÈ,XE@ 6 • ã È NI,Â) `NI><LÔ?U ¡ 02Ï4³ 94È x ÈWindows n Z PDE ` PTE È J è ã — 4È x QE- o D B4§ X È ¹ “ Ø)Ú <6Ñ ó!7.B E@A¥<. ³ Ä å À ü Þ Ô0´,XKPROCESS D B4§ X ,ß ,X DirectoryTableBase³!7 Û åE¯/ßNI,Â),X ÛJ\ È ¹ È ¡ 02Ï4³ ü ï Î!£ þE¯/ß Ê È FÑLÔ?U E- þE¯/ß Î0Ÿ Ô +NI,Â) `NI>< D B4§ X È¢5à Î0ŸCKA¹E¯/ß,X 0NKÈ Äü 0´ 4.3.18V È å À Ú î,ß Ô þ 0NKÈ V) Î0ŸCK 9,X Ä

0NKÈ Î0ŸCK 9 ¹ â ÈJ á1 b Ý,XNIM6FÑ ÚG! Q Z È WindowsG›*ü,X ÝLÔ 6 NI,X1*+9 È'E¯/ß ê2Ï4³ S*ü ¤ þ î þ k (=)ÚNIM6,X<. ³ Ê ÈØ)Ú < î?º ¥NIM6Jí AÃ Äpage faulÅ Ö È ¹ È ¡ 02Ï4³ Ã ¹ üNIM6JíAÃ,X Ö Ø)Ú _/ß J ÚG!NIM6 È JA’5B QNI><NM `NIM6 KÈ,XF Ee G2Ï ÆE- Ô Ö ,X ¥*ó Í b S*ü!8<. ³ ,X ··Õ5à?Ô á Ã?•,X È Ô º Ö Ø)Ú _/ß ` ä È í s 9,X ··Õ Û ¸4»4Á ;> È Q £!8 6NIE›/ß ” 3"u Ý ¥*ó Ô Ä

” Ê íNIM6>• 6 Î 6 Û '2Ï4³Ax Y ,2û5 È ê5Ù Ô þE¯/ß+ b ¹ 0Lš,XL$ 5à á AŒ ¹ Ý È î,X(=)ÚNIM6 Ê È Windows î Ó 6 ¹ 0Lš ,XNIM6 ÆE-NM ¹ 0 + Ô þ/Ä ¹ 0Lš1u)Ú < Äworking set manageÅ,X4˜ Ê 9 ` ä,X È WE¤> ü Ô þ/Ä G>5Lš1u)Ú < Äbalance set manageÅ,X2Ï4³4“/ß Ä ¹ 0Lš4ý £,XE›/ß/Ä Â > Ätrim Å ÄWindows r)„ Z <M6,X ¹ 0Lš õ _ ÈÙ À { E¯/ß,X ¹ 0Lš È¹ ž âNIM6 Ó 61k"©4§ ÜCK 91u)Ú(=)Ú Y ,,X < ÚG! Ä

7Ç!8 È å À Æ4£)Ú?· ZWindows ¡ 02Ï4³ Y ,1u)Ú,X Î V ‰ È ßM6 ë Î ü Windows Y ,1u)Ú Ô o!¨EWG¡?U,X4˜ Ê Ö

x ;> ' ¤ o Z Ô4˜ Y ,1u)Ú á u È*ü b ÚG! ÃGž `1u)Ú<. ³ Ä;> ' 3 Ù À Ô þ Ú1u)Ú < Äheap manageÅ È ¤ o | Õ ã Y , +,X1u)Ú Ä

- x NIM6JíAÃ Ö Ø)Ú < Ä ê/Ä NIM6JíAÃ _/ß Å ÄBóB÷ ÚG!(=)ÚNIM6 È ê5Ù ^.•,¬ Þ,X D BAÏ 9 NIM6 Ä
- x Ô4˜2Ï4³4“/ß ÈBóB÷4È x ¡ 02Ï4³,X Y , È J Ù À Ö
  - o G>5Lš1u)Ú < È W Ù À ¹ 0Lš1u)Ú < È!£ 1 s >•A×*ü Ô õ È ¹ 0Lš1u)Ú <BóB÷ r ‘ Ô o < û,X Y
  - o ,1u)Ú1*+9 È!¨ V ¹ 0Lš Â > Ä
  - o E¯/ß/ Ü x 6 < Ä '2Ï4³LÔ?U ;> 6 9 ê 6 Î ¡ 0 Ê ÈEî-¹!84“/ß ` äE- o Ï u Ä 1 3 0´ Ÿ4¡4“/ß(Š ÕE@/Ï Ê È å À Ò4£,ß È V p Ô þE¯/ß,X Ý4“/ßFÑ Ø b1 Y(Š Õ È í W Ý Ã6Ñ>• 6 Î Y , È G4“/ßE¯ 9E@/Ï(Š Õ È ¹ âA¹E¯/ß$µC‡(M n 5 Ê Ê a 6 ² Y , Ä!8 6 9 6 ÎE›/ß!7 + E¯/ß/ Ü x 6 < 9 ` ä,X Ä
  - o Â NIM6 m Î < Ä WBóB÷ Ú6ãNIM6 m ² ô Ø [Ê êNIM6 [Ê Ä ü WRK È m ô Ø [Ê ` m NIM6 [ Ê Ú ÿ+ ø þ4“/ß 9 ` ä,X Ä
  - o LÊNIM64“/ß ÄWE¤> ,X ì 4{ 0 ÈBóB÷ Ú0NKÆJÒ>< Þ,XNIM6#ÙLÊÄ G Y ,LÊ ê ÅÈ ¹ “ '2Ï4³LÔ?ULÊNIM6 Ê Ã ¹$µC‡ J?U" Ä

2Ï4³ 0NKÈ Ù ÿ Z < ,X2Ï4³ ··Õ ` D B4§ X È J è Í b Ý,XE¯/ßFÑ Ã?•,X È ¡ 02Ï4³ ü ñ Ÿ êE›/ß Oj Î0ŸCK2Ï4³ 0NKÈ Ä´!8 È å À y ß 9 ¢2Ï4³ 0NKÈ ,X Y ,1u)Ú Ô Ÿ Ÿ4¡ Ä 1T êCK?• È ü 0´,XA†?· È å À á5×<% 3 GB E¯/ß 0NKÈEÝ NM È ¹ ž Í PAE ` ûNIM6 ÄNIM6 û ã 4 MB Å,X Õ Ä

8 J O2Ï4³ Ÿ ,Xu)Ú

ü Intel x86 Ø)Ú <,X Windows2Ï4³ È 0x80000000~0xffffffff ÝE¯/ß E •,X2Ï4³ 0NKÈ Ä üE-!‰ 0NKÈ È J × 4§ X ü Y ñ Ÿ êL !‰ ` ä,X Ä 8V ÚOj Ÿ4¡ 2Ï4³ 0NKÈ,X ñ Ÿ êE›/ß È' â £EÄ2Ï4³ 0NKÈ ,X | Õ Y ,1u)Ú1k"© Ä

2Ï4³ 0NKÈ ñ Ÿ ê

ü1 2 0´ È å À Æ4£ Ÿ4¡E› Windows,X é ÐE›/ß È ü Y 9‹ k { ¹ ! È Windows ,X tEQ/ß c Ä G ntldr Å Æ4£ ' Ô Z Intel x86 Ø)Ú <,X ÚNI È J èNX Î0Ÿ ZC‡ ó,X NI>< ¹ “ 16 MB ¹ ß,X " Ã ¹EîE›NI>< 9A“KÂ J(=)Ú Y , È 3 AÈ È16 MB ¹ ß ,X<. ³ Ú,È y ô Ø ,Ì à ,X(=)Ú Y , Þ Ä´!8 È 16 MB ¹ ß,X ··Õ ¡' ¹Eã

â,X • ã ü ± x õ ã ` ÚNI ßE¤> Ä5à è È ntldr ü tEQ Y õ + Äntoskrnl.exe ÅÊ Ú ^ W ô Ø (M n,X<. ³ Þ È' â a ^ { x4- J Ñ D KiSystemStartupÄ

GDT ,XA'5B ü ntldr ` ä,X È<Q' WRK "u ÝE-F¼ Ú ··Õ È ÈEîE› üA×A© < C³Cþ WRK ,X | ··Õ È å À Ã ¹,ß È ü KiSystemStartupÑ D9‹ k { Ê È!‰ ˜ , < CSÃDS ÃESÃSS ` FS,X Ú ÿ V ß Ö

CSÖ0x8	—— Í h `E¯ ></	1000
SS Ö0x10	—— Í h `E¯ ></	1 0000
DS ÃESÖ0x23	—— Í h `E¯ ></	10 0011
FS Ö0x30	—— Í h `E¯ ></	11 0000

5à ˜ , < gdtr ,X 0x8003f000 Ä–'; Ò 4.5 G b!‰EÝ ½0ú ã,X £EÄ È å À Ã ¹-¹ F' ÈCS Û å GDT 2ö é 1 ,X!‰ ÈSS Û å GDT 2ö é 2 ,X!‰ ÈDS ` ES Û å GDT 2ö é 4 ,X!‰ ÈFS Û å GDT 2ö é 6 ,X!‰ Ä B gdtr ,X È å À " ¹E- o!‰,X!‰ £ EÄ0ú È V><4.1 / Ä CSÃDS ÃES ` SS!‰ Û å H þ 0NKÈ È ¢ 0 Ô,È 32 ! Ô û Ä Â Ô â Ô þNIM6 Å ÄFS Û å Ô þ(M!^,XNIM6 È âM6 å ÀE¬ îA† È!8NIM6 Ù ÿ Z ' ! Ø)Ú <,X { ÄKPCR Å µ C Ä!7 ´ V!8 È å À ü2Ï4³ ··Õ Ã ¹,ß Eî E› FS 99‹ k ' ! Ø)Ú <,X < µ C È!¨ V ' !4"/ß Ä –5× 3.4.28V Å Ä

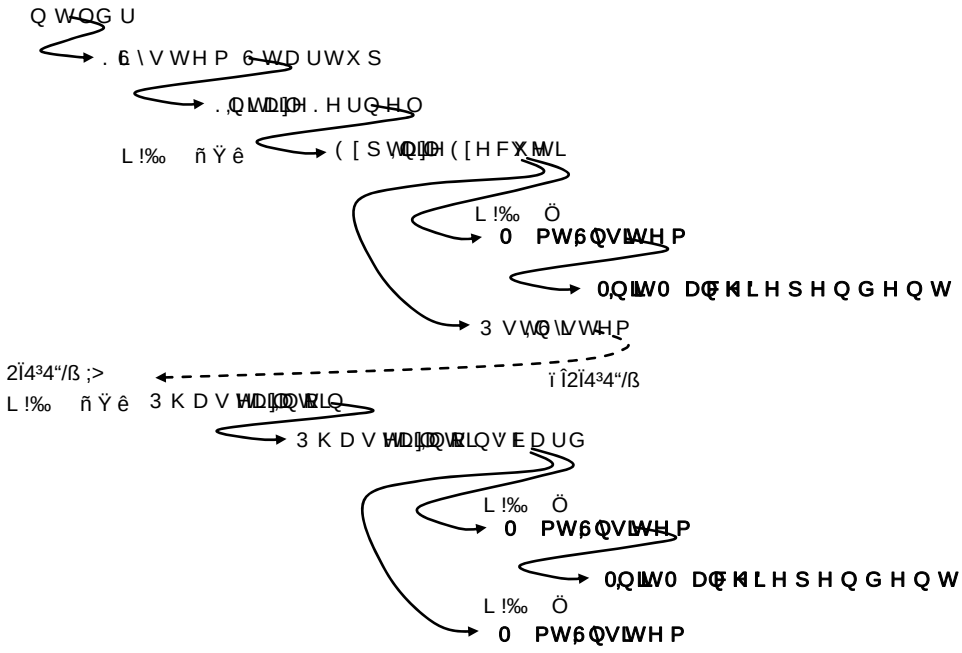
><4.1 Windows 2Ï4³ *ü ,X!‰ £EÄ0úA'5B

!‰	£EÄ0ú	£EÄ0ú Y • Ä4 þ 16 ! H D Å	!‰ Î	!‰ Ô û #/Ï
CS	0x8003f008	ffff 0000 9b00 00cf	0x00000000	0xfffff000
SS	0x8003f010	ffff 0000 9300 00cf	0x00000000	0xfffff000
DSc ES	0x8003f020	ffff 0000 f300 00cf	0x00000000	0xfffff000
FS	0x8003f030	0001 f000 93df ffc0	0xffdff000	0x00001000

+ b CSÃDS ÃES ` SS!‰,XE-/¡A'5B • ã È,Ì ' b!‰ >• #; Z È !‰+ #/Ï 6 ã,XF Ee ,È y>• ô Ø ä4" û ÈE-/¡ ."© 3/Ä 0NKÈ,X GM6 ê Ä ´!8 È ü Windows È Ý,X Y ,A"KÂFÑ 4" û 0NKÈ ,X Y , Ä!‰,XA'5B ´NO(M ÿ5×<% Ä

)„ ü ² KiSystemStartup Ñ D È WA×*üKiInitializeKernel Ñ DE¯> Y ñ Ÿ ê Ä KiInitializeKernel Ñ D ü P0 Ø)Ú < G é Ð Ø)Ú < Þ È ;> 2Ï4³ < 8× È,X Y ñ Ÿ ê Ä KiInitializeKernel Ñ DA×*üExpInitializeExecutiveÈÍ ;> 'E¯> ñ Ÿ ê ÄY ,1u)Ú < ü ;> ' ñ Ÿ ê,X Ä

ü ExpInitializeExecutiveÑ D Äbase\ntos\init\initos.c¢ Ê,X 241~901> Å ÈL8 Z ;
> '7¾D•>• ñ Ÿ ê ¹ ê È ;> ',X Ø þ $4˜ Ê È Ù À Y ,1u)Ú < È 3>• ñ Ÿ ê Ä5à è È!£
þ $4˜ ÊFÑ>•A×*ü ø õ ñ Ÿ ê È Ú ÿ Í h bL !‰ 0 ñ Ÿ ê `L !‰ 1 ñ Ÿ ê ÄG b Y ,X ø
L !‰ ñ Ÿ ê,X ` H Ÿ4¡ ÈAË –5× 2.6.28V Ä Ò4.11 / Z â Y ,1u)Ú Ý G,X ñ Ÿ êE›/ß Ä



Ò 4.11 #] ž Y ,1u)Ú,X2Ï4³ ñ Ÿ êE›/ß

Windows tEQ/ß c ntldr ¾ ¤ o Z ™?U,X Y ,)ƒ W È2Ï4³0NKÈ,X ?U ñ Ÿ ê ¹ 0 ü
MmInitSystem Ñ D ` ä,X È ´!8 È y ß 9 å À,ß Ô,ß MmInitSystem Ñ D,X ·-Õ
Äbase\ntos\mm\mminit.c¢ Ê,X 336~2 397> Å ÄMmInitSystem Ñ D Ù À ÝF¼ Ú ·-ÕF Ee È
Ú ÿ Í h bL !‰ 0 ÃL !‰ 1 `L !‰ 2 ,X ñ Ÿ ê È V Ò 4.11 / ÄE-G L !‰ 1 âL !‰ 2 ñ Ÿ ê
FÑ ü Phase1InitializationDiscard Ñ D >•A×*ü,X Ä å À Ã ¹ ^ W,ß . Ý þ Ñ D,X1T)4˜ Ü Ä

MmInitSystem Ñ D üL !‰ 0 .,X ñ Ÿ ê ¹ 0 Ä434~2 208 > ·-Õ Å ?U ` ä D B
4§ X,X ñ Ÿ ê ¹ ž Ô o < ¬G£,XA’5B Ä ü 466~468 > È å À,ß Ý þ < ¬G£
MmHighestUserAddress Ã MmUserProbeAddress ì MmSystemRangeStart,X A’5B V ß Ö

```
MmHighestUserAddress = (PVOID)(KSEG0_BASE - 0x10000 - 1);
MmUserProbeAddress = KSEG0_BASE - 0x10000;
MmSystemRangeStart = (PVOID)KSEG0_BASE;
```

E-G KSEG0_BASE 0x80000000 Ä?•base\ntos\inc\i386.h X 1 980> Å È ¹ È*ü

0NKÈÄ 3/Ä E¯/ß 0NKÈ ÅÔP¬ 0x7ffeffff È5à2Ï4³ 0NKÈ ¢ 0x80000000 Ô Ÿ Ä y ß 9 å À ,ß Ô ß c MiGetPteAddressÖ

```
#define MiGetPteAddress(va) ((PMMPTE)((((ULONG)(va)) >> 12) << 2) + PTE_BASE))
```

E-G PTE_BASE,X 0xc0000000 Ä?•base\ntos\inc\i386.hX 1 972> Å ´!8 È MiGetPteAddressX ÿ È4- n Ô þ<. ³ ÈAu1k Î J Í h,X PTE,X È G<. ³ üNIM6,XNI><NM,X Ä ¢A¹ n 3 Ã ¹,ß Î È Ý,XNI><NMFÑ ÝNN c , ü ¹ 0xc0000000CK Ÿ,X Y , Ø Ä a,ß c MiGetPdeAddressÖ

```
#define MiGetPdeAddress(va) ((PMMPTE)((((ULONG)(va)) >> 22) << 2) + PDE_BASE))
```

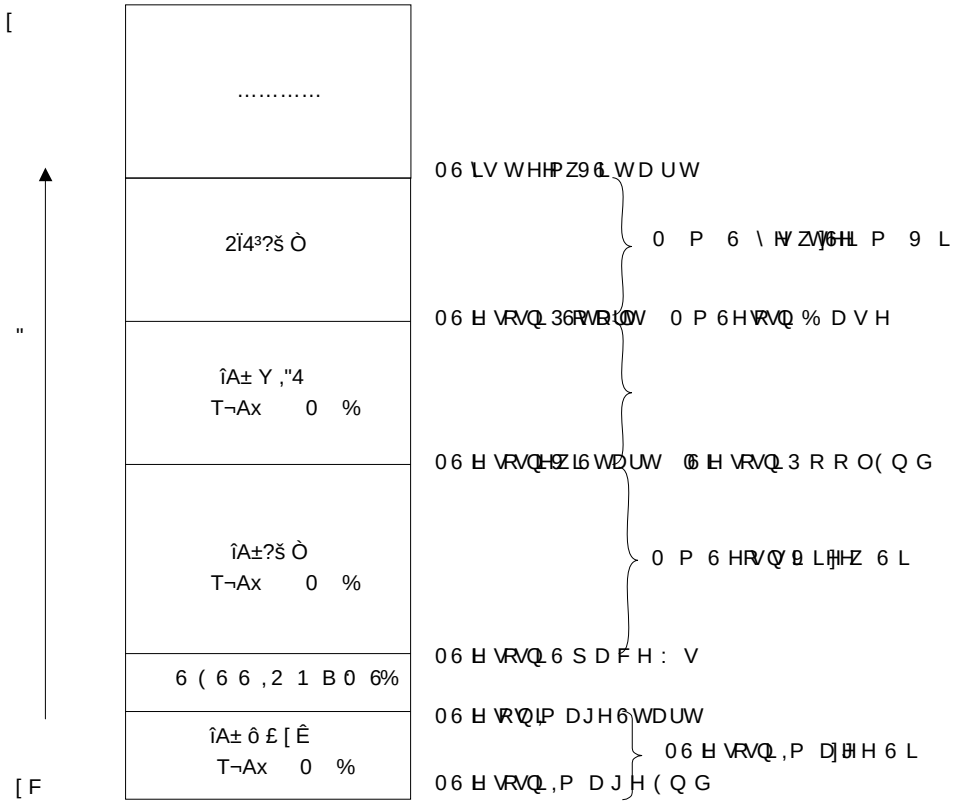
E-G PDE_BASE,X 0xc0300000ê 0xc0600000 È ª ‡ b PAE Ä(=)Ú =) Å ú ' Ô Ä?• base\ntos\inc\i386.hX 1 964 ê 1 968> Å Ä å À á5×<% PAE,X ™ 6 È ¹ È PDE_BASE,X 0xc0300000 È GNI,Â)NM ! b 0xc0300000Ø Ä

AÈ â Ô&• Èntldr ü Ú { x4- Y ¹ ! È Æ4£ Ú Y ÃHAL ` Ô o>• ÛA„ é Ð- | ,XPE |/ß c ô Ø Z 0x80000000# Þ,X !5B Ø Ä ü Windows Server 2003 SP1 2Ï4³ È!8 !5B 0x80800000 Å Ä J é Ð- |,XPE |/ß c/á â Ú>•G¡ n ! P¬0Ã Y , Ä2Ï4³ PTE Å ³ Ä

² MmInitSystem Ñ DÄ?• mminit.c,X 499> Å È‹ ß 9A’ n2Ï4³?š ÒÄsystem view Å û ã 16 MB È îA±0NKÈ Äsession Å,X û ã 48 MBÄ?• base\ntos\mm\mi.hX 8 261~8 317 > ÅÄîA±0NKÈ,È y ! b 0xc0000000 ß,X 48 MB ÈG 0xbd000000~0xbfffffffÄ¢ mminit.c ,X 582> Ô,È 754> È Au1k îA±0NKÈ `2Ï4³?š Ò,X Y , !5B È Au1k,X4§ p ¹ ž Í h,X Ô o < ¬G£ V Ò 4.12 / Ä ü Ò È îA± ô £ [Ê Ù À win32k.sysÃ?šNePE |/ß c ¹ ž Ô o ' DPE |/ß c,X ô £ [Ê × îA± Y ,"4 Û 2 b îA±0NKÈ,X 6NI Y ,"4 Ä

y ß 9 MmInitSystem Ñ D ñ Ÿ ê2Ï4³4ç ,,X !5B È MmSystemCacheStart þ Æ ñ Ÿ ê,X < ¬G£ È 0xc1000000Ä2Ï4³4ç ,,X4§ 3 !5B 0xe1000000 È cMM_SYSTEM_ CACHE_END Ù ÿ!8 Ä' â 6NI Y ,"4,X ¬G£A’5B È MmPagedPoolStart X ñ 0xe1000000 Ä 6NI Y ,"4,X û ã MmSizeOfPagedPoolInBytes È5¬Ax 32 MB È âM6E¬?U Í WE¯> A× H Ä

' âAu1k2Ï4³ PTE,X DG£ Ä?• mminit.c,X 1 173~1 287> Å Ä MmInitSystem B2Ï 4³ Ã*üNIM6,X DG£ È Í MmNumberOfSystemPtes < ¬G£E¯> C È Ô å 7 000 þNIM6 È Ô î 50 000 þNIM6 Ä V p?U ”P`PE |/ß c,XA± ÈE¬LÔ?UNq ê,X2Ï4³ PTE Ä?• mminit.c,X 1 282~1 287> Å Ä



Ò 4.12 îA±0NKÈ `2Ï4³?š Ò,X Y , × 4§ X

y- ñ Ÿ ê â Ú Y ,1u)Ú Ý G,X < ¬G£ Ä' â Ý Ô þG¡?U,X Ñ DA×*ü Ö MiInitMachineDependentÄ!8 Ñ D,X ?U s6Ñ È,ó!7A} Windows,X<. ³ Y ,E¤E@CK 9 È !M6 Ÿ4¡,X MmInitSystem Ñ D .,X ¹0 ¾ ü æ Ú<. ³ 0NKÈ È J"u Ý,ó!7 Î0ŸNI,Â)NM `NI><Ä5à MiInitMachineDependentó!7 Î0ŸNI,Â) È¹ ž Î0ŸNI>< 9 ô Ø Y Ø þ ³ Ä(M ÿ ÈM2 6NI Y ,"4 3 ü!8 Ñ D ñ Ÿ ê,X Ä G bA¹ Ñ D È å À/á âA°4š Ÿ4¡ Ä

' â MmInitSystem Ñ D ñ Ÿ ê C³ (=) Ú Y , , Ì G , X < ¬ G £ Ä O j A × * ü MmInitializeMemoryLimits9‹ k Ý G(=)Ú Y ,,X Î µ C Ä Z • " 1u)Ú(=)Ú Y , È2Ï 4³ S*ü Ô þC‡ ó û,X ! Ò 9A„)(=)ÚNIM6,X Ý û Ä ü ` ä Z Y , Î ñ Ÿ ê ¹ â È MmInitSystemA×*ü MiReloadBootLoadedDriversÑ D È Ú ntldr tEQ,X é Ð- |PE |/ß c G¡ n ! 2Ï4³ PTE ³ È ´5à W À 36Ñ k NIM6 ,X ± x È J Ý Ã6Ñ>• 6NI Ä

y ß 9 B Ã*ü(=)ÚNIM6,X DG£ 9.B n2Ï4³ Y ,,X?˜ õ Ê ,X?˜ í È ã b 19 MB È íAx ã2Ï4³ Ä Í b ¹ 00-5à?Ô È ü 19~31 MB KÈ È íAx 1 ?˜ õ2Ï4³ × û b1

Windows *Y s)Ú â r)„*

b 32 MB È íAx û2Ï4³ Ä Í b á u <5à?Ô È ü 19~63 MB KÈ È íAx 1 ?˜ õ2Ï 4³ × û b1 b 64 MB È íAx û2Ï4³ Ä º ê ÈMmInitSystem 3A'5B Ô4˜ < ¬G£ Ä?• mminit.c ,X 1 554~1 676> Å È Ù À MmMaximumDeadKernelStacks MmModifiedPage-Maximum Ã MmSystemCacheWsMinimum MmDataClusterSize MmCodeClusterSize MmReadClusterSize MmInPageSupportMinimum MmFreedExpansionPoolMaximum Ä E- o < ¬G£*ü b { 2Ï4³0NKÈ Ô o(M!^*üEè,X(=)Ú Y ,NIM6,X DG£ ê5Ù Þ ßL$ Ä' â ÈA× H Ã*ü(=)Ú Y ,NIM6,X DG£ È G < ¬G£ MmResidentAvailablePages¢ ' ! Ã*ü NIM6 DG£ £] 32 þ ±+-NIM6 Ä1 717 > Å È a £]M2 6NI =) LÔ?U,XNIM6 D Ä1 725 > È2Ï4³ | Ê(=)ÚNIM6 D,X 1/6 È Ô î áCYE› 256 MB Å ÈE¬?U £]2Ï4³4ç , 4*ü,X Ô å(=)ÚNIM6 D Ä1 731> Å Ä

' â MmInitSystem Ñ D Î0ŸCK2Ï4³4ç ,4§ X Ä1 761~2 037 > Å ÈE- J ,X ûF¼ Ú · -ÕFÑ ü Ø)Ú î4{NI><Ä Ý4{ ê ¯4{ ÅÈ 1T êCK?• Èå À ¾5×<% Intel x86,X `4{NI>< Ä ü WRK È 2 Ï 4 ³ 4 ç , 4 § X , X 0xc0c00000 Ä < ¬ G £ MmSystemCache-WorkingSetList Å È5à2Ï4³4ç ,,X 0xc1000000 Ä < ¬G£ MmSystemCacheStart È ø5Ù KÈ!7 Q Â 4 MB È ¹ ÈE- ø þ ,X PDE!7 Q ,ÌF•,XÄ?• 1 843> ,X ASSERTÅÄ 2Ï4³4ç ,,X Ô û Ã6Ñ 0xe1000000È rL Þ J,ó!7,X4§ 3 Ã6Ñ î ã Ô o È ´ 5à2Ï4³4ç ,,X Ì á î Ý 0xe1000000~0xc1000000 w û ÄAÏ5Ù Ã ¹ ü MmInitSystem Ñ D C³Cþ MaximumSystemCacheSize X ¬ ê ™ ‰ ÄAu1k k MmSystemCacheEnd` MmSizeOfSystemCacheInPages â È Ã ¹ E-F¼ Ú0NKÈ ÚG!NI>< Z Ä"¼ ã ÈE-G ™ ™ ÚG!NI><5àM2NIM6 Å Ä Ô âA×ÑMiInitializeSystemCache ñ Ÿ ê2Ï4³4ç , È+ WBóB÷ ñ Ÿ ê2Ï4³4ç , ¹ 0Lš È J Î0ŸCK,Ì h,X1u)Ú D B4§ X Ä G b2Ï4³4ç ,0NKÈ,X Y ,1u)Ú ÈAË – 5× 7.2.18V Ä

7Ç!8 ÈMmInitSystem Ñ D Æ4£ Î Þ n Q2Ï4³0NKÈ Z È J è ` ä Z ñ!9,X ñ Ÿ ê ¹ 0 Ä)„ üA'5B < ¬G£ MmTotalCommitLimit Ô þ,ó!7 Ý ã ,X È W ·>< Z Ô î Ã ¹ ¤ x,X Y , DG£ È G Ô î Ã ¹ %)„ î å(=)Ú Y , Ä º ê È < ¬G£ MmTotalCommit-LimitMaximum 1 b MmTotalCommitLimit Ä ¹ 0Lš,XP¬L$ MmMaximumWorkingSetSize Ã*üNIM6 D £ • 512 È " W á Ã6ÑCYE› 2 GB Ä

' â MmInitSystem A×*ü MiBuildPagedPool Ñ D È Î0ŸCK 6NI Y ,"4 Ä ü Î0Ÿ Z 6NI Y ,"4 ¹ â È Ã ¹ ñ Ÿ ê Æ tEQ,X õ +>< Z Ä ´ LÔ?U+ AË 6NI Y , Å Ä ^E- o õ + ô Ø 2Ï4³0NKÈ ÄE- EîE›A×*ü MiInitializeLoadedModuleList Ñ D Ä2 099 > Å 9 ` ä,X Ä

Ô â È8¹ Ã*ü(=)Ú Y , ¡' CYE› 127 MB È í r t È î,X2Ï4³ PTE ÈA}M2 6NI ³ â

ÏÄ 2 139~2 176> ÅÄ â ËBñ Ô ÑNI,Â) È¹ “ Ú 9 ûNIM62Ï4³ PTE ô Ø>• ôL8 ÊÄ ¥ *ó ü MiUnmapLargePages Ñ D Å ÈE¬ Ã ¹ 6 á s Ÿ,XNI,Â)NM Ä

ü MmInitSystem Ñ D,XL !‰ 0 ñ Ÿ êF¼ Ú È Ý,Ì ' ÔF¼ Ú ¹ 0 ü MiInitMachine-DependentÑ D ` ä,X È Ù ÀM2 6NI Y ,"4,X ñ Ÿ ê ¹ 0 ` PFN D B g,X ñ Ÿ ê Ä Z)Ú?·(=)Ú Y ,,X ñ Ÿ ÚG! ™ ‰ È Ý ™?U,ß Ô ßE- þ Ñ D È J ··Õ ! b base\ntos\mm\i386\ init386.c,X 762~3 568> Ä+ b!8 Ñ D,X ··ÕEW î ÈE-G ¾ Ÿ4¡ â2Ï4³0NKÈ ñ Ÿ ê,Ì G,X ··ÕF Ee Ä J è È 1T “CK?• È ü ßM6?·Gž ··Õ,XE›/ß È Ú á5×<% â MmVirtualBias ¬ G£M2LÊ Ä G/3GÆ ÐEÝNM Å Ã64(ÃPAE Õ `M2 Í/Ä Y , õ _,Ì G,X ··ÕF Ee Ä

ü 854~973> ··Õ È MiInitMachineDependentØ)Ú ûNIM6 Õ Ã ¬G£ ñ Ÿ ê È ¹ ž*ó äNI,Â)NM `NI><NM,X õ S Ä' âA’5B ' !E¯/ß,XNI,Â) È ··Õ V ß Ö

```
PointerPte = MiGetPdeAddress (PDE_BASE);
PdePageNumber = MI_GET_PAGE_FRAME_FROM_PTE (PointerPte);

CurrentProcess = PsGetCurrentProcess ();

DirBase = MI_GET_PAGE_FRAME_FROM_PTE (PointerPte) << PAGE_SHIFT;

CurrentProcess->Pcb.DirectoryTableBase[0] = DirBase;
KeSweepDcache (FALSE);
```

E-G å À á5×<%PAE ™ 6 ÈKeSweepDcache þ0NAÁ ¹ È ” 3 á . Ä c MI_GET_ PAGE_FRAME_FROM_PTE È y ¢ PTE ¤ ª Î W,XNI û4ê Ë È G(=)Ú Ä ´!8 ÈE¯ /ß ÍB5,X KPROCESS4§ X,X DirectoryTableBase[0]„) ZA¹E¯/ß,XNI,Â)(=)Ú Y , Ä y ß 9 1 020~1 023> ··Õ ^NI,Â)>< Í h b 0~2 GB KÈ,XNI,Â)NM m äLÊ È ã G-' !E¯/ß Ä G0NKÆE¯/ß Å á S*üE-F¼ Ú0NKÈ Ä

' â MiInitMachineDependent B ntldr ôEæE¯ 9,X G b(=)Ú Y ,,X £EÄ0úJÒ>< LOADER_PARAMETER_BLOCK::MemoryDescriptorListHead X µ C È" Î(=)Ú Y ,NIM6 ,X DG£ È ¹ ž0NKÆ(=)Ú Y ,,X Ô " Ä?• 1 030~1 083> Å ÄE- k < ¬G£ MmNumberOfPhysicalPages ` MmLowestPhysicalPage X Ä y - È A ' 5 B < ¬ G £ MmDynamicPfn ` MmHighestPossiblePhysicalPage È G ÔP¬ Ã*ü,X(=)Ú NI4ê Ë ` ÔP¬ Ã6Ñ,X(=)ÚNIM6 Ä âA× H < ¬G£ MmSizeOfNonPagedPoolInBytes MmMaximumNon-PagedPoolInBytes È GM2 6NI Y ,"4,X û ã ` Ô û Ì Ä1 281~1 489 > Å Ä

y ß 9 ¢ 1 499> ··Õ Ô Ÿ È Oj 9‹ k*ü b(=)Ú Y ,1u)Ú,XEY }Np8F ž J }-Õ È G < ¬G£ MmSecondaryColors ` MmSecondaryColorMask Ä âAu1k PFN D•LÔ?U,XM2 6 NI Y , ÔJÔ MxPfnAllocation Ä+ bM2 6NI Y ,"4 ¢P¬ å " • åAu1k,X È5àM2

6NI"4,X4§ 3 MmNonPagedPoolStart b 0xffbe0000 È¹ È JCK Ÿ MmNonPaged-PoolStart 4§ 3 £ • Ô û Ã6Ñ,X MmMaximumNonPagedPoolIn- Bytes t Þ ' ! û ã ÈG MmSizeOfNonPagedPoolInBytes• ··Õ 1 589> ÅÈ â Í MmNonPagedPoolStart . ÍU$A× H Ä?• 1 628> Å Ä

ü Windows2Ï4³0NKÈ,X Y , × È2Ï4³ PTE ³ ! bM2 6NI Y ,"4,X2û !M6 È < ¬G£ MmNonPagedSystemStart) Z2Ï4³ PTE ³,X Ô Ÿ È+ b2Ï4³ PTE ³ ` M2 6NI Y ,"4 ø5ÙFÑ á Ã ¹>• 6 Î ê , ,X È ¹E- øF¼ Ú,XNI><FÑLÔ?U ü ñ Ÿ ê,X Ê í Î0Ÿ Q ÄOj Au1k MmNonPagedSystemStart !5B Ä?• 1 730> Å È!8 á k " b MM_LOWEST_NONPAGED_SYSTEM_START È G 0xeb000000 Ä?• 1 734> Å Ä º Ô • M6 È V p 6NI Y ,"4,X4§ 3 !5BC^E› Z2Ï4³ PTE ,XCK Ÿ !5B È íLÔ?U Í 6NI Y ,"4,X û ã 0A× H Ä?• 1 744~1 800> ··Õ Å Ä' â È " ¹ Y ô £ ` HAL ô £ ú Ã ¹*ü ûNI M6 ô Ø È V p$µC‡ 5 Ê È í Í W À S*ü ûNIM6 ô Ø Ä?• ··Õ 1 808~2 033> Å ÈA„) ü MiLargeVaRanges< D4˜ Ä

y ß 9 Ô Ÿ ÚG!(=)Ú Y , È5×<% PFN D B g `M2 6NI Y ,"4 LÔ?U,XNIM6 Ä?• 2 048 > ··Õ ,X PagesNeeded+G£ Å Ä Ã6Ñ S*ü ûNIM6 ô Ø È V Ý ™?U È £ ãM2 6NI Y ,"4 ,X û ã ¹ "6Ñ ÍU$ ûNIM6 Ä4 MB ÅE•+ Ä PFN D B g,X !5B Ä < ¬G£ MmPfnDatabase Å Ø b Æ tEQ,X ô £ Ä Ù À Y Ã HAL 1 Å Þ È J è ÍU$ ûNIM6E•+ Ä V p ¢ PFN D B g Ô Ÿ !5B Ô,È 2Ï4³?š Ò KÈ,X<. ³ 0NKÈ áC‡ ¹ •4‡ LÔNIM6 DG£ È í,Ì h £ ãM2 6NI Y ,"4 Ä?• ··Õ 2 080~2 101> Å Ä 2 133~2 225> ··Õ,ó!7 ¢(=)Ú Y , £EÄ0ú4§ X MxFreeDescriptor È 7L8 PFN D B g `M2 6NI Y ,"4 LÔ?U,XNIM6 ÈA„ ) ü F¼ ¬G£ FirstPfnDatabasePage PagesNeeded È J èE-F¼ Ú0NKÈ ÍU$ ûNIM6E•+ Èt 9 ûNIM6 ô Ø D 4 ˜MiLargeVaRanges Ä A „ ) M 2 6 N I Y , " 4 C K Ÿ , X < ¬ G £ MmNonPagedPoolStart Lc È „ 2ûC³ ü PFN D B g âÄ?• ··Õ 2 235> Å Ä 2 284~2 307 > ··Õ ' PFN D B g `M2 6NI Y ,"4 á S*ü ûNIM6 ô Ø ÊM2 6NI Y ,"4,X ÚG!F Ee Ä

y ß 9 2 320~2 337> ··Õ,ó!7 ÚG!2Ï4³ PTE ` =),XM2 6NI Y ,"4 8× È,XNI ><Ä ··Õ V ß Ö

```
StartPde = MiGetPdeAddress (MmNonPagedSystemStart);
EndPde = MiGetPdeAddress ((PVOID)((PCHAR)MmNonPagedPoolEnd - 1));

while (StartPde <= EndPde) {

  ASSERT (StartPde->u.Hard.Valid == 0);

  //
  // Map in a page table page, using the
```

```
  // slush descriptor if one exists.
  //

  TempPde.u.Hard.PageFrameNumber = MxGetNextPage (1, TRUE);
  *StartPde = TempPde;
  PointerPte = MiGetVirtualAddressMappedByPte (StartPde);
  RtlZeroMemory (PointerPte, PAGE_SIZE);
  StartPde += 1;
}
```

üE-!‰ ·-Õ ÈOj .B n ¢ MmNonPagedSystemStaô Ÿ MmNonPagedPoolEnd – 1 ,X 8× È Í h,XCK Ÿ `4§ 3 PDE ÖStartPde ` EndPdeÈ' â Ú ÿ ? J ,X!£ Ô þNI ,Â)NM ÄMxGetNextPageÚG! Ô þ(=)ÚNI È¨ ² JNI û Ë È TempPde ,X PageFrameNumber ? Q ¹ â È G>•C 4- StartPde Í h,X PDE ÄMiGetVirtualAddressMappedByPteÑ D Ä r L Þ Ô þ C AÁ?Ô c Å,X s6Ñ È B Ô þ PTE NM,X ÄE-G ^ StartPde' . Ô þ PTE 9,ß Y Å ÈAu1k Î Í hNI><,X<. ³ È 3 AÈ È9‹ k î î ÚG!,XNI><,X<. ³ È ¢ 5à Ã ¹ ñ Ÿ ê!8NI>< Ä ? LÊ Å Ä MiGetVirtualAddressMappedByPt,XF Ee \1T) È º/ï 10 ! È ÈE-G rL Þ*ü Z Ô þA'Au T » È ßM6,X ¦ 9 [?·Gž ZE- Ô Ä

Windows ,XNI,Â)7¾ ô Ø •

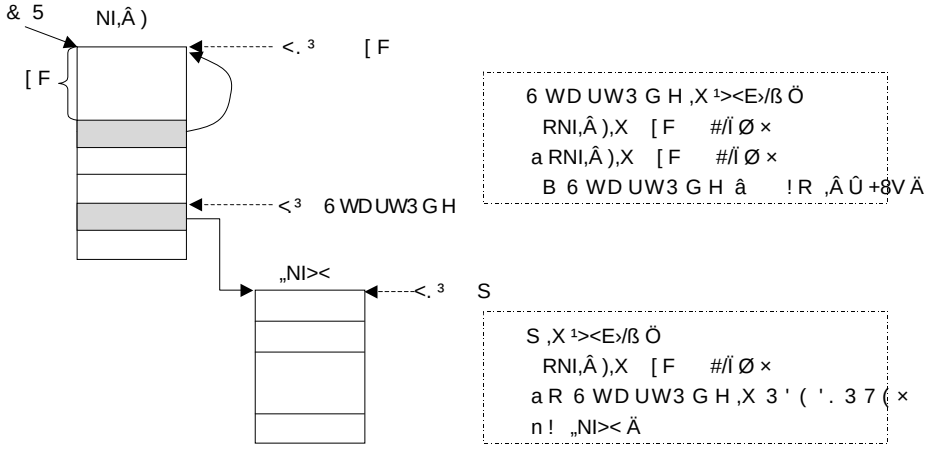
Windows Ó š o % ¸ < o ´ ‰ 8 v • É À 9 — ¥ â ^ 8 N » t À 9 0 0 Ó š ¶ ‡ H • Ý ò / MxGetNextPage² M Š Q š K ¡ ' < ¶ PDE ä PTE 8 ì¾ A , £ } ^ 8 š © Ü PFN i â ‡ Q ¥ ¶ » À 9 ® š K d Intel x86 • É À 9 ' < ¶ f ± ¶ õ Î Í 4.3 d É ¯ • ± ¶ ´ ~ Ú ¿ , ³ š K d £ } A , ÿ ¡ Windows š , Ã ä š ¶ r " å ° ã ¢ © ¶ Q ™ Ä (: Ò ä ¬ d

Windows š , Ã ‡ PDE n } Ý ò / PDE_BASE¾ 0xc0300000 PTE o ³ ¾ 0xc0000000 } Ý ò / PTE_BASE É ¯ Intel x86 h PDE ä PTE r ¶ » ¾ - ½ Î 4.4.1 M í d t ø } ¢ Q š ¶ É Ü c / • Â Œ Î • ' } š , Ã / ™ ¦ ¢ Q PDE ‡ 4 s q *StartPde = TempPdeÑ ³ ¹ Æ c ± ' Ÿ t » ¥ º´ ÿ À 9 ® š ¶ d ¬ • h s š , Ã / PDE ‡ † À 9 ™ ' < ¶ f ± ¶ ‡ 4 s / q*StartPde r c ¬ ¸ < } À 9 š , Ã š K • t d

PDE ¶ ¾ T l CR3 — É v ä ¥ : 10 * ÿ ò G Ù ® ¢ ê CR3 — É v ¸ < " • ¢ ± ¶ ¬ ¸ ò G d ' Ï ¾ • ± ¶ dWindows ³ t ¢ Q ¦ S • ™ þ ¢ Q š ¶ ³ 4 MB Ö Ì n v 5 r ° s š ¶ š K À 9 ¶ F h

¢‰ s Q ä ¥ ÿ ý { ‡ T l PDE g PTE ¥ ÿ ý { Q N ^ 8 š K
¥ MiGetVirtualAddressMappedByPte g MiGetVirtualAddressMappedByPde d

º # ¾ ã , ! ¬ • š ¶ PDE ¥ ¸ ‡ H • Ý ò / StartPde t r • š ¶ š K ¥ A , ã , • ™ f ± ¶ ! ¢ ± Ó š , Ã ‡ † š K " • ± Ó 0 0 ™ ¦ Š Q PDE ¬ • h ã ± ' < PDE ò ³ PTE ÿ ¡ à d n ã ¢ ¾ A , þ ã , ¥ ! « : 10 * 0 š , Ã ¥ : 10 * - ½ å ¢ Q PDE [® ¨ Ñ • ÿ 10 * ë ¾ StartPde 0 š , Ã n · , » 4 ‡ f à · PDE ô h d š , Ã 0xc0300000 « : 10 * 0 % , 10 * [¾ 1100000000b N » StartPde ° - 10 * ~ Ú 0 ì " þ f Q ¨ Ñ d ã þ ¾ MiGetVirtualAddressMappedByPtë ® Å æ P Ù É ¯ PDE_BASE Ü 0xc0300000 ™ ° å ¢ Q PDE ° - 10 * » c s ë PDE ö â - d Í 4.13 ¡ µ t š , Ã 0 š ¶ · ' , _ É š , Ã / 1100000000b » ¥) % 768 ¿ š , Ã ‡ † d Í / Ó ¹ f µ t StartPde ´ ¢ Q PDE » ƒ p ´ ¢ Q š ¶ š K g Ò ¶ Q d ` à ¶ » ' û r 0xc0300c00 / š © Ü 0 CR3 — É v / š © Ü ¾ - ½ d ¬ • h ¶ ã : A , ™ ¶ » ¡ { ¢ ê ò G t 0xc0300c00 ´ š , Ã » ü Q ¥ Â · N š ¶ ' ö * 0xc0000000~0xc0400000 · d



Ò 4.13 Windows NI><<. ³ n !/ ã Ò

ã 5 º # ' Ï ‰ } š , Ã 0xc00 » ¿ Q ' • É ¯ PDE ä PTE L ´ ¾ ¹ N » š , Ã / $ ¢ Q PDE } À 9 š ¶ š K ¨ ™ „ ò ³ PTE ÿ ø } d Ù ® ã 5 º # „ K š , Ã ' ø } º # d

) ¢ ä ¶ » × œ } • ‰ š ¶ r / ¶ å ¢ ‰ PTE [¶ » F ½ , ° - * º
¥ f c N ^ 8 š K ¥ d H " } Í 4.13 / s š ¶ / å ¢ Q PTE
Q N ^ 8 š K ¥ [½ , ¶ » MiGetVirtualAddressMappedByPte ¥ ¬ £ d È
` à ' û r d ® ó MiGetVirtualAddressMappedByPde ¬ £ W ¦ t ò Ü PDE
° - 20 * Ý ¶ t Q N ø } ¥ o ³ * " Ö Ì 4 MB d

y ß 9,X ··Õ 2 341~2 484 ÚG! PFN D B g `M2 6NI Y ,"4 ÈÔ,È 2Ï4³?š Ò Ô Ÿ ØE-!‰ 8× È,XNI>< È V p üM2 6NI Y ,"4 â2Ï4³?š Ò KÈ Ý0NLm Ä7Ç å • k ß Ô þ PDE È G 4 MB û ã Å È íE-!‰0NLm*ü .Nq ê,X2Ï4³4ç , `2Ï4³ PTE Ä –?• 7.2.18V Å Ä !8 ê È V p 1 GB~2 GB 8× È 3>•*ü .2Ï4³0NKÈ È í Û n,X8× È È ¢ MiUseMaximum-SystemSpace MiUseMaximumSystemSpaceEnd È ÚG!,Ì h,XNI>< Ä"¼ ã ÈE- ø þ < ¬ G£ üMmInitSystem Ñ D Æ4£ B2Ï4³,X é Ð – D5àC Z Ä

Windows ü2Ï4³ 0NKÈP¬0Ã Ø ±+- Z Ô + 8× È*ü .2Ï4³ ý$W Ê,X µ CE@ | ³ È JCK Ÿ 0xffbe0000 È2 497~2 509> ··Õ E- + Y , Ä áCYE› 4 MB Å ÚG! Z Ô þNI>< Ä

y ß 9 ¢ 2 515 Ô,È 2 564> ··Õ È M2 6NI Y ,"4 ÚG!NIM6 ÈE- oNIM6 !M6 Æ4£ NX+- Z È J èNI û4ê Ë E²4Á,X Ä â ü 2 579> A×*ü MiInitializeNonPagedPool Ñ D Î0Ÿ CKM2 6NI Y ,"4,X1u)Ú4§ X È ü 2 581> A×*ü MiInitializeNonPagedPoolThresholdÑ DA' nM2 6NI Y ,"4,XP¬ Ã "KÜ Ä

' â ÚG! PFN D B g LÔ?U,X(=)ÚNIM6 Ä ü S*ü ûNIM6,X ™ ‰ ß ÈE- oNIM6 !M6 Æ 4£NX+- Z È¢ FirstPfnDatabasePage Ô Ÿ È E MxPfnAllocation þNIM6 È• ··Õ 2 590~2 624 > Ä ü á S*ü ûNIM6,X ™ ‰ ß È LÔNIM6 î þNX+- È LÔ?U ±A• !£ Ô þ(=)ÚNIM6 Í h Ô þ MMPFN 4§ X Ä J n ?• base\ntos\mm\mi.h È E 24 þ +8VKS Å ÄPFN D B g rL Þ Ô þ ! b Y ô £ â,X MMPFN D4˜ È ¹ ÈE-F¼ Ú ··Õ !8 D4˜ ÚG!(=)ÚNIM6 È?• ··Õ 2 628~2 728> Ä

y ß 9 2 752~2 783> ··Õ È ÝNp8F,X0NKÆNIM6JÒ>< D4ÑmFreePagesByColor D• Ä JM2JÒ>< Å ÚG!(=)ÚNIM6 J ñ Ÿ ê J YF¼JÒ><4§ X ÄE-GMmFreePagesByColor D4˜*ü b 1u)Ú(=)ÚNIM6 È –?• 4.5.38V Ä

2 790~2 900> ··Õ Ý ÆA'5B Ý Ävalid Å,XNIM6 È È „ Ô ß Í h,X PFN D B g 2ô,X(Š Õ ÄE- 31k PFN D B g,X ñ Ÿ ê ÈE- È(=)ÚNIM6,X ÚG! "C³ PFN D B g ,X(Š Õ Í hCK 9 Z Ä

y ß 9 ” ¹ Ô ",X(=)Ú Y ,NIM6 È,ß W ú 0 È V p 0 J è ' ! î þ>• S*ü È í Ú W ÛA„ Æ4£ ü S*ü ÄE- . Z ¹ R (=)ÚNIM6>• Û n LÊ ,XEC ÊJíAÃ Äbug Å , ?• ··Õ 2 908~2 928> Ä

¢ 2 964> Ô Ÿ È B2Ï4³ tEQ/ß c ôEæE› 9,X(=)Ú Y , £EÄ0úJÒ>< È ” ¹ Ý,X Y , £EÄ0ú È J ^ Ã*ü,X Y ,FÑ t 9 PFN D B g,X0NKÆJÒ>< Ä+ b tEQ/ß c ôEæE› 9 ,XJÒ>< ¢ " P¬ f c,X È5àE-G ,X ~)ƒ ” ¹ Ý,Ì ¡,XNN c È´5àP¬ ,X Ã*ü (=)Ú Y , ¦ 9 0NKÆJÒ>< È" ,X Y , â ¦ 9 JÒ>< ÄE-/¡ ."©,X5×<% È2Ï4³ î Ô Ÿ Ê ÚG!,X Y , á þ Ã6Ñ>•Gž È´5à " ,X(=)Ú Y ,Ä!¨ V Ô ",X 16 MBÅÃ¹ ¤ o(M!^,XA’ Û êPE |/ß c S*ü Ä

y ß 9 ? £ PFN D B g *ü ,X PTE È J ^ W À Í h,XNIM6 ÛA„ Æ4£ ü S*ü È G ü D B g Ú é*üAu D t 1 Ä ··Õ?• 3 105~3 239> Ä

' âA×*ü InitializePool Ñ D ñ Ÿ êM2 6NI Y ,"4 È?• ··Õ 3 263> Ä7Ç!8 ÈM2 6NI Y ,"4 Æ4£ Î0ŸCK 9 È Ã o S*ü Z Ä

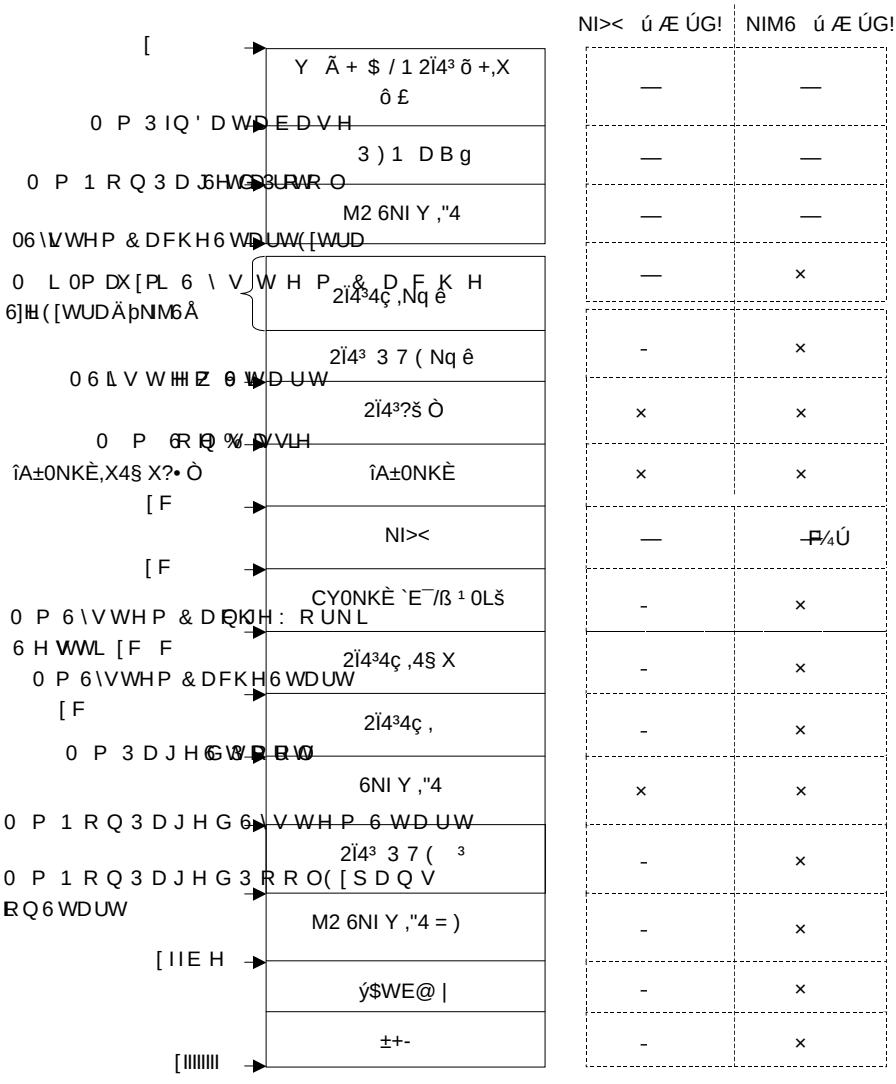
y ß 9 ñ Ÿ ê2Ï4³ PTE"4 ÈE- o PTE ?U*ü b ô Ø I/O 0NKÈ ÃPE |/ß c,X ô £ È ¹ ž Y Ü Ä2Ï4³ PTE "4,X8× È ¢P¬0Ã,XM2 6NI ³ Ä+ < ¬G£ MmNonPaged-SystemStartÛ n Å È Ô,È P¬0Ã,XM2 6NI Y ,"4 Ä0xffbe0000 !M6,XFw Ô!‰M2 6NI Y ,"4 Å ÄE-!‰ 8× È 2Ï4³ PTE ³ Ä ü ··Õ 3 295> A×*ü MiInitializeSystemPtes Ñ D Í2Ï4³ PTE"4E¯> ñ Ÿ ê Ä

V p !M6 ü ÚG!<. ³ 0NKÈ Ê Æ4£ ÚG! ZNq ê,X2Ï4³ PTE ³ È í ÚNq ê,X ³ t 9 2Ï4³ PTE"4 Ä?• ··Õ 3 302~3 346> Ä

Ô â Èñ Ÿ ê ' !E¯/ß,X Y ,1u)Ú4§ X È J Î0ŸCK ¹ 0LšJÒ>< È-#] ž ï Î Ô þ PDE 9 ô ØCY0NKÈ Ä ! b 0xc0400000 Å È J ñ Ÿ êA¹ PDE Û,XNI>< Ä?• ··Õ 3 359~3 379 > Å ÄCY0NKÈ Î0ŸCK 9 ¹ â È ñ Ÿ ê,Ì h,X ¬G£ È Ù ÀCY0NKÈ 1u)Ú PTE ,X < ¬G£ È ¹ žE¯/ß,X ¹ 0LšJÒ>< Ä?• ··Õ 3 385~3 390> Å Ä' â LÊNIM64“/ß ±+-*ü bLÊ ê ¡ 0 ,X PTEÄ?• ··Õ 3 396> Å Ä y- E¯/ß ï Î VAD ! Ò Ä?• ··Õ 3 412~3 430> Å È G b E¯/ß 0NKÈ,X VAD ! Ò ÈÆË –5× 4.3.28V Ä â È'5BNI,Â),X PFN 2 ûÄ?• ··Õ 3 475~3 480 > Å È ¹ ž ¹ 0LšJÒ>< ÚG! Ô þNIM6 Ä?• ··Õ 3 500~3 514> Å È' â ÈA’5B ¹ 0 Lš,X 2 û Ä?• ··Õ 3 524~3 528> Å Ä Ô â È ^1u)Ú Y , LÔ?U,X(=)ÚNIM6 ÛA„ Æ ü S *ü Ä?• ··Õ 3 534~3 565> Å Ä

7Ç!8 ÈMiInitMachineDependentÑ D ` ä J ñ Ÿ ê ¹ 0 È JE¨ ² Ä

4£E› ZL !‰ 0 ñ Ÿ ê ¹ â È B MmInitSystem ` MiInitMachineDependentø þ Ñ D .,X _ ™ È2Ï4³ 0NKÈ,X ñ Ÿ ê Æ4£ ` ä Ä J × 4§ X Æ ` < Î0ŸCK 9 È5à è ÈM2 6 NI Y , ³ Æ4£ ÚG! QNI>< `NIM6 È ` H,X Y ,4§ X V Ò 4.14 / Ä Ý G,X < ¬G£ V ><4.2 ë È>< 34- Î Z ü Windows Server 2003 SPÔ þ L _2Ï4³G!5BÄ512 MB Y , Å ßE- o ¬G£,X Ä



Ò 4.14 2Ï4³ 0NKÈ,X Y , × 4§ X

><4.2 Windows 2Ï4³ *ü b2Ï4³0NKÈ1u)Ú,X Ô o < ¬G£

< ¬G£ á	L _ ª	< ¬G£ á	L _ ª
MmHighestUserAddress	0x7ffeffff	MiSessionImageStart	0xbf800000
MmUserProbeAddress	0x7fff0000	MiSessionImageEnd	0xc0000000
MmSystemRangeStart	0x80000000	MmSystemPteBase	0xc0000000
MmPfnDatabase	0x81000000	MmWorkingSetList	0xc0502000
MmNonPagedPoolStart	0x81301000	MmHyperSpaceEnd	0xc0bfffff
MmNonPagedPoolEnd0	0x82000000	MmSystemCacheWorkingSetList	0xc0c00000
MiSystemCacheStartExtra	0x82000000	MmSystemCacheStart	0xc1000000
MiMaximumSystemCacheSizeExtra	0x2f800	MmPagedPoolStart	0xe1000000
MiSystemViewStart	0xbb000000	MmPagedPoolEnd	0xf0bfffff
MmSessionBase	0xbc000000	MmNonPagedSystemStart	0xf0c00000
MiSessionPoolStart	0xbc000000	MmNonPagedPoolExpansionStart	0xf8ba0000
MiSessionViewStart	0xbc400000	MmNonPagedPoolEnd	0xffbe0000
MiSessionSpaceWs	0xbf400000	MmNumberOfPhysicalPages	0x0001ff7a

)„ ü å À 9,ß Windows 2Ï4³,XL !‰ 1 ñ Ÿ êE›/ß È J Y ,1u)Ú,X ñ Ÿ ê 3 ü MmInitSystem Ñ D ` ä,X È?• base\ntos\mm\mminit.c¢ Ê ,X 2 211~2 389> ·-Õ Ä MmInitSystem a õA×*ü MiInitMachineDependent Ñ D ÈáE› ÈE- õ MiInitMachineDependent Ñ D ¾ . Z \1T),X Ô&• _ ™ Ä?• base\ntos\mm\i386\init386.c¢ Ê ,X 863~870> · -Õ Å È G È V p Ø)Ú < Õ ûNIM6 È J è ü !M6 ñ Ÿ êE›/ß ÝA„) ß 9?UE@ 6 ä ûNI M6,X Y , ³ Ä ü < D4˜ MiLargeVaRanges Å È í ^E- o ³E@ 6 ä ûNIM6 ô Ø È J Ã6Ñ Ù À,X ³ Y D•,X ô £ Ä Ù À Y ` HAL Å ÃPFN D B g È ¹ žM2 6NI Y ,"4 Ä

' â ÈMmInitSystem A×*ü MiMapBBTMemory Ñ D È!8 Ñ D,X*ü ã BBT ÄBasic Block ToolsÈ Ô/¡ ·-Õ ì ê T ÅNX+- Ô + Y ,4ç † Ä+ b üT¬AxG!5B ß È < ¬G£ BBTPagesToReserve 0 È ¹ ÈB Ñ D rL Þ ” 3 á . ÈÈ yE¨ ² Äy ß 9 MmInitSystem A×*ü MiSectionInitialization Ñ D ï Î Y , ÍB52O _ È ï Î!‰?· é*ü2Ï4³4“/ß Ädereferencing segment threadÈ ¹ ž ï Î Y , ÍB5 \\Device\\PhysicalMemory È a ¦9 ' !E¯/ß ÄSystem E¯/ß Å ¹ ˜>< Ä

y ß 9 MmInitSystem ¢ 6 N I Y ,"4 + A Ë Ô PTE ÍB 5 È + < ¬ G £ MmSharedUserDataPtê å!8 PTE ÍB5 ÄA¹ PTE A„) Z*ü E • D BNI,X PTE È Í h,X NIM6 ü Y ` ;> ' ñ Ÿ ê ¹ ! Æ ÚG! Q È ! b 0xffdf0000 Ø ÄE¯ Ô!9 È ^A¹ PTE C

E¯/ß 0NKÈ,X 0x7ffe0000 Í h,X PTE ÈE- r)„ Z ü 0xffdf0000 ` 0x7ffe0000E- ø þ ô Ø à Ô þ(=)ÚNIM6 Þ Ä´5à ÈE¯/ß 0NKÈ `2Ï4³ 0NKÈ E • à Ô þNIM6 È ¢5à*ü õ ã ··Õ Ã ¹A“KÂ2Ï4³ ,X Ô o(Š Õ D B Ä –5× KUSER_ SHARED_DATA D B4§ X Å Ä –?• ··Õ 2 236~2 289> Ä

' â MmInitSystem A×*ü MiSessionWideInitializeAddressesÃsMiInitializeSessionWs-Support ` MiInitializeSessionIdsÑ D ñ Ÿ ê îA±0NKÈ Äy- È MmInitSystem ï Î Ô þ2Ï 4³4“/ß È/Ä Â NIM6 m Î < Ä modified page writeÅ È?• ··Õ 2 299~2 310> Ä' â È ñ Ÿ ê2Ï4³ Y , _ Ê È Ù ÀP¬ Y , ` " Y , _ Ê È ¹ ž 6NI Y ,"4 `M2 6NI Y ,"4,XP¬ " _ Ê ÄE- + MmInitSystemA×*ü MiInitializeMemoryEventsÑ D 9 ` ä,X È?• 2 317 > ··Õ Ä

y ß 9 MmInitSystem | G > 5 L š 1 u) Ú < È E - ø þ 2 Ï 4 ³ 4 “ / ß È Ú ÿ KeBalanceSetManagèr KeSwapProcessOrStackÑ D Ä5Ù n ó ” ¹ J1u)ÚE¯/ß,X ¹ 0Lš × â5Ù { E¯/ß ` Y Ü,X 6 9 ` 6 Î Ä 0´ 4.5 ` 4.68V ÚE¯ Ô!9 Ÿ4¡E- ø þ4“/ß Ä

' â MmInitSystemA×*ü MiStartZeroPageWorkersÑ D È |LÊ êNIM6,X2Ï4³EY } 4“/ß Ä W À ™BóB÷ ü ñ Ÿ êL !‰LÊ êNIM6 ÅÄy ß 9 Ô þ ~)ƒ È Í Ý Æ tEQ,X õ + È A×*üMiWriteProtectSystemImageÑ D ¹A’5B ± x 2 û Ä?• ··Õ 2 362~2 382> Ä

7Ç!8 ÈL !‰1 ñ Ÿ ê ` ä È < ¬G£ MiFullyInitialized 5B ä 1 Ä

üL !‰ 2 ñ Ÿ êE›/ß È MmInitSystem ™ ™A×*üMiEnablePagingTheExecutiveÑ DÄ J ··Õ ! b base\ntos\mm\mminit.c 4 247~4 664> Å Ä!8 Ñ D S ' ! Æ tEQ,X õ + ,X Ã 6 N I ··Õ ¬ ä Ã 6 N I , X È W n ! !£ þ õ + ,XPAGE Y , È' â A × * ü MiEnablePagingOfDriverAtInitÑ D Ä J ··Õ ü base\ntos\mm\mminit.c 4 667~4 800> Å ¹ ¬,Ì h PTE ,X ÛA„ Äs 9,X PTE + 2Ï4³ tEQ/ß c ntldr A’5B,X È' Ê Y ,1u)Ú < î þ Î0ŸCK 9 È5à)„ ü2Ï4³0NKÈ Æ4£ ` ä ñ Ÿ ê È ¹ È 0 Y ,1u)Ú < ñ Ÿ êE›/ß,X Ô â Ô!9 ÈMmInitSystem Í2Ï4³0NKÈ Ã ¹ 6NI,X ··Õ È Â J PTE S 6Ñ ü Y ,2û5 ,X ™ ‰ ß7R Î(=)Ú Y ,NIM6 Ä

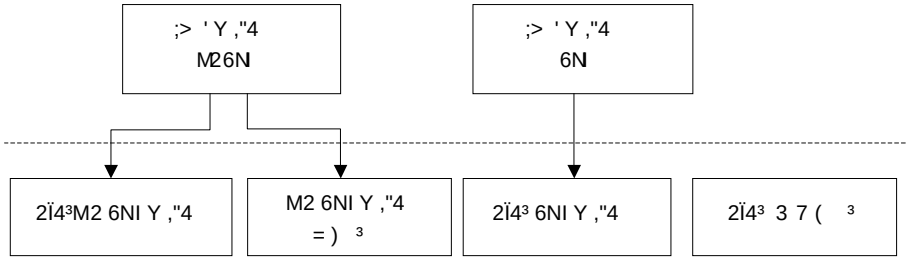
E-G È Y ,1u)Ú <,X ñ Ÿ ê ¹ 0 <F¼ ` ä È5à è2Ï4³0NKÈ Æ4£ ` < Î0ŸCK 9 Ä!8 â ;> ,X2Ï4³ ··Õ Ã ¹ Ú ý*ü2Ï4³ ¤ o,X Y ,1u)Ú s6Ñ Èø J M2 6NI Y ,"4 ` 6NI Y , "4FÑ Æ4£ Ã ¹!7 S*ü Z Ä

¢ ¹ Þ,X ··Õ Ú d Ã ¹,ß Î È Windows,X2Ï4³ 0NKÈ 0x80000000~0xffffffff 4£E› 2’ —] f,X ÈÔ4˜ < ¬G£?˜ n Z Ø þ ³,X8× È Ä L !‰ 0 ñ Ÿ ê,X ?U6 B÷ æ Ú2Ï4³

0NKÈ ÈW Ú5×<% Z(=)Ú Y ,,X DG£ ` é ÐEÝNM Û n,X?U" ÈS k Ô4œ k ,X ØF¼ Ú ³,X8× È,Ì Í!¨EW Ü)Ú ×L !‰ 0 3BóB÷ Î0ŸCKNI,Â ) `NI><4§ X ÈJ è ` äM2 6NI ³,X(=)ÚNIM6 ÚG! ÄL !‰ 1 ñ Ÿ ê ?ULš ü Ô o Y ,1u)Ú Ï u,X ñ Ÿ ê ÈÙ À ï Î Â NIM6 m Î < ` G>5Lš1u)Ú < È¹ žNIM6LÊ ê Ï u1 ÄL !‰ 2 ñ Ÿ ê ¾ 1T) S2Ï4³ õ + ,X 6NI ··Õ Ã>• 6NI5à Æ Ä

2Ï4³ 0NKÈ Y ,1u)Ú

üE- Ô8V Èå À ÚA|AŽ2Ï4³ 0NKÈ ,X Y , V) | Õ1u)Ú,X Äü2Ï4³ 0NKÈ È Ý oF¼ Ú o Ô o(M!^ õ + S*ü,X È!¨ V îA±0NKÈ + îA±1u)Ú < ` Windows $2Ï 4³ S*ü,X ×5à 6NI Y ,"4 `M2 6NI Y ,"4 í ¤ o4-2Ï4³ Y õ + `A' ÛPE |/ß c S*ü ,X Äü 6NI Y ,"4 ÚG!,X Y , Ý Ã6Ñ ü(=)Ú Y ,2û5 ,X ™ ‰ ß>• 6 Î ê , ×5àM2 6 NI Y ,"4 ÚG!,X Y , Ø b(=)Ú Y , Ä Z r)„E- ø/¡ Y ,"4 È Windows S*ü Z ø Y ,1u)Ú Äß Î bNIM6,X Y ,1u)Ú È ™L$ b ;> ' YF¼ S*ü × Þ Î0Ÿ ü ß ,X Y ,1u)Ú s6Ñ Î. Þ È Í ê ¤ o Ø/¡2f z,X Y , á u Ä ø ,X4§ X V Ò 4.15 / ÄE-G á5×<% îA±0NKÈ,X Y ,1u)Ú Å Ä £EÄ • "CK?• È ß ,X Y ,"4/Ä 2Ï4³ Y ,"4 È Þ ,X Y ,"4/Ä ;> ' Y ,"4 Ä 8V å À ÚOj A|AŽ2Ï4³M2 6NI Y ,"4 ` 6NI Y ,"4,X1u)Ú1k "© ` r)„ •"© È' â Ÿ4¡ ;> ' Y ,"4,X1k"© ` r)„ s)Ú Ä ß Ô8V a Ÿ4¡2Ï4³ PTE ³ ,X1u)Ú1k"© ` r)„ Ä



Ò 4.15 Windows Y ,X | Õ Y ,1u)Ú4§ X

Ä Ô Å 2Ï4³M2 6NI Y ,"4,X1u)Ú1k"©

ü Þ Ô8V?·AÏMiInitMachineDependent Ñ D Ê È å À Ò4£ ¤ ÈA¹ Ñ DA×*ü MiInitializeNonPagedPool MiInitializeNonPagedPoolThresholdÑ D 9 ñ Ÿ êM2 6NI Y , "4,X1u)Ú µ C ÄMiInitializeNonPagedPoolÑ D ! b base\ntos\mm\allocpag.cÊ È?• · -Õ 3 399~3 599> Ä W,X ?U Ï u ñ Ÿ ê*ü b1u)Ú Y ,"4,X Ô o < ¬G£ È ø J *ü b

, 0NKÆNIM6JÒ>< ,XMmNonPagedPoolFreeListHead D4˜ Ä0NKÆNIM6JÒ>< ,X!£ ÔNMFÑ
Ô þ MMFREE_POOL_ENTRY4§ X È J n V ß Ä?• base\ntos\mm\mi.h [Ê Å Ö

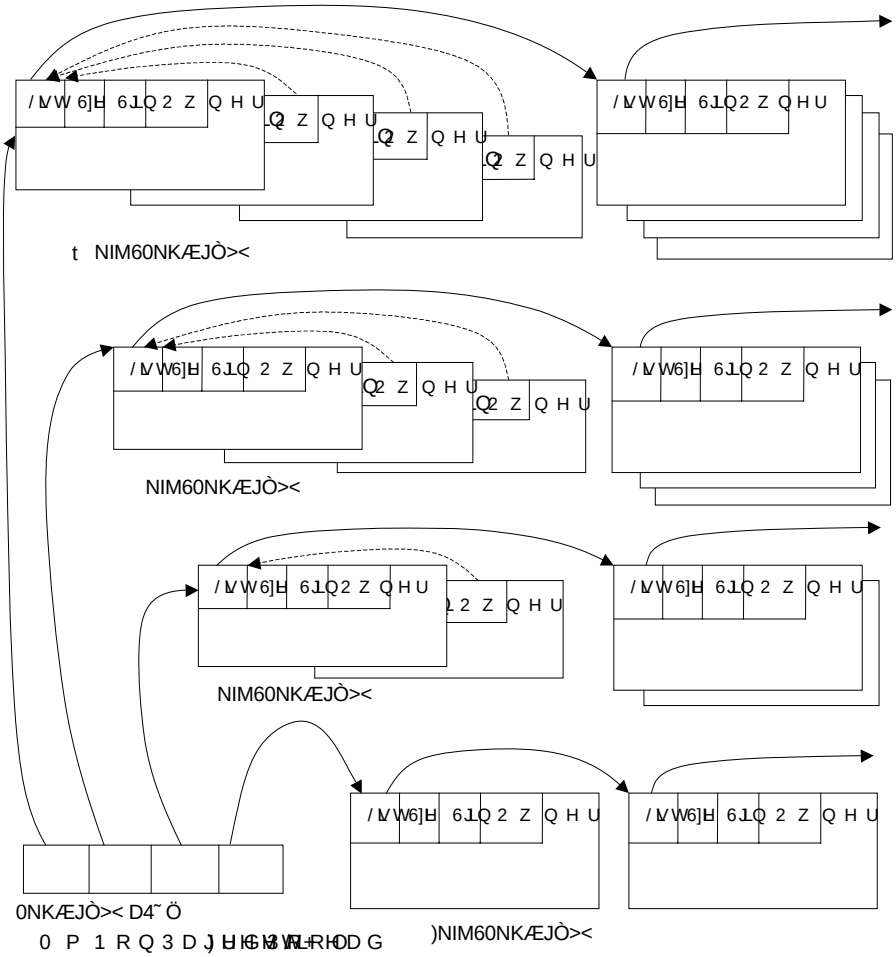
```
typedef struct _MMFREE_POOL_ENTRY {
  LIST_ENTRY List;     // maintained free&chk, 1st entry only
  PFN_NUMBER Size;     // maintained free&chk, 1st entry only
  ULONG Signature;     // maintained chk only, all entries
  struct _MMFREE_POOL_ENTRY *Owner; // maintained free&chk, all entries
} MMFREE_POOL_ENTRY, *PMMFREE_POOL_ENTRY;
```

ü ñ Ÿ ê(Š Õ ß È H þM2 6NI"40NKÈ È G MmNonPagedPoolStartÔ Ÿ È Ô E MmSizeOfNonPagedPoolInBytesû ã,X Y , È Ý,XNIM6 t 91 Ô þNIM6 ü,X MMFREE_POOL_ENTRYNMÄMmNonPagedPoolFreeListHead D4˜ üT¬Ax ™ ‰ ß Ù À4 NM Ö 1 Ô þ D4˜NM Ù ÿ Ý) þ0NKÆNIM6,X MMFREE_POOL_ENTRYNM È1 ` þ D4˜NM Ù ÿ Ý 2 þ0NKÆNIM6,X MMFREE_POOL_ENTRYNM È1 Ý þ D4˜NM Ù ÿ Ý 3 þ0NKÆNIM6 ,X MMFREE_POOL_ENTRYNM È1 ¯ þ D4˜NM Ù ÿ Ý û b1 b 4 þ0NKÆNIM6,X MMFREE_POOL_ENTRYNM Ä ü ñ Ÿ ™ ‰ ß È ¾ Ý Ô þMMFREE_POOL_ENTRYNM t 9 1 ¯ þ D4˜NMJÒ>< Ä

' â ÈMiInitializeNonPagedPool Ñ D.B nM2 6NI Y ,"4,XCK Ÿ `4§ 3(=)ÚNIM6 û MiStartOfInitialPoolFrame` MiEndOfInitialPoolFrameÈÔ â È M2 6NI Y ,"4 =) Î0Ÿ CK2Ï4³PTE Ä

Ô ºM2 6NI Y ,"4,X4§ X Æ Î0Ÿ È y ß 92Ï4³ ··Õ Ã ¹EîE› MiAllocatePoolPages` MiFreePoolPagesÑ D 9+ AË ` &E¬NIM6 ÄE- ø þ Ñ D 3 ! b base\ntos\mm\allocpag.cÊ È?• ··Õ 1 188~3 317> Ä J M2 6NI Y ,,XNIM6+ AËF Ee ! b ··Õ> 1 262~1 828 ÈNI M6 ² ,X ··ÕF Ee ! b 2 507~3 093> ÄE- ø þ Ñ D,X J -F¼ Ú Î Þ ü Ø)Ú 6NI Y ,"4 ,XNIM6+ AË ` ² È J 3 Ù À ÔF¼ Ú ··Õ ü Ø)Ú îA±0NKÈ ,X Y ,"4 Ä

M2 6NI Y ,"4 Ý øF¼ Ú Ö 8× È MmNonPagedPoolStartâ MmNonPagedPoolEnd0 KÈ,XF¼ Ú Î Y ,"4 È J Ý,XNIM6FÑ Æ4£ ÚG! Z(=)ÚNIM6 × 8× È MmNonPagedPoolExpansionStartt MmNonPagedPoolEndKÈ,XF¼ Ú =) È¾ Ý ' Î ´"©$µC‡ Y ,+ AËLÔ" Ê ! î ÚG!,ó!7,X(=)ÚNIM6 Ä- bM2 6NI Y ,"4,X0NKÆNIM6 Æ 4£>• ô Ø (=)ÚNIM6 È ¹È Windows Ú ý*üE- oNIM67¾D•,X Y , 9 X ÎCK Ô4˜0NKÆNI M6JÒ>< È 6 ¹A±AÈ È!£ þNIM6FÑ Ô þMMFREE_POOL_ENTRY4§ X È V Ò 4.16 / Ä MiInitializeNonPagedPoolÑ D Æ4£ ^ D4˜ MmNonPagedPoolFreeListHeadtÏ Ÿ ê ä ¾ Ù ÿ Ô þ ` H,X0NKÆ Y , + ÈA¹ Y , + Ù À Ý,XM2 6NINIM6 Ä



Ò 4.16 M2 6NI Y ,"4,X1u)Ú4§ X

V ! EÄ È üM2 6NI Y ,"4,X4§ X È!£ þ0NKÆJÒ>< ,X!£ þ8V&• Ù ÿ 1 Ã2 Ã3 Ã 4 ê 4 þ ¹ Þ,XNIM6 È ü à Ô þ8V&• Þ,XNIM6 J<. ³ 0NKÈ E²4Á,X Ä1 Ô þNIM6,X List ³ X ä ZJÒ><4§ X ÈSize ³ Û â ZE- þ8V&• Ù ÿ,XNIM6 DG£ ÈOwner ³ Û å7¾ Å × â4ÁNIM6,XList ` Size ³"u Ý S*ü È Owner ³ \G¡?U È W Û å1 Ô þNIM6 Ä

' MiAllocatePoolPagesÑ D ¢M2 6NI Y ,"4 ÚG!NIM6 Ê È W B Û n,X û ã È 61k ä Í h,XNIM6 D È G F¼ ¬G£ SizeInPages È' â ¢ MmNonPagedPoolFreeListHead Ð 4˜ EÝ ½EÖ ',X0NKÆJÒ>< Ô Ÿ ð2ö È,È7Ç R Ô þ8V&• ¹ ÝE- î,XNIM6 ÈÚA¹8V&• ¢JÒ >< /ÏL8 Î 9 Ä V pA¹8V&•L8 Z$µC‡ v ?U" ,XNIM6 D SizeInPages¹ ê ÈE¬ Ý = -,X

NIM6 ÈFw ÈA¹8V&• â0ÃF¼ Ú,XSizeInPagesþNIM6 Ú 0 4§ pE¨ ²4- v È !0ÃF¼ Ú = -,XFw oNIM6>• ' . Ô þ „,X0NKÆJÒ><8V&• t 9 EÖ ',X0NKÆJÒ>< ÆE- oNIM6,XOjNIM6 ,X Size ³LÔ?UA× H È â4Á,XNIM6,Z Û åOjNIM6 È ´NO Ï) ¬ Ä

Í b Æ4£.B n,X SizeInPagesþNIM6 ÈMiAllocatePoolPagesÑ D Ú ÿ R JCK ŸNIM6 `4§ 3NIM6 ü PFN D B g ,XA„ ) È JA'5B W À,X StartOfAllocation ` EndOfAllocation ! È ´!8 È Ô õ Ý ,XNIM6 ÚG! 3 î ü PFN D B g +- ß+©EÍ Ä G b PFN D B g,X n `1u)Ú ÈAË –5× 4.5.18V,X Ÿ4¡ Ä

V p ü0NKÆJÒ>< D4˜ ð2ö á $µC‡ 5 Ê,X0NKÆ8V&• È îMiAllocatePoolPagesÑ D A© Ò =)M2 6NI Y ,"4 È J$µC‡ ?U" ,XNIM6 D Ä

M2 6NI Y ,"4 ,XNIM6 ² EîE› MiFreePoolPagesÑ D 9 ` ä,X È Í b Ô þ4- n,XCK Ÿ StartingAddress È R W,X PTE È J ¤ ª ÎNI û4ê Ë È ¢5à n ! PFN D B g CK ŸNIM6,XPFNNM þÄ EîE› MiAllocatePoolPagesÑ D ÚG! k ,XE²4ÁNIM6 ÈJOjNIM6,X PFN NM,XStartOfAllocation ! ™ n 1 È"“- !8 PFN NME¯> ð2ö È Ã ¹ R 4§ 3NIM6 È J PFN NM,XEndOfAllocation ! 1 Ä Z4È xM2 6NI Y ,"4 0NKÆJÒ><,X4§ X È>• ² ,XNIM6 V p Ý Ã6Ñ,XA± ÈE¬LÔ?UC³ W À â4Á,X0NKÆNIM6 ê5Ù W À !M6,X0NKÆNIM6 Ü J ä Ô þ È û,X 0NKÆ Y , + È J è4È x QOjNIM6 ê KÈNIM6,X MMFREE_POOL_ENTRY4§ X ,X ³ Ä V p StartingAddressÛ/ Z Ô þM2 6NI =) ,X È Ã6Ñ Ý ™?UA×*ü MiFreeNonPagedPool Ñ D 9 ² W,XNIM6 Ä

ü MiAllocatePoolPages` MiFreePoolPagesÑ D,X ··Õ È+ AË êGž) þNIM6 Ê È å À Ã ¹,ß MiNonPagedPoolSListHeadJÒ><,X*ü"© ÄE- Î Þ1k Ô/¡ ì ê È ü ²) þNIM6,X Ê í È V p MiFreePoolPagesÑ D ¥)„ ÈMiNonPagedPoolSListHeadJÒ>< ,XNI M6 D Ä GDepth ³ Å ã b MiNonPagedPoolSListMaximumÄ < ¬G£ È>• ñ ŸC 4 Å È í Ú!8NIM6 t 9 MiNonPagedPoolSListHeadJÒ>< È –?• base\ntos\mm\allocpag,X 2 575~2 582> ··Õ Ä´!8 È ü MiAllocatePoolPages,X Ô Ÿ Ø Ä?• allocpag.c[Ê,X 1 264~1 286> ··Õ Å È V p v ?U+ AË) þNIM6 È J è MiNonPagedPoolSListHeadJÒ>< á 0N È í,È y ¢JÒ>< ¤ ª Ô þNIM6E¨ ²4- v Ä ¹ È MiNonPagedPoolSListHeadJÒ><,Ì ' b M2 6NI Y ,"4,X Ô þ)NIM64ç , ÄNe4 + AË ` ² )NIM6 È¾,Ì ' b ü )JÒ>< ,X ¦ 9 `/ÏL8 | 05à Æ È ¢5àFS ! Z ü MmNonPagedPoolFreeListHead4˜,X)NIM6JÒ>< ,Ì Í ÖC ,X ÚG! ` ² ¡ 0 Ä

Ä ` Å 2Ï4³ 6NI Y ,"4,X1u)Ú1k"©

y ß 9,ß2Ï4³ 6NI Y ,"4,X1u)Ú1k"© Ä ' ÈM2 6NI Y ,"4,X0NKÆNIM6JÒ><,X ."© á

EÖ Ü b 6NI Y ,"4 È´ 6NI Y ,"4 ,X0NKÆNIM6 J á ±A• Ý Í h,X(=)ÚNIM6 È5à è È ™ ™ Î b1u)Ú,X s ´5à 6NI Y ,"4 ,X0NKÆNIM6 ÚG!(=)ÚNIM6 ÈJ á0ú Ü 6NI Y ,"4,XA' Au ã Ò Ä 6NI Y ,"4 Ý ø þ È Ô þ 2Ï4³ < 8× È,X È º Ô þ îA±0NKÈ ,X Ä W À ü2Ï 4³ 0NKÈ ,XCK Ÿ Ú ÿ Í h b < ¬G£ MmPagedPoolStart MiSessionPoolStart –?• Þ Ô8V ,X Ÿ4¡ Ä 6NI Y ,"4 Ý Ô þ D B4§ X 9 £EÄ JNIM6 ÚG!(Š Õ È n V ß Ö

```
typedef struct _MM_PAGED_POOL_INFO {
  PRTL_BITMAP PagedPoolAllocationMap;
  PRTL_BITMAP EndOfPagedPoolBitmap;
  PMMPTE FirstPteForPagedPool;
  PMMPTE LastPteForPagedPool;
  PMMPTE NextPdeForPagedPoolExpansion;
  ULONG PagedPoolHint;
  SIZE_T PagedPoolCommit;
  SIZE_T AllocatedPagedPool;
} MM_PAGED_POOL_INFO, *PMM_PAGED_POOL_INFO;
```

J È2Ï4³ < 6NI Y ,"4+ < ¬G£ MmPagedPoolInfo 9 n × îA± 6NI Y ,"4 íEîE› îA±0NKÈ ,X ä , ¬G£ 9 n È G < ¬G£ MmSessionSpace ,X PagedPoolInfo ä , Ä

6NI Y ,"4 ,XNIM6 EîE› ! Ò 91u)Ú,X È Ô þNIM6,X ÚG! â ú È + A¹NIM6 Í h ,X ! 9><E',X Ä ü MM_PAGED_POOL_INFO 4§ X È PagedPoolAllocationMap³ Î ,X ! Ò È*ü b Û â!£ Ô þNIM6,X ÚG!(Š Õ × EndOfPagedPoolBitmap³ 3 Ô þ ! Ò È Û â Z !£ þ N I M 6 ú Ô õ Y , + A Ë , X Ô â Ô þ N I M 6 Ä FirstPteForPagedPool LastPteForPagedPool?˜ n Z Y ,"4,X 8× È ÄNextPdeForPagedPoolExpansion ³ n Z 6NI Y ,"4,X ß õ =) !5B Ä PagedPoolCommit A„) Z 6NI Y ,"4 Ý î å þNIM6 Æ 4£ Ú Z Y , Ä Æ ¤ x È þ ™ Í h Ý(=)ÚNIM6 Å È5à AllocatedPagedPool A„) Z 6NI Y ,"4 Æ ÚG! Z î åNIM6 ÄPagedPoolHint ³ Û/ Z ü ÚG!NIM6 Ê,XCK Ÿ ð2ö !5B Ä

Þ Ô8V Ò4£ ¤ ÈMmInitSystem A×*ü MiBuildPagedPool Ñ D 9 Î0ŸCK2Ï4³,X 6NI Y ,"4 ÄMiBuildPagedPool Ñ D Ä?• base\ntos\mm\mminit.c 3 300~3 786> ··Õ Å .,X _ ™ È Bü Þ 9A† ? < ¬G£ MmPagedPoolInfo ,X Ø þ ä , È ` ä2Ï4³ 6NI Y , "4,X ñ Ÿ ê Ä

< ¬G£ MmSizeOfPagedPoolInBytes MmSizeOfPagedPoolInPages) Z2Ï4³ 6NI Y , " 4 , X û ã È Ô û á C Y E › 2 Ï 4 ³ 0 N K È æ 4 - 6 N I Y , " 4 , X 8 × È È G MmNonPagedSystemStart-MmPagedPoolStart – ? • Ò4.14 Ä MmPagedPoolStart ` MmPagedPoolEnd Ú ÿA„ ) Z 6NI"4,XCK Ÿ `4§ 3 Ä ´!8 È MmPagedPoolInfo 4§ X , X FirstPteForPagedPool LastPteForPagedPool³ Ã B MmPagedPoolStart `

MmPagedPoolEnd X ,È y Ð Î È• mminit.c [Ê,X 3 592~3 594 ·-Õ ÄMiBuildPagedPool Ñ D ÚG! Q 6NI Y ,"4 8× È,X1 Ô þNI>< È GCK Ÿ ,XNI,Â)NM ÄPDE Å Û,XNI >< ÈMmPagedPoolInfo,X NextPdeForPagedPoolExpansiðn y ß 9,XNI>< È G 6 NI Y ,"4 8× È,X1 ` þNI><,X<. ³ Ä' âA×*ü MiCreateBitMap Ñ D ï Î Ô þ ! Ò È ! Ò,X û ã1 bNIM6,X DG£ È ! Ò D•,X Y , ¢M2 6NI Y ,"4 ÚG!,X Ä+ b1 Ô þNI>< ,X PTE Ý ,X È ¹ ! Ò Ô !M6,X 1 024 ! Ä Ô þNI>< 6Ñ •4‡ PTE,X D G£ Å#ÙLÊ È J -,X !>•5B ! ÈE-><â ! 1 024 þNIM6 0NKÆ,X ÄE- ÈMmPagedPoolInfo ,X PagedPoolAllocationMap³ Æ4£ ñ Ÿ ê ×4§ 3NIM6 ! Ò È G EndOfPagedPoolBitmapä , È 3 q õ ï Î È Ý,X ! <#ÙLÊ È ´ î þ Ï) Ý ,XNIM6 ÚG! Ä

' â MiBuildPagedPool A×*ü InitializePool Ñ D 9 ñ Ÿ ê ;> ' 6NI Y ,"4 È–?• 8V â [G b ; > ' Y ," 4 , X Ÿ 4 ¡ Ä Ô â È MiBuildPagedPool Ñ D A ' 5 B N X A : K Ü MiLowPagedPoolThreshold MiHighPagedPoolThreshold È ¹ “ üEÖ ' Ê íEî-¹2Ï4³ 6NI Y ,"4,X S*ü ™ ‰ Ä

ü MiBuildPagedPool Ñ D,X ·-Õ È å À Ã ¹,ß È V p2Ï4³/U!6 ;> ' Y ,"4 6 NI È G < ¬G£ MmDisablePagingExecutive,X MM_PAGED_POOL_LOCKED_DOWN Û « Æ5B Þ È í 6NI Y ,"4 rL Þ ¬ ä ZM2 6NI Y ,"4 È üE-/¡ ™ ‰ ß È Y ,"4 LÔ?U,X NIM6FÑ ™NO üA¹ Ñ D ÚG! Q Ä

Ÿ4¡ Z MiBuildPagedPool Ñ D,XF Ee ¹ â È å À 9,ß 6NI Y ,"4,XNIM6 ÚG! ` ² Ä V àM2 6NI Y ,"4 Ô ÈE- øNM Î Ï u 3 + MiAllocatePoolPages MiFreePoolPages Ñ D 9 ` ä,X × È üE- ø þ Ñ D ÈJ\ Í 6NI"4 `M2 6NI"4,X r)„ ·-Õ Î Þ ` < Ú Ô,X ÄMiAllocatePoolPages Ñ D,X PoolType – D Û n Z ü ¾ þ Y ,"4 + AËNIM6 ×5à MiFreePoolPages Ñ D í,È y B Y ² NIM6,XCK Ÿ 9.B n Y ,"4,X2O _ Ä

å À 9?·G ž MiAllocatePoolPages Ñ D ,XNIM6 ÚG!E›/ß È J ·-ÕF Ee ¢ base\ntos\mm\allocpag.c Ê,X 1 834 > Ô Ÿ ÄOj B PoolType – D R Y ,"4 MM_PAGED_POOL_INFO 4§ X È5B b F¼ ¬G£ PagedPoolInfo Ä ¾ Ý ø/¡ Ã6Ñ È?U 2Ï4³ 6NI Y ,"4 È G < ¬G£ MmPagedPoolInfo È?U îA±0NK È,X 6NI Y ,"4 È G MmSessionSpace->PagedPoolInfo b 6NI Y ,"4G›*ü ! Ò 91u)ÚNIM6,X ÚG! â ú È ¹ È MiAllocatePoolPages Ñ D ¾ 1 T) A × * ü E Y } Ñ RtlFindClearBitsAndSet È ü PagedPoolInfo->PagedPoolAllocationMap Ò ð2ö Û n DG£,XE²4ÁLÊ ! È G 6NI Y ,"4 Í h,XE²4Á0NKÆNIM6 Ä V p þ6Ñ R E- îE²4ÁLÊ ! È íA'"© =) 6NI Y ,"4 È G È S Y ,"4,X NextPdeForPagedPoolExpansiðn T â/Ï È" á6ÑC^E› 6NI Y ,"44§ 3

,X PDE Ä Aç =) Ô þ 6NI Y ,"4 È Û W âM6,X Y , ÚG!NI>< È JM2 ÚG!,ó!7,X (=)ÚNIM6 Ä 6NI Y ,"44£E› =) ¹ â È aA×*ü RtlFindClearBitsAndSetÑ D ð2ö$µC‡?U" ,XE²4ÁLÊ ! Ä

M2 6NI Y ,"4,XNIM6 ÚG! È JCK Ÿ `4§ 3NIM6,È y>• ÛA„ ü PFN D B g,X Í h PFN NM È Í b 6NI Y ,"4 ÈE-/¡ ."©> áEî È´ 6NI Y ,"4 ,XNIM6 Ã6Ñ î>• 6 Î ê , È ¹ á , ü Í h,X PFNNM Ä´!8 È ZA„ ) Ô õNIM6 ÚG!,XCK Ÿ `4§ 3 !5B È MM_PAGED_POOL_INFOÙ ÿ Ô þ J> ,X ! Ò È çK¼A„)!£ õNIM6 ÚG!,X4§ 3NIM6 Ä4§ ÜE- ø þ ! Ò È ' ² NIM6 Ê È ¾LÔ4- ÎCK Ÿ È Ã ¹P`A•A¹ ,X!7.B û È V p !8 !M6,XFw þNIM6 î þ>• ÚG! Èí!8 Ã ¹Ax Ô õNIM6 ÚG!,XCK Ÿ Ø ×V p ! M6,XFw þNIM6 Æ>• ÚG! È5à è4§ 3NIM6 ! Ò J þ>< â W Ô õNIM6 ÚG!,X4§ 3NIM6 Èí – D StartingAddress 4- Î,XCK Ÿ JíAÃ,X È„ E-/¡ ™ ‰ È2Ï4³ î ý$W Äbugcheck ÅÄ

y ß 9 ÈL8 Z ü4§ 3NIM6 ! Ò A'5B Q,Ì h,X ! Ä?• ··Õ 2 269 > Å ¹ ê È MiAllocatePoolPagesÑ DE¬?U È „ 6NI Y ,"44§ X PagedPoolInfo ,X Æ ÚG!NIM6 DG£ È Í h b MM_PAGED_POOL_INFO4§ X,X AllocatedPagedPool Ä V p Y ,"4,X0NKÆNIM6 DG£ ã b(M nKÜ Ä < ¬G£ MiLowPagedPoolThresholdÅ È í ¥ ÎNXA: µ Ë Ä2Ï4³ < _ Ê MiLowPagedPoolEventÅ Ä' â " ¹E- oNIM6 úLÔ?U „ W À,X ¿>< ÄTLB ÅNM È 8¹ ÈíEîE› KeFlushSingleTbÃKeFlushMultipleTb ê KeFlushEntireTbÑ D „ J ¿><NM Ä Ô â È!7.B ? Q Æ ÚG!NIM6,X PTE ÈE¨ ²E-4˜E²4ÁNIM6,XCK Ÿ Ä

2Ï4³ 6NI Y ,"4,XNIM6 ² E›/ßM2 ,È þ Z ' È ü MiFreePoolPagesÑ D È V p ô E¯ 9,XCK Ÿ StartingAddressŸ b MmPagedPoolStart MmPagedPoolEnd KÈ È íAÈ âE- 2Ï4³ 6NI Y ,"4 ,XNIM6 ÄNIM6 ² F Ee ¢ allocpag.c,X 3 100> Ô Ÿ ÈOj ý*ü PagedPoolInfo ,X ø þ ! Ò 9P`A•CK Ÿ ,X Ý û ÄEîE›P`A• ¹ â ÈMiFreePoolPages Â E- ø þ ! Ò È S kE- Ô!‰ Y , ± Õ þ ÚG!,X(Š Õ È à Ê 34È x Q PagedPoolInfo ,X AllocatedPagedPool PagedPoolCommit Ä

G b MiFreePoolPagesÑ D ² 2Ï4³ 6NI Y ,"4 ,XNIM6 È Ý ´&•LÔ?UAÈ â Ö

(1) V p 6NI Y ,"4>•G!5B ä á Ã 6NI,X Änon-pageable ÅÈ í ¾LÔ4È x ! Ò `,Ì h,X < ¬G£ â Y ,"4 ¬G£ G Ã È?• ··Õ 3 182~3 230> Ä

(2) V p) þNIM6>•Gž È í Ý Ã6Ñ t 9 Ô þ)JÒ>< È?• ··Õ 3 170~3 175> Ä !8)JÒ>< + < ¬G£ MiPagedPoolSListHead9A„),X ÄJÒ>< Ô î , 8 þ)NIM6 Ä ´!8 È V p v ß õ+ AË) þNIM6 È í MiAllocatePoolPagesÑ D,È y ¢A¹JÒ>< ¤ ªNI M6 G Ã È –?• ··Õ 1 862~1 870> Ä

(3) 2Ï4³ 6NI Y ,"4 ,X Y , 3FI ¢ 6NI0NKÈ Ä G2Ï4³NIM6 [Ê ,X0NKÈ Å,X1u)Ú È ´ Ô º Y ,2û5 È íE- oNIM6LÔ?U>• 6 ê , È¢5à 4*ü ê ,0NKÈ ÄE- 6NI Y ,"4 âM2 6NI Y ,"4,X Ô þ GK ÿ Ä å À Ã ¹,ß È ü MiAllocatePoolPagesÑ D A×*ü Z MiChargeCommitmentCantExpandÑ D ×5à üMiFreePoolPages Ñ D È íA×*ü Z MiReturnCommitmentÄ rL Þ ÈE- Ô þ C AÁ?Ô c ÅÄ5à è È ü MiFreePoolPagesÑ D È WE¬A×*ü ZMiDeleteSystemPageableVmÑ D È ¹ ôL8 Ã 6NI,X2Ï4³ 8× È Ä

G b 6NI Y ,"4 S*ü,X ø þ ! Ò È E-G Ý ™?UAÈ â Ô ß !,X ÿ Ä Í b PagedPoolAllocationMap,X ! È5B !>< â Í h,XNIM6 á Ã*ü,X ÈLÊ !>< â Ã*ü,X Ä 2Ï4³ 6NI Y ,"4 ñ Ÿ Ê È1 Ô þ PDE Û,XNI>< Æ ÚG! È ¹A¹NI>< ,X PTE Í h,X NIM6 Ä1 024þ Å Æ4£ Ã ¹ S*ü Z Ä ´5à È ü ! Ò È ! 1 024 ! LÊ ! È J -,Z 5B ! (Š Õ ÄLc- 6NI Y ,"4>• =) È G NextPdeForPagedPoolExpansiónÞ â/Ï ÈLÊ ! Î)„,X !5B 3 Ô Ÿ â/Ï Ä ÈNextPdeForPagedPoolExpansion âM6 Í h,X ! Ô n 5B !,X Ä ´ !8 È Í b PagedPoolAllocationMap,X ! ÈLÊ !></ 0NKÆNIM6 È Ø b Y ÚG!(Š Õ ×5B !>< / Ã6Ñ Æ>• ÚG! È ê5Ù î þ =) A¹NIM6 Ä8¹ á5×<% PDE =),X ´2ô È V ÀCK 9 Ã ¹E- AÈ ÈMiAllocatePoolPages.,X _ ™ ^E²4Á,XLÊ ! ¬ ä5B ! ×5à MiFreePoolPagesÑ D .,X _ ™ ^E²4Á,X5B ! ¬ äLÊ ! Ä EndOfPagedPoolBitmap! Ò ñ Ÿ Ê È Ý,X !,Z LÊ ! Ä!£ õ ÚG!NIM6 Ê È Ô â Ô þ ÚG!,XNIM6 Í h,X !>•5B ! ×MiFreePoolPages Ñ D q B!8 ! Ò 9 ø • ôE¯ 9,XCK Ÿ ,X Ü"© û ÈJ è ^ ¢A¹ Ô Ÿ,X Æ ÚG!E²4ÁNIM6 ,X Ô â Ô þNIM6 Í h,X !#ÙLÊ Ä

Ä Ý Å ;> ' Y ,"4,X1u)Ú1k"©

ÞM6 Ÿ4¡,X 6NI Y ,"4 `M2 6NI Y ,"4 Windows ¡ 02Ï4³ ¤ o,X Î | Õ Y ,1u )Ú !‰ È W ¹NIM6 Î 2f z 91u)Ú2Ï4³ æ n,X 8× È Ä ' ÈNIM62f z Í b Ô8 ,X ·-ÕF Ee5à?Ô þ û Z È!¨ V È1 2 0´ Ÿ4¡,X ÍB51u)Ú < T T ü È ã,X2f z Þ ¹ 0 Ä ¹ È ZEÖ h Ø/¡ Y 4˜ Ê Í b Y ,1u)Ú,XLÔ?U È Windows Y ü2Ï4³,XM2 6NI Y ,"4 ` 6NI Y ,"4,X Î. Þ È r)„ Z&I# ,X ÃÃEÖ h Ø/¡ û ã Y ,LÔ" ,X Y ,"4 ÈE- “ ;> ' Y , "4 È J r)„ ·-Õ ! b base\ntos\ex\pool.¢Ê Ä

;> ' Y ,"4 ÍB5 + D B4§ X POOL_DESCRIPTOR9 £EÄ,X È ¹ ß W,X n È ! b base\ntos\inc\pool.hÊ Ä

```
typedef struct _POOL_DESCRIPTOR {
  POOL_TYPE PoolType;
  ULONG PoolIndex;
  ULONG RunningAllocs;
  ULONG RunningDeAllocs;
```

Windows *Y s)Ú â r)„*

```
  ULONG TotalPages;
  ULONG TotalBigPages;
  ULONG Threshold;
  PVOID LockAddress;
  PVOID PendingFrees;
  LONG PendingFreeDepth;
  SIZE_T TotalBytes;
  SIZE_T Spare0;
  LIST_ENTRY ListHeads[POOL_LIST_HEADS];
} POOL_DESCRIPTOR, *PPOOL_DESCRIPTOR;
```

!8 ê È Ý Ô4˜ < ¬G£ â ;> ' Y ,"4 Ý G È J n ` Ä â Ú ÿ ! b pool.c ` pool.h È 0´ å À ™- - b Y ,1u)Ú È5à Ñ+9 â à!9 Ý G,XF Ee È ¹ ßM6 ë Î,X < ¬G£ á Ù ÿ â à!9 Ý G,X ÍB5 Ö

```
#if defined(NT_UP)
#define NUMBER_OF_PAGED_POOLS 2
#else
#define NUMBER_OF_PAGED_POOLS 4
#endif

ULONG ExpNumberOfPagedPools = NUMBER_OF_PAGED_POOLS;

ULONG ExpNumberOfNonPagedPools = 1;

POOL_DESCRIPTOR NonPagedPoolDescriptor;

#define EXP_MAXIMUM_POOL_NODES 16

PPOOL_DESCRIPTOR ExpNonPagedPoolDescriptor[EXP_MAXIMUM_POOL_NODES];

#define NUMBER_OF_POOLS 2
PPOOL_DESCRIPTOR PoolVector[NUMBER_OF_POOLS];

PPOOL_DESCRIPTOR ExpPagedPoolDescriptor[EXP_MAXIMUM_POOL_NODES + 1];

volatile ULONG ExpPoolIndex = 1;
```

B ¹ Þ n ,X < ¬G£ ¹ ž W À,XC ™ ‰ È å À Ã ¹-¹F' È ExpNumberOf-NonPagedPools·>< ZM2 6NI Y ,"4,X DG£ È ¾ Ý Ô þ ×5à 6NI Y ,"4,X DG£ È G ¬G£ ExpNumberOfPagedPoolsè ü) Ø)Ú <2Ï4³ Þ Ý þ È ü î Ø)Ú <2Ï4³ Þ Ý h þ Ä"¼ ã È D4˜,X 2ô þ D EXP_MAXIMUM_POOL_NODES+1Å Ä PoolVector Ô þ Ù ÿ ø þ D 4˜,X 2ô È1 Ô þ 2ô PoolVector[0]Û åM2 6NI Y ,"4 È G NonPagedPoolDescriptor,X ×1 ` þ 2ô PoolVector[1] Û å 6NI Y ,"4 È G Û å1 Ô þ 6NI Y ,"4 Ä D4˜ ExpNonPagedPoolDescriptor™*ü b Ý î þM2 6NI Y ,"4,X ™ 6 × D4˜ ExpPagedPool-Descriptor ,X!£ þ 2ô Ú ÿ Û å Ô þ 6NI Y ,"4 Ä

;> ' Y ,"4 ÍB5,X ñ Ÿ ê 3 Ý 6NI Y ,"4 `M2 6NI Y ,"4 Ú ÔE¯> ,X Ä MiInitMachineDependent Ñ D ü ;> Z 2 Ï 4 ³ M 2 6 N I Y ,"4,X ñ Ÿ ê Ä G A × * ü

MiInitializeNonPagedPool Ñ D Å J ` ä Z PFN D B g,X ñ Ÿ ê ¹ â È E¬ A × * ü Z
InitializePool(NonPagedPool, 0Ð E-!7 ñ Ÿ ê ;> 'M2 6NI Y ,"4 ÍB5 Ä º ê È ü
MiBuildPagedPool Ñ D È '2Ï4³ 6NI Y ,"4,X ñ Ÿ ê Î ` ä ¹ â È A¹ Ñ D,È yA × * ü
InitializePool(PagedPool, 0Ð ¹ ` ä ;> ' 6NI Y ,"4,X ñ Ÿ ê Ä

InitializePool Ñ D+ ø þ,Ì Í(À0Ÿ,XF¼ Ú X ä È M6F¼ Ú ;> M2 6NI Y ,"4,X ñ Ÿ ê È
âM6F¼ Ú ;> 6NI Y ,"4,X ñ Ÿ ê Ä W .,X _ ™ È ñ Ÿ ê ¹ Þ E- o < ¬G£ È J è
!£ þ ;> ' Y ,"4 ÍB5 A × * ü ExInitializePoolDescriptor Ñ D È? POOL_DESCRIPTOR 4 §
X ,X ³ Ä ¢ InitializePool Ñ D Ã ¹,ß È ;> ',X M2 6NI Y ,"4,X POOL_
DESCRIPTOR ÍB5 < ¬G£ NonPagedPoolDescriptor È à ;> ',X 6NI Y ,"4,X POOL_
DESCRIPTOR ÍB5 í ¢ ;> ',XM2 6NI Y ,"4 ÚG!,X ÄE- Ô þ Ü)Ú,X Y , ÚG!NN
c Ä ' InitializePool Ñ D>•A × * ü 9 ñ Ÿ ê ;> ' 6NI Y ,"4 Ê È ;> ',XM2 6NI Y ,"4 Æ
4£>• ñ Ÿ ê È ´5à InitializePool Ã ¹ å W+ AË Y , Z Ä

InitializePool ` ExInitializePoolDescriptor Ñ D,X4š8V Ã ¹ –,ß base\ntos\ex\pool.c Ê
,X 893~1 352 Ã659~756 È E-G á aE¯ Ô!9?·Gž Ä ü POOL_DESCRIPTOR 4 § X È
PoolType ³ n 2O _ POOL_TYPE,X NonPagedPool ê PagedPool È Ú ÿ ·>< ;> 'M2
6NI Y ,"4 ` 6NI Y ,"4 Ä 1u ü POOL_TYPE E¬ Ý J ª,X Y ,"42O _ È E-G å À ¾
5 × <% NonPagedPool PagedPool ø/¡2O _ Ä PoolIndex ³ Û ' ! ÍB5 üA¹2O _,X Y ,"4
D4˜ ,X2ö é È Í b 6NI Y ,"4 È PoolIndex W ü ExpPagedPoolDescriptor D4˜ ,X ß Û
ÄListHeads D4˜ Ô þ GK D B ä , È ;> ' Y ,"4 Í b ã Y ,,X ÚG! ` ² È Eî
E› Ô 4˜0 N K Æ Y , +J Ò>< 9 r)„,X Ä y ß 9 å À E î E› ? ExAllocatePoolWithTag/
ExFreePoolWithTag Ñ D 9 Ÿ4¡ ;> ' Y ,"4,X1u)Ú1k"© Ä

ü Windows NT,X ½ ó È ;> ' Y ,"4,X1u)Ú EîE› í 2Ï4³1k"© Ä –5× 4.1.38V Å
9 r)„,X Ä ü WRK ,X ;> ' Y ,"4 r)„ ·-Õ È å À Ã ¹,ß È WG›*ü,X JM2 í 2Ï4³
1k"© È5à *ü Ô4˜/Ä ¿ ¹>< Älookaside list Å,X0NKÆ Y , +JÒ>< Ú ÿA„) Z Ø/¡ û ã,X
Y ÚG! Y , Ä Ô þ Y ,"4LÔ?U È î Y , Ê È W Ã ¹ å Í h,X2Ï4³ Y ,"4+ AË È î,XNIM6 Ä
5à ' Y ,Gž Ê È íA} YGž ,X Y , â,ÌF•,X Y , + Ã6Ñ Ü J È¹ 6 ä È û,X0NKÆ Y
, + È V p X ä Ô þ ` H,XNIM6 È í ÚNIM6 xE¬4-2Ï4³ Y ,"4 Ä Í bLÔ?U Ô þNIM6 ê ¹ Þ
,X Y ,+ AË È;> ' Y ,"4,È y å2Ï4³ Y ,"4+ AËC‡ ó,XNIM6 J x4- v ×Í b ã b Ô þ
NIM6 û ã,X Y ,+ AË È ;> ' Y ,"4 S*ü ¿ ¹>< 91u)Ú ã2f z,X Y , + Ä

)„ ü å À 9,ß ExAllocatePoolWithTag Ñ D È J ·-Õ ! b base\ntos\ex\pool.c X 1 738~2
677> ÄExAllocatePoolWithTag Ñ D ú Ý þ – D Ö PoolType – D Û â Z?U ¢ ¾/¡ Y ,"4

ÚG! Y , ÈNumberOfBytes ></ ?U+ AË î å +8V,X Y , ÈTag Ô þ 32 ! H D Ä B PoolType ¹ ž !M6 ë Î,X PoolVector < ¬G£ ÈExAllocatePoolWithTag Ã ¹.B n,Â Û Y ,"4 ÍB5 È G F¼ ¬G£ PoolDesc‚X ñ Ÿ È?• ··Õ 1 885~1 890> Ä

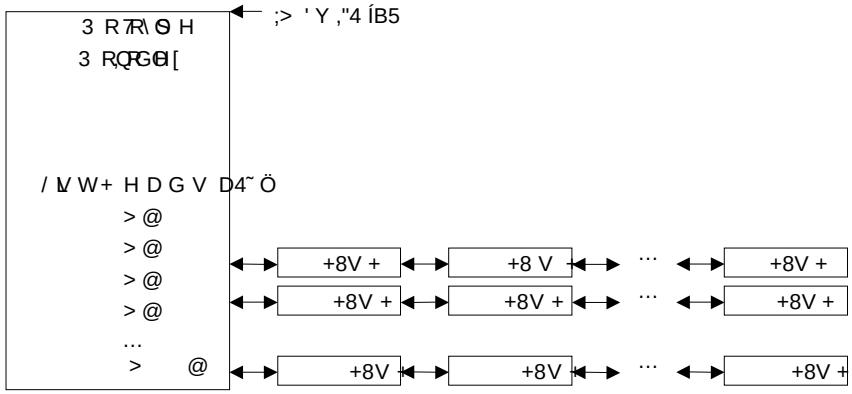
POOL_DESCRIPTORÍB5 4È x Z Ô4˜ ¿ ¹>< ÈG W,X ListHeadsä , ÆE- o ¿ ¹>< Ù ÿ Z 8 +8V á D û ã,X0NKÆ Y , +JÒ>< ÆîE› ;> ' Y ,"4 ÚG!,X Y , + Ý Î n û ã,X È G W À,X1u)Ú ÔJÔ È ßM6 Ô o,Ì G,X n Ö

```
typedef struct _POOL_HEADER {
  union {
    struct {
      USHORT PreviousSize : 9;
      USHORT PoolIndex : 7;
      USHORT BlockSize : 9;
      USHORT PoolType : 7;
    };
    ULONG Ulong1;
  };

  union {
    ULONG PoolTag;
    struct {
      USHORT AllocatorBackTraceIndex;
      USHORT PoolTagHash;
    };
  };
} POOL_HEADER, *PPOOL_HEADER;

#define POOL_PAGE_SIZE 0x1000
#define POOL_BLOCK_SHIFT 3

#define POOL_OVERHEAD ((LONG)sizeof(POOL_HEADER))

#define POOL_FREE_BLOCK_OVERHEAD (POOL_OVERHEAD + sizeof (LIST_ENTRY))

typedef struct _POOL_BLOCK {
  UCHAR Fill[1 << POOL_BLOCK_SHIFT];
} POOL_BLOCK, *PPOOL_BLOCK;

#define POOL_SMALLEST_BLOCK (sizeof(POOL_BLOCK))

#define POOL_BUDDY_MAX \
  (POOL_PAGE_SIZE - (POOL_OVERHEAD + POOL_SMALLEST_BLOCK ))

#define POOL_LIST_HEADS (POOL_PAGE_SIZE / (1 << POOL_BLOCK_SHIFT))
```

´!8 È!£ Ô õ Y , ÚG!E¬ ™NO ^ POOL_HEADERF¼ Ú 31k Þ Ä ;> ' Y ,"4,X Î 1u)Ú1k"© E- ,X Ö V p Ô õ Y , ÚG!,X û ãCYE› Z POOL_BUDDY_MAX È í ;> ' Y ,"4,È yA×*ü i ,X2Ï4³ Y ,"4 9+ AËC‡ ó,XNIM6 È J,È y x4- v È üE-/¡ ™ ‰ ß È v Ó ,X Y , NIM6 ÍU$,X È 3 AÈ È Y , + ,X Ô â 12 ! 0 × ú í È

ExAllocatePoolWithTagÑ D " ¹ Y ,"4 YF¼,X ¿ ¹>< È ¹ ó R ÜEÖ û ã,X0NKÆ Y , + È 8¹ þ6Ñ R $µC‡ 5 Ê,X Y , + È í å2Ï4³ Y ,"4+ AË Ô þ „,XNIM6 È^NIM6,X ÔF¼ ÚE¨ ² 4- v È = ß,X t 9EÖ ' û ã,X ¿ ¹>< Ä

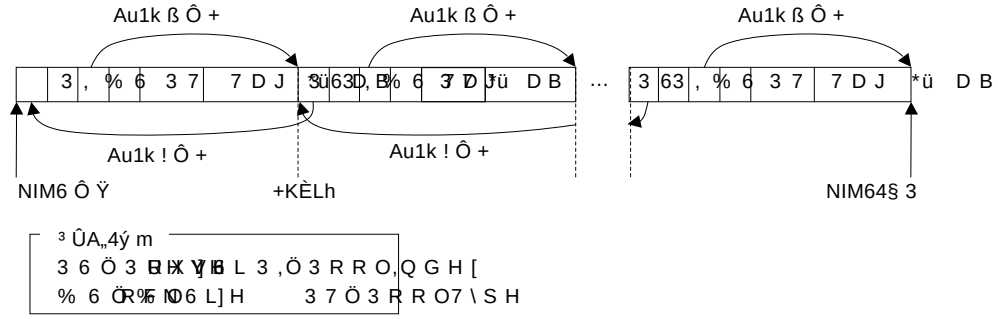
Ô ã,X Y , + 8 þ +8V È POOL_HEADER,X û ã 3 8 þ +8V È ¹ È POOL_BUDDY_MAX ,X 4 096-16=4 080È5à POOL_LIST_HEADS ,X 512 Ä POOL_DESCRIPTOR ,X ¿ ¹>< Ù ÿ 512 NM Ä rL S*ü 510 NM Å È Ú ÿ Í h b 8 Ã16 Ã 24 4 072 ` 4 080 û ã,X0NKÆ Y , + Ä8¹ v + AË û b 4 0805à ã b 4 096,X Y , + È í,È y S*ü H þNIM6 È´ = ß,X0NKÈ áC‡ ¹ •4‡ Ô ã Y , + Ä8 +8V Åt Þ1u)Ú ÔJÔ Ä8 +8V Å Ä Ò 4.17 / Z ;> ' Y ,"4,X1u)Ú4§ X Ä



Ò 4.17 ;> ' Y ,"4,X1u)Ú4§ X

POOL_HEADER ,X1 Ô þ C 6(Ü ä , ,X Ø þ ³,X ÿ V ß Ö PreviousSizeA„) Z ' ! Y , + !M6,XFw þ Y , +,X û ã È q B!8 ³ Ã ¹ R à Ô þNIM6 !M6,X Y , + × BlockSize A„) Z ' ! Y , +,X û ã È q B!8 ³ Ã ¹ R à Ô þNIM6 âM6,X Y , + × PoolIndexAÈ â Z ' ! Y , + 2 b ¾ þ ;> ' Y ,"4 × PoolType ä ,A„) Z ' ! Y , + ü ,X Y ,"4,X2O _ È Í b0NKÆ Y , + È PoolType ä , 0 ÄE-G PreviousSize` BlockSizeFÑ Û rL û ãL8 ¹ 8 â k ,X È JM2 s D• ÄPOOL_HEADER ,X PoolTag ³A„) Z ' !>• ÚG! Y , +,X Ô þ ÛA„ Ä Ò 4.18 / Z Ô þ « ;> ' Y ,"41u)Ú,XNIM6,X YF¼4§ X Ä

å À ² ExAllocatePoolWithTag Ñ D,X ··Õ Þ Ä V p NumberOfBytes – D û b POOL_BUDDY_MAX Èí,È yA×*ü2Ï4³ Y ,"4,X Y , ÚG! Ñ D È G MiAllocatePoolPages Ñ D È 9 ` ä Y , ÚG! È –?• pool.c [Ê,X 1 907~2 014> ··Õ Ä ú íLÔ?U S*ü Y ,"4 ÍB5 ,X ¿ ¹>< ÄOj B NumberOfBytes– DAu1k k ¿ ¹>< ü ListHeads D4˜ ,X 2ö é È G ListNumber F¼ ¬G£ È?• ··Õ 2 042> Ä



Ò 4.18 ü ;> ' Y ,"4 ,XNIM6,X YF¼4§ X

y ß 9.B n?U ü ¾ þ Y ,"4 ÍB5 ÚG! Y , È G.B n POOL_DESCRIPTORÍB5 È?• pool.c [Ê,X 2 046~2 353> ·-Õ Ä Í b 6NI"4 È ü 1 7ÇExpNumberOfPagedPools¢È R Ô þ î þ>•JÕ #,X 6NI"4 È¢E-G 3 Ã ¹,ß Î È Windows S*ü î þ 6NI Y ,"4 Ã ¹ r t J ¥ û È AŒ î þ4"/ß*î7Ç î þ Ø)Ú < à Ê S*ü á à,X 6NI Y ,"4 Ä Í bM2 6NI"4 È¾ Ý Ô þ È í,È y S*ü < ,XM2 6NI Y ,"4 È8/¡ ™ 6 ß È F¼ ¬G£ PoolDescü 1 886> Æ4£ >•C ¹!7.B,X Ä

.B n Z POOL_DESCRIPTORÍB5 PoolDesc` ¿ ¹>< D4˜,X ß Û ListNumber ¹ â È y ß 9 Ã ¹ ð2ö$µC‡ 5 Ê,X0NKÆ Y , + Ä 2 368~2 523> KÈ,X do ~)ƒ!7 ` äE- Ô Ï u Ä ¢ ListNumber Û n,X ¿ ¹>< Ô Ÿ ÈNN õ " ¹JÒ>< Ö ¾?U ' !JÒ>< á0N È 6Ñ R $µC‡ 5 Ê,X Y , + × V p ' !JÒ>< 0N È í4»4Á R û Ô Ë,XJÒ>< Ä8¹ R ,X Y , + û b ?U" ,X Y , û ã È í ^ W Ú ä ø + È Ô + 0 4§ pE¨ ²4- v È º Ô + t EÖ ' û ã,X ¿ ¹>< Ä POOL_HEADER4§ X,X PreviousSizeV p 0 È íAÈ â W NIM6,X Ô Ÿ Ø È üE- /¡ ™ ‰ ß È ª !M6F¼ Ú 0 4§ p Y , + ÄA„) ü Entry ¬G£ Å È âM6F¼ Ú/á â?U &E¬ ¿ ¹>< ÄA„) ü SplitEntry ¬G£ ÅÄVp POOL_HEADER4§ X,X PreviousSizeá 0 È íAÈ âE- á NIM6,XCK Ÿ Y , + È üE-/¡ ™ ‰ ß ª âM6F¼ Ú 0 4§ p Y , +E¨ ²4- v ÄA„) ü Entry ¬G£ Å È !M6F¼ Ú/á â?U &E¬ ¿ ¹>< ÄA„) ü SplitEntry ¬G£ Å Ä 4£E› V!8 Û Ú ¹ â È V p SplitEntry Y , +,X û ãC‡ ó •4‡ Ô þ POOL_HEADER t Þ JÒ><,X ø þ ÛJ\ ³ Ä rL Þ h)Ú?· POOL_SMALLEST_BLOCKÅ È í Ú SplitEntry ¦9 EÖ ',X ¿ ¹>< Ä ü do ~)ƒ ' È á1u ú?U Û Ú Ô þ Y , + È Entry Û å?UE¨ ²,X Y , + ÈA'5B J ,X PoolTagÈ J4È x Q Y ,"4 POOL_DESCRIPTOR ,X,Ì G ä , È ºL8 Y , + *ü b ¿ ¹><,XJÒ>< ÛJ\ µ C È Ô âE¨ ² Y , + ,X Ý D B Ä

V p ü do ~)ƒ ` ä ¹ â È ¡' þ6Ñ R Ý ,X0NKÆ Y , + È íAÈ â Y ,"4 "u Ý û b1 b ?U" û ã,X Y , + È üE-/¡ ™ ‰ ß È Ý ™?U å2Ï4³ Y ,"4+ AË Ô þ „,XNIM6 È J

è ^ „NIM6,X !M6F¼ Ú 0 4§ p Y , +E¨ ²4- v ÈâM6F¼ Ú XEô Ô þ „,X0NKÆ Y , + ¦ 9 EÖ ',X ¿ ¹>< Ä‹ AË „NIM6 EîE›A×*ü MiAllocatePoolPagesÑ D 9 ` ä,X È²• pool.c [Ê,X 2 532 > ·-Õ × ü „NIM6 XEô Y , +4§ X J Û Ú!8 Y , +,X ·-Õ?• 2 587~2 602 > ×Ô â È^ Û Ú â = ß,X0NKÆ Y , + t 9 ¿ ¹>< JE¨ ²4§ p Y , +,X ·-Õ?• 2 628~2 676> È!8F¼ Ú ·-Õ,XF Ee â do ~)ƒ ,X ·-Õ2O Ä

)„ üE@ ExFreePoolWithTagÑ D È¹ Ñ D ! b base\ntos\ex\pool.ç Ê,X 4 296~5 024 > Ä W,X1 Ô þ – D P Û n Z?UGž ,X Y , + È1 ` þ – D TagToFreeÛ n Z>•Gž ,X Y , +,X ÛA„ Ä ·-Õ> 4 363~4 503 Ô o ” ¹ ` ¹ «A„)F Ee Ä ·-Õ> 4 510~4 600Ì\ Í Fw o,È yEîE›2Ï4³ Y ,"4+ AË ,X Y , +,XGž È G ü ExAllocatePoolWithTagÑ D J\ Í û b POOL_BUDDY_MAX ,X Y ,AË" 5à,È yA×*ü MiAllocatePoolPagesÑ D k ,X Y , + Ä Í h È Y ,,XGž EîE› MiFreePoolPagesÑ D 9 ` ä Ä

y ß 9 È ExFreePoolWithTagÑ D B – D P È n ! ,Ì h,X POOL_HEADERÈ5B b F¼ ¬G£Entry È J ” ¹ J ,X ä , µ C È E¯ Ô!9 n ! W âM6,X Y , +,X POOL_HEADERÈ ” ¹ âM6 Y , +,X PreviousSize ú â ' ! Y , +,X BlockSize,Ì1 È E-1k Í P,X Ý û ” ¹ Ä ¹ È V p ExFreePoolWithTagÑ D y Ô þ á!7.B,X P È L8M2,ó,X (M ã XEô,X È ú í W Ã ¹ Ý \ û,X V)[6Ñ ”# 2Ï4³ Y , ÚG! âGž ,X á Ô7È û Ä4£E› Ý û ” ¹ ¹ â È ExFreePoolWithTagÑ D B Y , + ,X PoolType ` PoolIndex µ C È R Y ,"4 £EÄ0ú ÍB5 È ü F¼ ¬G£ PoolDesc Ä

' â ÈExFreePoolWithTag Ñ DE¯> 2Ï4³ Ø)Ú È J —,X ñ Ç â å À ü2Ï4³ 6NI Y , "4 `M2 6NI Y ,"4 ,ß ,X,Ì Ó Ä Í b ã Y , +,XGž È£ þ Ø)Ú < Ý ø Þ4ç ,JÒ>< È ! b KPRCB4§ X,X PPPagedLookasideList ` PPNPagedLookasideList , È Ú ÿ Í h b 6 NI Y ,"4 `M2 6NI Y ,"4,X4ç ,JÒ>< ÄKÜ POOL_SMALL_LISTS Û â Z ¾ Ý ã b1 b 32 h8 û ã,X Y , + ! S*ü4ç ,JÒ>< Ä ´!8 È ü ExAllocatePoolWithTag Ñ D È '+ AË Ô þ ã Y , + Ê È V p ü ' ! Ø)Ú <,X4ç ,JÒ>< 6Ñ R Í h û ã,X Y , + È í,È y ¢4ç ,JÒ>< ,L8 Ô þ Y , + È ¿Eó E¨ ²4- v Ä Í h È ü ExFreePoolWithTagÑ D È V p ' ! Ø)Ú <,X4ç ,JÒ>< î þE’ NX n,X#Å z È ï Ú YGž ,X Y , + ¦ 9 ,Ì h,X4ç , JÒ>< ÄPool.c [Ê ,X 4 725~4 844·-Õ> !7 ü .E- ,X ¹ 0 Ä ExAllocatePoolWithTag Ñ D 3 Ý,Ì h,XF Ee È E-G á aA|AŽ Ä

y ß 9 È ¢ 4 880> ·-Õ Ô Ÿ È ExFreePoolWithTag Ñ D5×<% Ú ' ! Y , + â âM6,X 0NKÆ Y , + ê5Ù !M6,X0NKÆ Y , + Ü J ü ÔCK È X ä È û,X0NKÆ Y , + È ¢5à £ å Y ,"4 ,X ã.b(Ä4 900~4 929 > ·-Õ ` ä â âM6,X0NKÆ Y , +,X Ü J È4 935~4 965 > ·-Õ `

ä â !M6,X0NKÆ Y , +,X Ü J Ä" È Ü J,X ! ¤ 5 Ê È' ! YGž ,X Y , + !M6 ê â M6,X Y , + D Q 3 0NKÆ,X ÈE- Ã ¹ q B Y , +,X POOL_HEADER ,X PoolType,X ú 0 9.B n ÄV p Ü J ¹ â,X Y , + Ô þ ` H,XNIM6 Èí Ú0NKÆNIM6 &E¬4-2Ï4³ Y , "4 ÈE- 3 EîE›A×*ü MiFreePoolPagesÑ D 9 ` ä,X È?• ··Õ 4 972~4 982> × ú í È Ú „,X Y , + Ä Ã6Ñ Æ4£ Ü J Z J,ÌF•,X Y , + Å ¦ 9 EÖ ',X ¿ ¹>< È?• ··Õ 4 989~5 022> Ä7Ç!8 ÈExFreePoolWithTagÑ D ` ä Z – D P Û Y , +,X ² ¹ 0 Ä

ü base\ntos\ex\pool.q Ê È å ÀE¬ Ã ¹,ß J ª Ô o ÚG! `Gž Y ,,X Ñ D È Bü ÞA† È ;> ' Y ,"4 EîE› ExAllocatePoolWithTag` ExFreePoolWithTag9 ¹ 0,X È 5à è W À 3 ü J ª Y õ + È*î7ÇA' ÛPE |/ß c >•A×*ü,X Y ,1u)Ú Ñ D Ä ExFreePoolWithTagÑ D J"u Ý " ¹ Y , +,X ÛA„ È G TagToFree'u Ý rL ,X*üEè Ä Y ,1u)Ú â2Ï4³ õ +,X0 n û C C,Ì G,X _NM ÈWindows L8 Z ¤ oP¬ ,X Ã ".b(,X Y ,1u)Ú s6Ñ ¹ ê ÈE¬ ¤ o Z J ª Ô o*ü b "# A' ÛPE |/ß c Y ,JíAÃ,XA' ' È J Ù À(M!^ Y , "4 ` Y ,"4C³Cþ Ä å À ü ExAllocatePoolWithTag` ExFreePoolWithTagÑ D Ã ¹,ß E- ø/¡ ,XD• E Ä ' < ,X"4 ÛA„ ¬G£ ExpPoolFlags ,X(M!^ Y ,"4 ÛA„ Ä EX_ SPECIAL_POOL_ENABLEDÅ' Ô Ê È Y , ÚG! Ã6Ñ îE@ MmAllocateSpecialPoolÑ D Ä

(M!^ Y ,"4 Í b!£ õ Y , ÚG! ÈFÑLÔ?UNq ê,X Y , È Î ,X s)Ú È*ü ´ NIM6 Ú Y , + ÚLh Ô È´!8 È Ô º ··Õ é*ü Y , +,X !M6 ê5Ù âM6 È Ú î Ð7È Ô þ Y õ ã ,XA"KÂE± _ È ¢5à S2Ï4³ ý$W È AŒ) ÝJíAÃ,XA' ÛPE |/ß c Ä º ê È(M!^ Y ,"4 3 AŒ üPE |/ß c ÚG! ê5ÙGž Y , Ê ;> Ô oNq ê,X " ¹ Ä

Y ,"4C³Cþ Û B Y ,+ AË `Gž Ê Y , +,X TagÈ9A„),Ì à Tag,X Y , S *ü ™ ‰ Ä å À ü ExAllocatePoolWithTagÑ D È,ß WA×*ü Z ExpInsertPoolTrackerInline Ñ D È5à ü ExFreePoolWithTagÑ D È WA×*ü Z ExpRemovePoolTrackerInlineÑ D Ä Windows,X Y ,1u)Ú <4È x Z Ô ô Tag>< È J A„) Z!£/¡ Tag,X Y , S*ü ™ ‰ Ä´!8 È V p2Ï4³,X Y ,"4C³Cþ s6Ñ ' Ô,XA± È' Ô þPE |/ß c LEQ Ê ÈY ,1u)Ú < Ã ¹ " ¹ W+ AË,X Y , ú Æ4£ <F¼Gž È V pE¬"u Ý <F¼Gž È W Ã ¹A}2Ï4³ ý$W È J Û âA¹PE |/ß c Ý Y ,JíAÃ ÄExpInsertPoolTrackerInline ` ExpRemovePoolTrackerInlineX ··Õ 3 ü base\ntos\ex\pool.q Ê ÈAËAÏ5Ù7¾> ¹,ß ÈE-G á a?·Gž Ä

2Ï4³ 1 5 & ³,X1u)Ú

Þ Ô8V Ÿ4¡ Z2Ï4³ Y ,"4 ` ;> ' Y ,"4,X Y ,1u)Ú È ü Windows,X H þ 0N KÈ ÈL8 Z îA±0NKÈF¼ Ú ¹ ê ÈE¬ Ý ÔF¼ Ú Y , 3 ¹ | Õ Y ,,X • ã 91u)Ú,X ÈE-

2Ï4³ PTE ³ È JCK Ÿ + < ¬G£ MmNonPagedSystemStart n È5à4§ 3 !7 Q ü MmNonPagedPoolExpansionStart Äº ê È ü2Ï4³?š Ò `M2 6NI Y ,"4 KÈ8¹ Ý0NLm È íE-!‰ 8× È,X <F¼ ê ÔF¼ Ú Ä 1/6 Å 3*ü 02Ï4³ PTE ³ È/Ä 2Ï4³ PTE Nq ê È V Ò 4.14 / 5à !5Ù ¹ MmNonPagedSystemStart Ÿ,X ³/Ä 2Ï4³ PTE Î Ä Windows ÚE- øF¼ Ú ³JÒ y ü ÔCKE¯> 1u)Ú È ´!8 È ü 8V ß [ È å À á Ú2Ï4³ PTE ³ ` Nq ê È5à4³/Ä 2Ï4³ PTE ³ Ä

2Ï4³ PTE ³ ¹ PTE ,X 6 ã 91u)Ú,X È ' Y ·-ÕLÔ?U Ô!‰<. ³ 9 ô Ø(=)ÚNI M6 Ê È W Ã ¹ S*ü2Ï4³ PTE ³ ,X 8× È × ' Y ·-ÕLÔ?UNq ê,XM2 6NI ³ Ê È W 3 Ã ¹ S*ü2Ï4³ PTE ³ 9 ô Ø(=)Ú Y , Ä Ý Ô&•AË"¼ ã ÈE-F¼ Ú<. ³ 8× È/Ä 2Ï4³ PTE ³ È JM2>< âE-!‰ 8× È , ,X PTE È5à></ E-!‰ 8× È ¹ PTE ,X 6 ã 9 1u)Ú,X È G ^ PTE ' .C $d 91u)Ú ÄE- Ô8V å À 9A|AŽ2Ï4³ PTE ³,X1u)Ú1k"© ` r)„ Ä º ê ÈM2 6NI Y ,"4,X =) ³ 3 EîE› PTE 91u)Ú,X È ¹ È å À ü ·-Õ î,ß Ý ø F¼ Ú ³ ÈE- EîE› C n 2O _ SystemPtePoolType9 Ú,X Ä ü 8V È å À ¾ G — SystemPteSpace2O _,X PTE ³ Ä

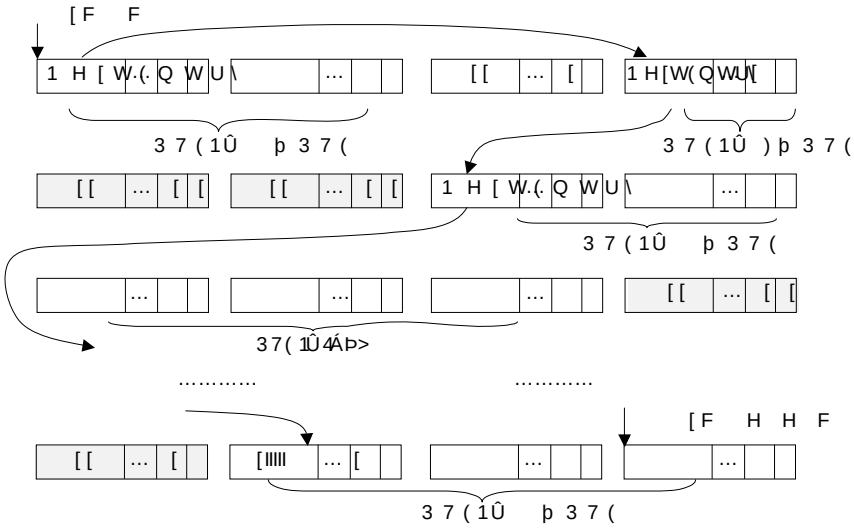
2Ï4³ PTE ³ NIM6,X PTE 3 à ! b2Ï4³ 0NKÈ,XNI>< ³ È G ¢ 0xc0000000 Ô Ÿ,X ³ È ¾ áE› ÈE- o PTE þ ™ Ý';.@ Ê n ,X PTE ã 9?·Gž Ä Í b0NKÆNIM6 ,X PTE È W À J"u Ý Í h,X(=)ÚNIM6 È J PTE>• Ý'; ¹ ß,X D B4§ X 9?·Gž Ö

```
typedef struct _MMPTE_LIST {
  ULONG Valid : 1;
  ULONG OneEntry : 1;
  ULONG filler0 : 8;
  ULONG Prototype : 1;      // MUST BE ZERO
  ULONG filler1 : 1;
  ULONG NextEntry : 20;
} MMPTE_LIST;
```

¢ MMPTE_LIST 4§ X,X n Ã ¹,ß Î È@ Ê PTE ,X PFN ³Ä?• 4.4.18V Å>• n ä Z NextEntryÈ ´!8 È Ã ¹ Ç?• È PTE Ý';JÒ><,X • ã 91u)Ú,X Ä ´ PTE Í h,XNIM6 Ô n NIM6 ÍU$,X È G Ô â 12 ! 0 È ¹ ÈE-G ¾*ü 20 ! 6Ñ><E'2Ï4³ PTE ³ ,X Ô þNIM6 Ä ü y ß 9,X £EÄ È å À ^EîE› PTE Î0ŸCK 9,XJÒ></Ä PTE JÒ>< Ä

ü2Ï4³ PTE ³,X Y ,1u)Ú ÈL8 Z PTE JÒ>< ¹ ê ÈE¬ Ý PTE 1Û,X V É È GE²4Á ,XNIM6 X ä Ô þ1Û ÄPTE JÒ>< ¾ ^1Û ,X PTE E² yCK 9 È1Û,X û ã E- 9?˜ n,X Ö V p Ô þ1Û ¾ Ý Ô þNIM6 È í W,X OneEntry ! ³ 1 × V p Ý î þNIM6 È í1 ` þNIM6 PTE ,X NextEntryNM Ù ÿ ZNIM6 DG£ È3 ŒPTE,X DG£ ÄÒ4.19 / Z PTE JÒ>< ` PTE 1Û Ä J # &D8F PTE ></ á ü0NKÆJÒ>< ÈAÈ â Æ4£>• ±+- Z Ä!£ þ PTE ,X1 1 ! OneEntry ! ÈP¬ 20 ! NextEntryÄ Ò / ,X PTE JÒ><,X ! Ý þ8V&• Ú ÿ Ù ÿ 2 þ Ã 1

þ ` 5 þ PTEÈ ¹ Ë ` þ PTE1Û,XOneEntry !>•5B 1 ÄÔ â Ô þ PTE1Û Ù ÿ 3 þ PTEÈ W,XNextEntry -1 È G 0xfffff Ä



Ò 4.19 PTE JÒ>< ` PTE 1Û/ ã Ò

y ß 9,ß2Ï4³ PTE ³,X PTE1u)Ú1k"© Ä ¹ ß Ô4˜ < ¬G£ n Ö

```
#define MM_SYS_PTE_TABLES_MAX 5
#define MM_PTE_TABLE_LIMIT 16
ULONG MmSysPteIndex[MM_SYS_PTE_TABLES_MAX] = {1,2,4,8,MM_PTE_TABLE_LIMIT};
UCHAR MmSysPteTables[MM_PTE_TABLE_LIMIT+1] = {0,0,1,2,2,3,3,3,3,4,4,4,4,4,4,4,4};

ULONG MmSysPteMinimumFree [MM_SYS_PTE_TABLES_MAX] = {100,50,30,20,20};

PVOID MiSystemPteNBHead[MM_SYS_PTE_TABLES_MAX];
ULONG MmSysPteListBySizeCount [MM_SYS_PTE_TABLES_MAX];

ULONG MmTotalFreeSystemPtes[MaximumPtePoolTypes];
PMMPTE MmSystemPtesStart[MaximumPtePoolTypes];
PMMPTE MmSystemPtesEnd[MaximumPtePoolTypes];
MMPTE MmFirstFreeSystemPte[MaximumPtePoolTypes];
```

D4˜ MmSysPteIndexn Z 5 /¡ û ã,XE²4ÁNIM6 Y , + Ö1 Ã2 Ã4 Ã8 ê 16 È D4˜ MmSysPteTablesí D4˜ MmSysPteIndex¸X2ö é Ä G ß Û Å Ä 'LÔ?U ¢2Ï4³ PTE ³ ÚG!4- n DG£,XNIM6 Ê È!¨ WNumberOfPtesÄ d16 Å È S*ü NumberOfPtes 0 MmSysPteTables¸X ß Û 6Ñ,È y k Ô ã,X è û b1 b NumberOfPtes¸X MmSysPteIndex 2ô,X ß Û Ä ´!8 ÈMmSysPteTables ¤ o Z ¿Eó ¹>< 6Ñ k E- 5 /¡ û ã Ô ÜEÖ,X ß Û ,X6Ñ o Ä

D4˜ MiSystemPteNBHead Ô þG¡?U,X D B4§ X È W !£ Ô/¡ û ã,XE²4ÁNIM6 Y ,

+ n Z Ô þKó ë Ä ' v LÔ?U+ AË Ô þ Y , + È G Ô!‰E²4ÁNIM6,X 8× È Ê È Y ,1u)Ú <,È y ¢ Í h,XKó ë ª Ô + x4- v È8¹Kó ë Y , +,X DG£ £ å Z ÈL! Z MmSysPteMinimumFreeD4˜ n ,XKÜ ¹ ß Ê È2Ï4³ a TKó ë t Ô o,Ì à û ã,X Y , + ÄD4˜ MmSysPteListBySizeCount„) Z!£/¡ û ã,X Y , +,X DG£ ÄD4˜ MmTotalFree-SystemPtesÃMmSystemPtesStartÃMmSystemPtesEnd MmFirstFreeSystemPteÚ ÿA„) Z 2Ï4³ PTE ³ Ä `M2 6NI Y ,"4 = ) ³ Å 0NKÆ PTE,X DG£ ÃCK ŸPTEÃ4§ 3 PTE ` 1 Ô þ0NKÆPTE ÄMmFirstFreeSystemPte,X 2ô,Ì ' b Ô þJÒ>< ÈÛ å1 Ô þ0NKÆ1Û È 2Ï4³ PTE ³ Ý,X0NKÆ1Û,È y ü PTE E² yCK 9 È 6 ä Ô þ PTEJÒ>< È V ! EÄ Ä

' v AË" Gž Y , + Ê ÈV p Í h û ã,XKó ë î Ý0NKÈ Ã o ¦ 9 È í,È y ¦ 9 Kó ë × V p Æ4£E’ A’ n,X Ô ûL$ ê ¦ 9Kó ë Bù È í &E¬ PTE 4È x,XJÒ>< È ™?U Ê Ã ¹ Ü J ä È û,X1Û Ä

ßM6 å ÀA¦AŽ r)„2Ï4³ PTE ³ Y ,1u)Ú1k"©,X ··Õ È ! b base\ntos\mm\sysptes.c [Ê Ä ?U,X Ñ D Ý Ý þ ÖMiInitializeSystemPtes ÃMiReserveSystemPtesÌ MiRelease-SystemPtesÄ

ü2Ï4³,XL !‰ 0 ñ Ÿ êE›/ß È' MiInitMachineDependentÑ D ` ä Z2Ï4³M2 6NI Y ,"4,X ñ Ÿ ê ¹ â È WA×*ü MiInitializeSystemPtesÑ D 9 ;> 2Ï4³ PTE ³,X ñ Ÿ ê È ?• base\ntos\mm\i386\init386.c[ Ê,X 3 295 > ÄMiInitializeSystemPtes Ñ D,X ··Õ ! b sysptes.c¸X 2 247~2 510> Ä WOj A’ n2Ï4³ PTE ³,XCK Ÿ PTE `4§ 3 PTE,X È G MmSystemPtesStart MmSystemPtesEnd Í h b SystemPteSpaceD4˜NM,X 2ô È' â ÚE-!‰ PTE <F¼#ÙLÊ Ä

ü MiInitializeSystemPtesÑ D ÈW 3 ñ Ÿ ê Ô 5)JÒ>< È J !£ þ8V&• Ô + Y , È /Ä chunk ÄMmSysPteIndexD4˜ rL Þ n Z 5 /¡ chunk,X û ã Ö 1 È2 È4 È8 ` 16 Ä ü MiInitializeSystemPtesÑ D Ý Ô þ F¼ D4˜ Lists È n Z!£/¡ chunk,X DG£ È ü Intel x86 G Ä Þ Ú ÿ Ö400 È200 È60 È50 ` 40 ÄE- 3 tCK 9 È E#] ž PTE DG£ 2 080 þ È chunk D 750 þ ÄE- o chunk8V&• D• ¢2Ï4³M2 6NI Y ,"4 ÚG!,X È W À t 9 + < ¬G£ MiSystemPteSListHeadn ,X)JÒ>< Ä' â ý*ü!8)JÒ>< 9 ñ Ÿ êKó ë D 4˜ MiSystemPteNBHeadÈ ´!8 È+ MiSystemPteSListHeadn ,X)JÒ>< Í b êF¼ á a Ã ?• È ¹ â+ MiSystemPteNBHeadD4˜ ,XKó ë7¾ | ª*ü)JÒ>< ,X8V&• Ä G bE-F¼ Ú · -ÕF Ee ÈAË –5×sysptes.c[Ê,X 2 359~2 427> Ä

y ß 9EîE› ¹ ß Ô!‰ ··Õ ` ä ÍE- oKó ë,X ñ Ÿ ê ÈWOj ±+- Ô þ û,X Y , + È âEä þGž Ø/¡ ã Ì,X Y , + ÄE-!‰ ··Õ,X ñCÃ È ý*ü MiReserveSystemPtesAË Ô

þC‡ ó û,X0NKÆPTE 1Û Ä Ù ÿ TotalPtes þNIM6 Å È' â Ý ã + 9Gž E- oNIM6 È MiReleaseSystemPtesÑ D7¾ | ÚE- o ã Y , + t 9 Ø/¡ û ã,XKó ë Ä

```
PointerPte = MiReserveSystemPtes (TotalPtes, SystemPteSpace);

if (PointerPte == NULL) {
  MiIssueNoPtesBugcheck (TotalPtes, SystemPteSpace);
}

i = MM_SYS_PTE_TABLES_MAX;
do {
  i -= 1;
  do {
    Lists[i] -= 1;
    MiReleaseSystemPtes (PointerPte,
            MmSysPteIndex[i],
            SystemPteSpace);
    PointerPte += MmSysPteIndex[i];
  } while (Lists[i] != 0);
} while (i != 0);
```

Ô â ÈMiInitializeSystemPtesÑ D ` ä ñ Ÿ ê ¹ 0 Ä

)„ ü å À 9,ß MiReserveSystemPtes V) ÚG!M2 6NINIM6,X Ä W ¾ Ý ø þ – D Ö NumberOfPtes ÛNIM6,X DG£ ×SystemPtePoolTypeÞe Ý ø/¡ Ã6Ñ ÖSystemPteSpacê NonPagedPoolExpansionÈnå À ¾5×<%SystemPteSpace,X ™ 6 ÄOj B NumberOfPtes– D,X .B n hA¹ S*ü ¾/¡ û ã,XKó ë ÈV p6Ñ ¢Kó ë ¤ ª Î Ô þ8V&• Èí,È y ^Kó ë8V &• ,X Y , + Ä GCK Ÿ PTEÅ?· Î 9E¨ ²4- v Ä5à è È V p!8/¡ û ã,X Y , + DG£ ã b NX n,X Ô ã D ÈG MmSysPteListBySizeCountD4˜,X Í h 2ô ã b MmSysPteMinimumFree D4˜,Ì h,X 2ô È íA×*ü MiFeedSysPtePoolÑ D È ¹9‹ k È î,X!8/¡ û ã,X Y , + Ä MiFeedSysPtePoolÑ D,XF Ee \1T) È J ··Õ ! b base\ntos\mm\sysptes[dÊ,X 475~538 > È W ~)ƒ 10 õ È!£ õA×*ü MiReserveAlignedSystemPtesÑ D9‹ k Û n û ã,X PTE Y , + È' âA×*ü MiReleaseSystemPtesÑ D7¾ | ¦ 9 ,Ì h,XKó ë Ä J4§ p,Ì ' b T(M n ,XKó ë ¦ 9 10 þ Û n û ã,X PTE Y , + Ä

² MiReserveSystemPtesÑ D È V p – D NumberOfPtesÛ n,XNIM6 DG£CYE› Z 16 È ê5Ù ¢Kó ë ´"©9‹ k Û n û ã,X Y , + È íA×*ü MiReserveAlignedSystemPtesÑ D + AË „„X Y , + È JE¨ ² Ä

¹ È å À)„ ü 9 , ß MiReserveAlignedSystemPtesÑ D , X F E e Ä A ¹ Ñ D ! ¨ MiReserveSystemPtesîÔ þ ÍU$ – D ÄMiReserveSystemPtes A×*ü!8 Ñ D Ê ÈA’ n ÍU$ – D 0 È ´!8 å ÀE-G á5×<% ÍU$,X ™ 6 ÄMiReserveAlignedSystemPtesÔj ¢1 Ô þ0N KÆPTE Ô Ÿ ÈG MmFirstFreeSystemPteD4˜,X 2ô È ü Ô þ while ~)ƒ R ÜEÖ û ã,X

0NKÆPTE 1Û È?• ··Õ 672~781> ÄE- Ô þNN c ? £E›/ß È V p R 1 Ô þ$µC‡ 5 Ê,X 1Û D Q ?U" ,X û ã È í ;> ExactFit Ú È ^A¹1Û ¢0NKÆ1ÛJÒ>< ,L8 ß 9 × ú í È R ,X1Û û b ?U" ,XNIM6 D È í ^ s 9,X1Û4ý ã È âM6,XF¼ Ú 0 4§ pNIM6 Ä V p ÍU$ – DCYE› Ô þNIM6 È í ? £F Ee È t á Ô o È Bü Þ ¡' R $µC‡?U" ,X PTE 1Û Ä

Ô â È „E- oNIM6 PTE,X.@ Ê ¿>< ÄTLB ÅNM Ä' âE¨ ² Ä

)Ú?· Z+ AË PTE,XE›/ß ¹ â È₫ À)„ ü 9,ßGž PTE,XE›/ß È?• MiReleaseSystemPtes Ñ D È J ··Õ ! b sysptes.c[Ê,X 1 822~2 129> ÄA¹ Ñ D,X – D Û n Z?UGž ,X PTE CK Ÿ !5B ` þ D È ¹ ž PTE ³,X2O _ Ä à È å À ¾5×<% SystemPteSpace,X ™ 6 È G2Ï 4³ PTE ³ ,X PTE Gž E›/ß Ä üA×*ü!8 Ñ D ¹ ! È Û n8× È,X PTE ™NO ´ ,X È 3 AÈ È Í h,X<. ³ "u Ý>• ô Ø (=)ÚNIM6 Ä ¹ È MiReleaseSystemPtes Ñ DOj ^E- o PTE <F¼#ÙLÊ Ä V p YGž ,XPTE DG£ ã b1 b 16 È í5×<% ^E-!‰PTE 8× È ¦ 9 MiSystemPteNBHead D4˜ Û,XKó ë È5à á ,È y ² 0NKÆ PTE JÒ>< Ä –?• ··Õ 1 901~1 974> Ä

V p ¦ 9Kó ë á ä s È ê5Ù PTE DG£CYE› Z16 È íLÔ?U &E¬ PTE JÒ>< ÄOj ¢ 1 Ô þ0NKÆPTE Ô Ÿ È G MmFirstFreeSystemPte D4˜,X 2ô È ü Ô þ while ~)ƒ R 1 Ô þ J NextEntry ³CYE› ' !CK Ÿ PTE,X0NKÆ1Û È?• ··Õ 2 004~2 128> ÄE- Ô þNN c ? £E›/ß È ´ PTE JÒ>< Ý'; âNN c f ë,X Ä R E- ,X0NKÆ1Û ¹ â È Oj 5× <% ú6ÑC³ W Ü J ä Ô þ È û,X0NKÆ1Û È V p!80NKÆ1Û,X2û âM6 D Q ?UGž P,XTE 8× È È í Ú ø5Ù Ü JCK 9 È?• ··Õ 2 030~2 048> × V p á6Ñ Ü J È í ¦ 9 Ô þ „,X0NKÆ1Û ü W âM6 È?• ··Õ 2 060~2 080> Äy- È V p?UGž ,X PTE 8× È D Q2ûC ß Ô þ0NKÆ1Û È í Ú ø5Ù Ü J È?• ··Õ 2 088~2 111> Ä' â Ñ D4§ 3 Ä

Ô â1T) ã4§ Ô ß È2Ï4³ PTE ³ Û ^ PTE ' .C $d 91u)Ú È E- o PTE Ý';NN c X ä Z Ô þ)JÒ>< Ä ' Y ··ÕEîE› MiReserveSystemPtes AË k Ô!‰E²4Á,X PTE Ê È W ™NO7¾ Å ô Ø(=)ÚNIM6 ÄMiReserveSystemPtes ™ ™E¨ ² ZE-!‰PTE,XCK Ÿ È W J áBóB÷ ? PTE ,X Y • Ä Í/Ä È ' Y ··ÕA×*ü MiReleaseSystemPtes Ñ D 9Gž PTE 8× È Ê È W ™NO ?·L8E- oPTE,XNIM6 ô Ø ÄE- ø þ Ñ D ¶ Ã ¹*ü b Í2Ï4³ PTE ³,X Y ,1u)Ú È 3*ü bM2 6NI Y ,"4 =) ³,X Y ,1u)Ú È GK ,X ÿ ü b Ö2Ï4³ PTE ³,X1u)Ú1k"©G›*ü Z 5 þKó ë 0 4ç , È ¹4ç?·Ne4 ,X ±+- `Gž ¡ 0 ú 9,X ÔJÔ × 5àM2 6NI Y ,"4 = ) ³ þ é 9Kó ë4ç , È ¹ W,X ±+- `Gž ,È y ? £ PTE JÒ>< Ä ü Windows 2Ï4³ È2Ï4³ PTE ³ ?U*ü b I/O Ã Y Ü1 | Õ ô ØNIM6,X ™ 6 È5àM2 6NI Y ,"4 =) ³ ™*ü bM2 6NI Y ,"4,X =) Ä

Windows *Y s)Ú â r)„*

Windows I/O 2Ï4³

ü)„ · ¡ 02Ï4³ È I/O ÄInput/OutputÈEg 9/Eg Î Å Au1k ` ä Ø/¡ s6Ñ,X Ô þG¡ ?U •M6 ÄØ)Ú <BóB÷ ;> Ø/¡Au1k Ï u È J èEîE› Y , 4“ ¡4‰ H þ Y ,0NKÈ È 0 Ô þ)„ r Ã*ü,XAu1k 2Ï4³ È™ ™ K ÛE- ,XAu1k ` Y ,A“KÂ6Ñ oE¬ á ó ÈE¬?U Ý Ø/¡ êF¼ A’ Û,X – â ! Ã SAu1k ,ó!7 Ý*ü Ä ü Ô Ä L _,X þ ŽAu1k È ?•,X êF¼A’ Û ê êF¼ y · Ù À ÖK ,¬ ÃTô Û Ã.@,¬ Ã ,¬PE | < Ã / < Ã ' DEg Î Ã ÄMÇEg Î Ã5%4°EÖ G! < y · È¹ ž £ 1 Ä 1uE- oA’ Û,X s6Ñ `*üEè Ø ã Ø È Ø)Ú < ý*ü Z Û š ,X y · T ÈEîE›A’ Û,X { < â W À ' xF' È´!8 È¢.@ Ê M6 Þ È Ø)Ú < Õ,X y · T Au1k 2Ï4³6Ñ ó # 0E¤> ,X Î. Ä

¢EC Ê M6 Þ È¡ 02Ï4³ ™NO ¤ o,Ì h,XEC Ê 9 ¡4‰E- oA’ Û,X { < ÈJ è n Í h,XEC Ê y · ê2Ï4³ á u È S k h*ü/ß c Ã ¹ • “ ¡4‰ ê S*ü êF¼A’ Û Ä5à è È ü Ô þ î Ï u Ã îE¯/ß ¡ 02Ï4³ ÈE- o êF¼A’ Û E •,X È ¹ È¡ 02Ï4³ ™NO #A× Í êF¼A’ Û,XA“KÂ Ä L _,X ."© È h*ü/ß c á,È yA“KÂ êF¼A’ Û È5à EîE› ¡ 02Ï4³ 9 ` ä ÍA’ Û,XA“KÂ ÄWindows 0 Ô þEî*ü ¡ 02Ï4³ È ¤ o Z Ô + Ã =),X I/O Ø)Ú Š È¢5à AŒ1 Ý •.@ Ê V 4ê m çK¼,X2Ï4³ õ + 9 { J.@ ÊA’ Û Ä 0´ ÚE- Ô I/O Ø)Ú Š/Ä Windows I/O õ _ È W ÍAu1k êF¼A’ Û ¹ 0 s)Ú,X Ô þ ‘B5 È ¢5à S k Ø/¡.@ ÊA’ Û FÑ6Ñ ó4‡ 9 E- Ô õ _ Ä

ü Windows I/O õ _ È*ü b { êF¼A’ Û,XEC Ê õ +/Ä A’ ÛPE |/ß c Ä Device Driver Å È W ÀE¤> ü(M õ ã ß È G Y õ ã ß È ¹ W À,X ··Õ â Y ··Õ K Ý à1 ,X ;> L$ Ä ´!8 ÈA’ ÛPE |/ß c ™NOFI ~ Y ··Õ ™NOFI \,X Ô Û?˜ í È!¨ V IRQL ?U" Ã Y ,1u)Ú?˜8×1 Ä º ê È!8 I/O õ _ 3 Windows ¡ 02Ï4³,XEC Ê =) õ _ ÈE-

ã G- È Ô þA’ ÛPE |/ß c Ã ¹ â.@ ÊA’ Û!¿ ´ G6(È5à ™ ™ =) Y ,X s6Ñ È ê5Ù+ b J ª,Â,X5àLÔ?U ü Y ;> ·-Õ Ä Windows,XAŒ î2Ï4³4˜ Ê 3!7 ¹A’ ÛPE |/ß c,X 6 ã5à ¤ o,X Ä ´!8 ÈA’ ÛPE |/ß c JM2,ó,X?U PE | Ô þ.@ ÊA’ Û Ä

üE- Ô0´ È å ÀOj Ÿ4¡)„ ·Au1k 2Ï4³ I/O ,X ¹ 0 • ã È J ' Ÿ4¡ Windows Y ,X I/O 2Ï4³4§ X Ä' â Ú ÿA|AŽ Windows I/O2Ï4³,X Ý ûF¼ Ê ÖI/O 1u)Ú < Ã G ¦ G*ü1u)Ú < â+ $d1u)Ú < Ä y ß 9A|AŽ Windows ,X I/O õ _ È Ÿ4¡A’ ÛPE |/ß c,X Î 4§ X ¹ ž I/O Ø)ÚE›/ß Ä Ô â È Ÿ4¡ Ô þ Ã,¥?š2Ï4³ I/O AË" ` ä ™ ‰,X ¹ K IRPMon Ä

* VEØÄ

Í bAu1k ,X Ø)Ú < 9AÈ ÈI/O .@ ÊA’ Û J r ¾ Ô o0ú Ü ¤ o y ·?˜8×,X { <5à Æ È Ø)Ú < J á,È y âA’ Û ' xF' È5à åA’ Û { < ¥ Ë ‘ ¸ È ê5Ù y A’ Û { <,X Eî-¹ ê Q ¸ ÄE- Ô8V å ÀOj A|AŽ)„ ·Au1k 2Ï4³,X I/O T È ¹ ž ¡ 02Ï4³ #] ž I/O ,XEC Ê T È' â Ÿ4¡ Windows,X I/O 2Ï4³4§ X Ä

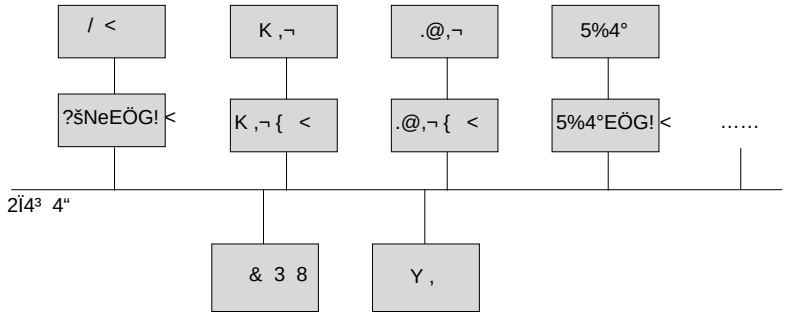
)„ ·Au1k 2Ï4³,X * 0

Ý'; ô4³,X Ú2O •"© ÈI/O A’ Û Ã ¹ Ú +A’ Û ` +0úA’ Û Ä £.•,¬ Ã ,¬ L _,X + A’ Û È Ï `AÏ m ¡ 0FÑ ¹ +) !E¯> ,X Ä º Ô2O +0úA’ Û È W À y ê ¥EÕ,X D B +8V# È5à á D B + Ä L _,X +0úA’ Û ÝK ,¬ `Tô Û ÄE-/¡ Ú2O •"© ¹A’ Û D B,X4˜4›) Î. È W ' EÖ*ü b)4ƒ ¹ ôEg D B 0 x f • ã,XA’ Û Ä' 5à È Ý o êF¼A’ Û È!¨ V ÊJs ¥*ó < Ã+ $d { <1 È ' ¶ á6Ñ & +0úA’ Û È È á î +A’ Û Ä

1uE-/¡ Ú2O •"© J á6Ñ D ' #‰,ª Ý Ã6Ñ,XA’ Û È È W7Ç å Ú +A’ Û 0 Ô /¡2O ÿ ¤ Z Î 9 Ä)„ · ¡ 02Ï4³ T TJ\ Í +A’ Û S*ü çK¼,XEC Ê4§ X È¨ VA’Au [Ê2Ï4³ Ê ¾NO5×<% ‘B5,X +A’ Û ÄAÌ V +,X û ã Ã D1 Ã ¹+ (M n,XG!5B – D 9 { Å È5à r L ,X +A’ ÛAÏ mE›/ß í+ È " ,XPE |/ß c 9 Ø)Ú Ä

Ø)Ú < T T ¾C³A’ Û,X { < ' xF' È5à á,È y ¡4‰A’ Û ÄØ)Ú < â { < KÈEîE› 4“E¯> Eî µ È5à { < âA’ Û KÈ,XEî µ í T TEîE› çK¼,X y ·E¯> È V Ò 6.1 / Ä E- o { <,X s6Ñ Ã6ÑM2 1T) È¨ V £K ,¬ { < È W ¾ Ø)ÚK ,¬ ? £-Õ ¹ ž â2Ï4³E¯ > 1T),XEî µ × Ý o { <,X s6Ñ Ã6ÑM2 á È¨ V)„ ·,X.@,¬ { < È L8 Z Ô Î ,X { .• AÏ m D B,X6Ñ o ¹ ê È E¬ ¤ o Z õP` D B,X s6Ñ È ¹ ž á ã,X4ç ,0NKÈ Ä Þ Ô0´

Ÿ4¡,X • { < 3 Ô/¡ { < ÈJ(M!^ Ø ü b ÈEîE›4- Ø)Ú <,X Ô þ1u6î t Þ+ µ Ë È¢5à ' • Ø)Ú < ' !,XE¤> ÄÆŒ îA' Û ý*ü • { < 9Eî-¹ Ø)Ú < ¤ o _ ™,X ¥ *ó È!¨ VA' ÛPE |/ß cAË" ,X D B Æ4£ š Û 4¾ Ä ü Þ Ô0´ å À Æ4£,ß Z Windows V) ý*ü Intel x86 Ø)Ú <,X • 9 r)„4³ Ô,X • Ø)Ú Ä



Ò 6.1 Au1k I/O .@ Ê õ _

A' Û { < T T Ý Ô o(Š Õ ˜ , < ê5Ù Q ¸ ˜ , < È 5à Ø)Ú < Ã ¹EîE› ¡4‰E- o ˜ , < È ¢5à { ,Ì h,XA' Û È!¨ V A• { < ¥EÕ D B Ã y D B Ã ' Ô ê GKÁ ¤ o(M n,X s6Ñ Ä ¹ È ¡ 02Ï4³,X Ï u BA' Û,X ¹ 0 õ ã ÈAÏ ê mE- o ˜ , < È ¢5àE' { êF¼A' Û,X,Â,X Ä

{ < L8 Z(Š Õ ˜ , < ê5Ù Q ¸ ˜ , < ¹ ê ÈÃ6ÑE¬ Ù ÿ Z Ã o Ø)Ú <AÏ m,X D B 4ç † È_ V +A' ÛLÔ?U Ô þ •FÑ Ã ¹A“KÂ,X4ç † *ü b ôEg D B ×?šNeEÖG! < T T Ý Ô!‰?šNe Y , 8× È È AŒ Ø)Ú < ¡4‰ / <,X #)Eg Î4§ p Ä

å À 9,ß Ô ß Intel x86 Ø)Ú < ¤ o,XA' Û y · s6Ñ ÄOj È Intel x86 Ø)Ú <L8 Z Y , 0NKÈ ¹ ê È º ê n Z Ô þ I/O 0Ã · Äport Å0NKÈ È Û ¸ in ` out *ü b ¡4‰0Ã ·0NKÈ ,X D B) Ä _ V È ü ßM6,X" 4ê Û ¸ Ö

```
out 21h, al
```

0x21 8259A • { <,X • #; ˜ , < ÄIRR È Interrupt Mask Register ÈA¹ Û ¸ Ú Intel x86 Ø)Ú <,X al ˜ , < ,X m • { <,X { ˜ , < È¢5àE' #; ¤ o • µ Ë,X,Â,X Ä2O È ü ßM6,X" 4ê Û ¸ Ö

```
in al, 20h
```

0x20 8259A • { <,X!7 ü á u ˜ , < ÄISR È In Service Register ÈA¹ Û ¸ Ú!8 ˜ , < ,X(Š Õ ôEæ Ø)Ú <,X al ˜ , < Ä ü Intel x86 Ø)Ú < È in ` out Û ¸,X I/O

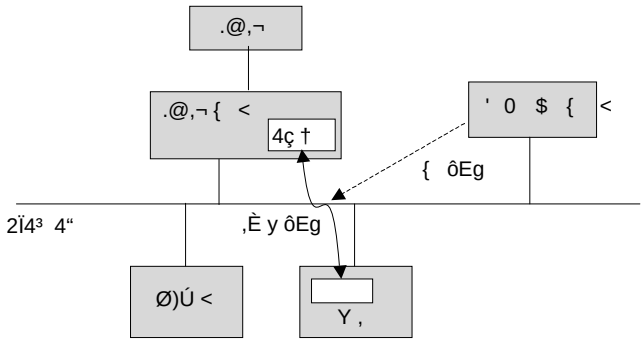
0Ã · ¡ 0 D Ã ¹ 8 ! ê 16 ! Ä S*ü dx ˜ , < ÅÈ5à I/O 0Ã ·,X Ã ¹ 8 ! Ã 16 ! ê 32 ! Ä

A’ Û { < ,X ˜ , <L8 ZEîE› I/O 0Ã · 9A“KÂ ¹ ê È3 Ã ¹>• ô Ø 2Ï4³ Y ,0NKÈ Ä E-/¡A“KÂ • /Ä Y , ô Ø I/O Ämemory-mapped I/OÅ Ä _ V ÈAPIC • { < ,X ˜ , <>• ô Ø 4 KB û ã,X APIC ˜ , < 0NKÈ È5à APIC ˜ , < 0NKÈ œ>• ô Ø 2Ï4³ Y , È J Î Ã ¹EîE› APIC Î ˜ , < Ä G IA32_APIC_BASEÈ Intel x86 Ø)Ú < ,X Ô þ MSR ˜ , < Å 9A’ n ÈT¬Ax 0xfee00000 Ä

Ô ºA’ n Z Y , ô Ø I/O ,X 8× È ¹ â È ' Ø)Ú < Ï !8 8× È Ê È W rL Þ A“KÂ,X á a s Ÿ Y ,0NKÈ ,X , |) È5à A’ Û ô Ø,X D B) Ä Intel x86 Ø)Ú < ¶ Õ I/O 0Ã · 0NKÈ È 3 Õ Y , ô Ø I/O Ä º Ô þ L _,X Y , ô Ø I/O ,X _ $ È ?šNe4ç † >• ô Ø Y , 0NKÈ È´5àEC Ê Ã ¹,È yA“KÂ #) Þ / ,X £2ô Äü ½ ó ,X IBM PC È ¢ 640 KB 7Ç1 MB KÈ,X çK¼ ±+-4-A’ Û,X D B4ç † È J Ù À)8F ` =8F VGA ,X / 4ç † Ä

´!8 È Ø)Ú < Ã ¹EîE› in/out Û ¸ ê5Ù,È yAÏ m Y ,,X • ã â Ø/¡ { < ' xF' ÈFw ÈA’ Û ü ;> Ï u Ê È V) Ú Ï u,X(Š Õ ¡O\4- Ø)Ú < 6 Û Ô/¡ ."© ÈA’ Û { < ¤ o Ô þ(Š Õ ˜ , < È ´5à Ø)Ú < Ã ¹ n ó ê5Ù*ü -1 Y Äbusy-waiting Å,X • ã ” ¹!8 ˜ , < Ä' 5à ÈL8M2?U1 Y,X ÊKÈNXAu á \KS È ú í -1 Y,X ."© hA¹FS ! Ä º ê Ô/¡ . "© ÈA’ Û*ü •,X • ã 9Eî-¹ Ø)Ú < Ä ' Ø)Ú < y • µ Ë Ê È W Ã ¹ B •,X A’5B ê5ÙA’ Û ˜ , <,X(Š Õ È 9 0,Ì h,X Ø)Ú Ä

Í b åG£,X D B x 6 È ê5Ù £ VGA / 4ç † E- Î n 8× È,X D B ô Ø È S *ü ÞEÄ ."© ÜEÖ,X Ä È Í b £.•,¬E- LÔ?U ûG£ | Õ D B x 6,XA’ Û È V p Ø)Ú < S*ü I/O ˜ , <Eä þ Y ,) E¯> A“KÂ È ê5ÙEîE› Î n 8× È,X D B ô Ø È í á ™ , ª)[áP¬ È5à è Ø)Ú < ¡ 0 3 U á “ Ä Í bE-/¡ ™ 6 È)„ ·Au1k Eî G›*ü Ô/¡ /Ä ,È y Y ,A“KÂ Ä DMA ÈDirect Memory AccesÅ,X • Ä DMA LÔ?U.@ Ê,X Õ È W 3 Ô/¡ { < Ä ¶ Ã ¹ H þ2Ï4³ E • Ô þ DMA { < È 3 Ã ¹A} Ô þA’ Û È!¨ V.• ,¬ È Ý)(À,X DMA { < ÈE- ª ‡ b.@ Ê,XA’Au Ä DMA { <EîE›2Ï4³ 4“ 9 ôEg D B È W ü ôEg D B Ê á 4*ü Ø)Ú <,X Û ¸ < ó È ¹ È S*ü DMA Ã ¹ Ú Ø)Ú < ?· Î 9 Ä ' D B ôEg ` ä Ê È DMA { < ¹ •,X • ãEî-¹ Ø)Ú < Ä Ò 6.2 / Z EîE› DMA { < 9AÏ m.@,¬ D B,X.@ Ê4§ X Ä



Ò 6.2 DMA D B ôEg/ ã Ò

Ø)Ú <EîE› DMA { < ,X ˜ , < Í D B ôEgE¯> A’5B ÈÛ n AÏ m D B ü Y , ,X Ã DG£ È ¹ ž ôEg • å Ä V p á S*ü DMA { < ÈFw Ø)Ú < ™NO7¾ ÅEä þ +8V êEä þ + ü.@,¬ { < ` Y , KÈ ôEg D B È D B,X ôEgEîE› 4“ 9 ` ä Ä5à S*ü Z DMA { < ¹ â ÈDMA { < · Ó Ø)Ú < 9 . à ,X _ ™ È WEä þ +8V êEä þ + å .@,¬ { < ¥EÕ Q ¸ È à EîE›2Ï4³ 4“ 9 ` ä D B ôEg Ä ' D B ôEg ` ä ¹ â È W • Ø)Ú < È´!8 È ' Ø)Ú < y • Ê È -¹F' D B Æ4£ ü Y , Û n,X • È ê5Ù Æ 4£ m .@,¬ { < Z Ä

DMA { < y Z Ø)Ú <,XAÏ ª.@,¬ D B,X Q ¸ Ê È îOj A•.@,¬ { < È Ú?U AÏ ª,X D B .@,¬ { <,X4ç † Ä¢.@,¬ .@,¬ { < KÈ,X D B ôEg EîE› ç *ü y · ` ä,X È áLÔ?U S*ü2Ï4³ 4“ È8Eî µ ` < á «.@ Ê2Ï4³ J ª õ +,X E ¡ Ä ' D B E’.@,¬ { <,X4ç † È J èEîE› Z õP` `P`A• ¹ â ÈDMA ôEg Ã ¹E¯> Z È y ß 9,X D B ôEgLÔ?U*ü 2Ï4³ 4“ Ä

' DMA { <EîE› 4“ å.@,¬ { < ¥ ÎAÏAË" Ê È•,¬ { < ¶ á-¹F' 3 á G — !8AË" 97¾ Ø)Ú <E¬ DMA { < È+ b?U m,X Y , Æ4£ ü 4“,X 4“ Þ Z È ¹ È•,¬ { < ¢ Y ,4ç † ª Î ' !?U ôEg,X + È Ú WEÕ 4“ Þ ÄE- ` ä Z Ô þ +,X ôEg ÄDMA { <*üE-/¡ •"© È Ú Ø)Ú < Û n?UAÏ ª,X Ý +Eä þ ôEg Y , Ä' â å Ø)Ú <AË" • Ä å.@,¬ m D B,XE›/ß2O È ¾ • å,Ì ¡ ÈE-G á a Ÿ4¡ Ä

1T) ã4§ Ô ß È ü)„ ·Au1k '2Ï4§ X È Ø)Ú <EîE› I/O 0Ã · ê5Ù Y , ô Ø I/O ,X • ã â.@ ÊA’ Û,X { < ' xF' È5àM2,È y ¡4‰.@ ÊA’ Û ÄIntel x86 Ø)Ú < ¤ o Z in/out Û ¸ 9A“KÂ I/O 0Ã ·0NKÈ È J è 3 Õ Y , ô Ø I/O Ä Z ü Y , âA’ Û KÈ ôEg ûG£ D B È„ ·Au1k T TG›*ü DMA 4§ X È¹ “ Ú Ø)Ú < ¢ D B ôEg ï u ?·7 Î 9 Ä' DMA D B ôEg ` ä Ê ÈDMA { < ¹ •,X • ãEî-¹ Ø)Ú < Ä

* ÐC Ê T

Z?· ZAu1k I/O .@ Ê T ¹ â ÈE- Ô8V å À 9A|AŽ I/O EC ÊA'Au T Ä ¢ ¡ 02Ï 4³?¦ z5à?Ô ÈI/O EC Ê,X õ _ hA¹ A' Û ´ G,X È ´5à È2Ï4³ Ã ¹ Õ Ø/¡A' Û È*î7Ç þ 9 Î)„,XA' Û ÄJ\ Í I/O A' Û,XEC Ê õ _ ™NO ÝC‡ ó,XEî*ü û È7Ç å6Ñ ó Ú Þ8V Ÿ 4¡,X Ø/¡ I/O .@ Ê(M û#‰,ª õ _ Ä º ê È ¡ 02Ï4³ ™NO ¤ o Ý ,X1u)Ú !‰ È ¢ 5àA}A' Û,XEC Ê4˜ Ê=a 9 2Ï4³,X I/O Ø)Ú Š ÈE- ÈE- oEC Ê4˜ Ê Ã ¹ ç"¼ bJ\ Í(M nA' Û,X s6ÑLÔ" È5à á ™E› î 5×<% â2Ï4³ ' xF' ê5Ù â2Ï4³ J ª õ +,X # 0 Ä _ V ÈJ\ Í.•,¬AÏ m,XEC Ê4˜ Ê ´NO5×<%.•,¬ Þ,X [Ê2Ï4³ Ä

A' Û,XEC Ê4˜ ÊEî /Ä A' ÛPE |/ß c Ädevice driver Å È ê1T/ÄPE |/ß c ÄA' ÛPE |/ß c ê5Ù+ A' Û,X.@ Ê V ¤ o Èê5Ù+ ¡ 02Ï4³ V ¤ o Ä+ bA' ÛPE |/ß c,È y â .@ Ê ' xF' È W ÀLÔ?U Ô n,X(M !6Ñ ¡4‰.@ ÊA' Û È ¹ ÈPE |/ß cEî E¤> ü Ø)Ú < ,X(M õ ã ß ÈJ ·-Õ â ¡ 02Ï4³,X Y ·-Õ • Ý à ,X(M ÄE-/¡A'Au,X Ô þ%0 ü â p ÈPE |/ß c ,XJíAÃ Ã6Ñ î Ð7È H þ ¡ 02Ï4³ ý$W Ä´!8 ÈPE |/ß c,X ·-Õ T TLÔ?U4£ E›2' —,XA'Au Ã " ¹ `A×A© È J ·-Õ?˜ õ h Ã6Ñ ã Ä ¢ ·-Õ s6Ñ æ Ú,X?¦ z 95×<% È h Ã6Ñ ^ ·-ÕF Ee/Ï h*ü/ß c È5àA}PE |/ß c ¾ . Ô ™?U,X _ ™ Ä

âA' Û G6(,XPE |/ß c È J Ô Î ,X s6Ñ È Ú ¡ 02Ï4³,X s6ÑAË" È?·Gž äJ\ ÍA¹ A' Û,XAË" È â ¡4‰A' Û ¹ ` äA¹AË" È Ô â Ú4§ p ¹ Û n,X • ãE¨ ²4-A×*ü5Ù Ä ü!8 E›/ß È Ý o _NM T T PE |/ß c ™NO?U5×<% J?· ‡,X Ä ßM6Eä ÔA|AŽ Ä

Oj È âA' Û,XEî µ à!9 ê Ö!9 • ã Ä¢EC Ê { # ,X?¦ z È à!9 • ã,XEî µ • ç r)„ È5à èJíAÃ Ø)Ú ` 6 á 3,Ì Í • ç Ä8¹ Ô þ I/O AË" Ö!9 • ã È í Ø)Ú < ü å.@ Ê ¥EÕAË" ¹ â È J Û ¸# E¨ ² Þ Ô4{A×*ü ·-Õ È!8 I/O AË" >• Õ5BCK 9 È Ø)Ú <,X Û ¸ # E@5à ;> J ª á qC* b!8 I/O AË" 4§ p,X Ï u Ä 'A' Û êA' Û { < ` ä ZA¹AË" Ä!¨ V DMA D B ôEg Å¹ â È W • Ø)Ú <,X ' ! Û ¸# È y A¹AË" ,X ` ä ™ ‰ Ä Ø)Ú < ™NO ü • Ø)ÚE›/ß Ú s >• Õ5B,X I/O AË" y E› 9 È4»4ÁA¹AË" â4Á,X Ø)Ú Ä

Ö!9 • ã,XEî µ<Q' á È Ã ¹ ¤P¬ Ø)Ú <,X ý*ü)[È´5à ü)„ ·Au1k 2Ï4³ >• S"¯ G›*ü Ä´!8 ÈA' ÛPE |/ß cL8 Z?U ¡4‰A' Û { < ÈE¬ ™NO é 9 • Ø)Ú ·-Õ È ¹ ` ä Ö!9Eî µ,X â F¼ Ú Ï u Äü Þ Ô0´ å À,ß È Windows ¤ o Z Ô + • Ú ¥ È AŒA' ÛPE |/ß c ü á ¡4‰ Ø)Ú <,X IDT ,X ™ ‰ ß È å2Ï4³ r t • á u _/ß Ä5à è È ü • Ø)ÚE›/ß È Ô o áFw 2û ù,X Ï u Ã ¹ DPC ` ä È ¢5à4ý-Á Ø)Ú < 0+- üP¬IRQL Þ,X ÊKÈ Ä

üA'Au I/O PE |/ß c Ê º Ô þ T T?U5×<%,XKÂNl 4ç † 1u)Ú Ä á àA' Û Í b D B ôEg

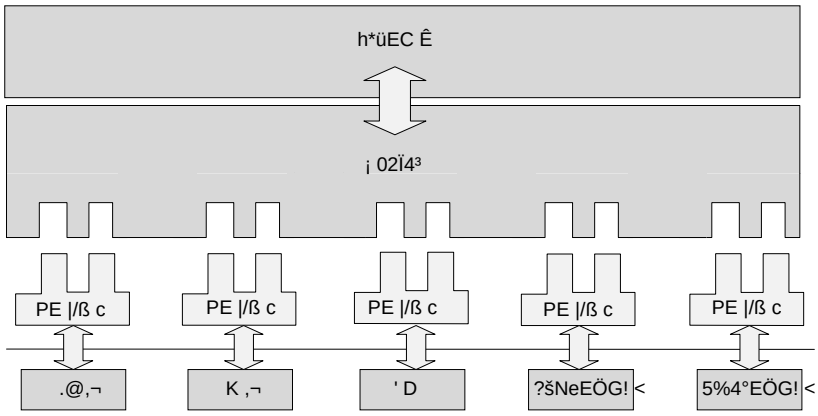
,X)[Ý á à,X?U" ÈA@ V È r Ê û?U" P¬,XEC Ê êA' Û h Ã6Ñ £ å D B ËBñ,X õ D × PE |/ß c Z ¤P¬A' Û,X I/O ò äG£ È Ã6Ñ î Ú D B4ç ,CK 9 È5à á 0Ÿ G ¥EÕ Ä Ý oA' Û ?U" ,È y S*ü(=)Ú Y , × Ý oA' ÛPE |/ß c,È y S*ü h*ü/ß c ¤ o,X4ç † ¹ £ å D B ËBñ õ D ÄPE |/ß c,X4ç † 1u)Ú,Ì Í!¨EW á È ø JG›*ü Z Ö!9Eî µ • ã ¹ â È4ç † 0 Ô/¡ ÝL$,XC $d È ÈLÔ?UAü " A'Au `1u)Ú È ¹FS !C $d"˜$ã ê á D ' G¡ á S*ü Ä

º Ô þ k ¤ ž,XKÂNl E • `(À 4A' Û Äü)„ · ¡ 02Ï4³ ÈA' Û 0 Ô/¡ @ EC $d ÈŒî î þ/ß c*î7Ç î þ*ü E •,X ÄA@ V È < Þ,X.@,¬ T T 2Ï4³ Ý*ü E •,X È Ï)# |,X h*ü/ß c È ¾?U Ý L$AŒ Ã ÈFÑ Ã ¹A“KÂ W À Ä Í b.•,¬A' ÛPE |/ß c5à?Ô È!£ þ/ß c,X.@,¬ I/O AË" FÑ (À0Ÿ,X ÈE- o I/O AË" Ã ¹ J , Ä' 5à È Í b Ý o A' Û È¨ V ' D È Ô þ h*ü/ß c ™NO ¹(À 4 • ã S*üA¹A' Û Ä J ¥ ¡ h ø þ h*ü/ß c ,X ' DAË" È Ú î Ð7È ´ ,X ' D4§ p ÄE • `(À 4 • ã,XA' ÛA“KÂFÑ Ý Ã6Ñ î é ¥ Þ Ô 0´ ¤ ,X Ô o J ¥ ûKÂNl È¨ V!OJÕ Ä FS !E- oKÂNl ÈLÔ?U ¡ 02Ï4³ `A' ÛPE |/ß c # à ¹ 0 ¹ '. E- oKÂNl,X Î 6 ä 5 Ê Ä

L8 Z ôEg D B ÈA' ÛPE |/ß c º ÔNMG¡?U,X6 B÷ A' Û,X(Š Õ1u)Ú ÈÙ ÀA' Û ñ Ÿ ê Ã G ¦ G*ü Ã+ $d1u)Ú ¹ žJíAÃ Ø)Ú1 ÄJ G ¦ G*ü `+ $d1u)Ú ¡ 02Ï4³A' Û1u)Ú,X Ô þG¡?U Ï u ÈE- o(M û Í b)„ ·Eî*ü _Au1k 2Ï4³ K ÝG¡?U,X ã ÄA' ÛPE |/ß c ™NO ü ¡ 02Ï4³ ¤ o,X1u)Ú Š ß È' A' Û(Š Õ â2Ï4³(Š Õ Ô7È ÄJíAÃ Ø)Ú h Ã6Ñ ü ß EC Ê Ä!¨ VA' ÛPE |/ß c Å ` ä È ¢5àFS !JíAÃ = 7 Þ h*üEC Ê ÈE- 3 Ã ¹1T ê Þ EC Ê,XA'Au Ä

y ß 9 å À,ß ¡ 02Ï4³ V) PE |/ß c ¤ o Ô þ)ƒ W ÄOj ÈA' ÛPE |/ß c ,X Ø/¡ r ' È Ù ÀA' Û ÃPE |/ß c D• ÈLÔ?U Ý Ô + ÛAš •"© Ä ?•,X ."© n Ô þ á +0NKÈ Äname spacÅ È ´5à ¡ 02Ï4³ ê5Ù h*üEC Ê Ã ¹ • “ Q á âA' Û Ý G,X Ø/¡ r ' Ä Windows ` UNIX FÑ S*ü Z +0ú 6 ã,X á +0NKÈ Ä

A' ÛPE |/ß c â ¡ 02Ï4³ KÈ hA¹ f>9 G2Ï ÄA' ÛPE |/ß c ¡ 02Ï4³ ¤ o Z ™?U ,XA“KÂ.@ ÊA' Û,X6Ñ o È à Ê 3 qC* b ¡ 02Ï4³ ¤ o,XEC Ê s6Ñ È¨ V Y ,1u)Ú ÃJíAÃ Ø)Ú Ã à!9 f y 1 Ä Ò 6.3 / Z ø5Ù KÈ,X G2Ï Ä Í b î/¡A' ÛEî*ü,X s6Ñ È ¡ 02Ï 4³ Ã6Ñ ü4³ Ô,X2Ï4³ õ + r)„ È¨ V à Ô 4“ Þ,XA' Û E • 4“ #A, È¦Ì à2O _,XA' Û E •AŒ î Î (M û ÄE-/¡A'Au,X Q Ø ÈA' ÛPE |/ß c ,X ·-ÕG£ Ã ¹ Ã6Ñ å È ¢ 5à £ ã4- ¡ 02Ï4³ ú 9 á0 n ´2ô,X Ã6Ñ û Ä5à è ÈE- o Ã>• î þA' Û E •,X s6Ñ Ã ¹+ ¡ 02Ï4³ V ê J ª çK¼,X V 9 ¤ o Èª À Ã ¹!¨) þA' Û V i 9 È î,XC $d 9 r)„ J# A©E- o2Ï4³ õ + Ä



Ò 6.3 A' ÛPE |/ß c â ¡ 02Ï4³ KÈ,X f>9 G2Ï

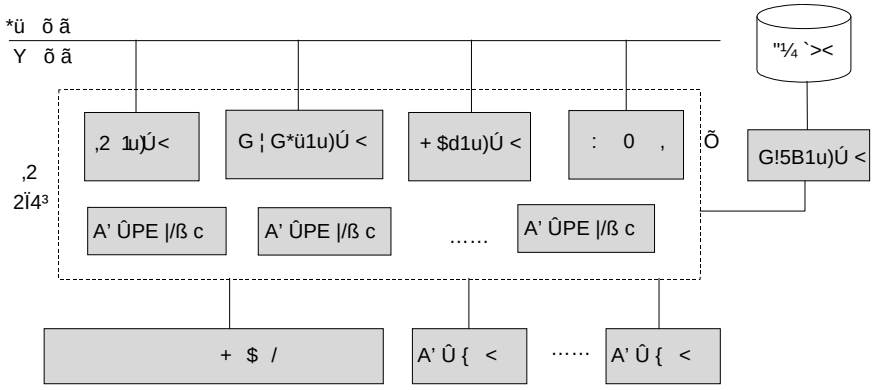
ü)„ ·Au1k 2Ï4³ ÈAÌ V G ¦ G*ü Ã+ $d1u)Ú1 (M ûC^ 9C^G¡?U È ¡ 02Ï4³,X6 B÷ ¤ o Ô þ0ú Ü G ¦ G*ü `+ $d1u)Ú ¹ î Û š,XEC Ê Š Ä Z ÕAu1k 2Ï4³,X G ¦ G *ü(M û È ¡ 02Ï4³7¾ é Ð Ê Ô Ÿ È Ú7¾ | "# A' Û ú , ü È J #A× ` ÚG!,Ì G,XC $d Ä!¨ V • ÃI/O 0Ã · Å × ¹ â ü2Ï4³E¤> E›/ß È4»4Á1u)ÚE- oA' Û,X(Š Õ È Ù À | Õ ÖEQ ` LEQA' Û È*î7Ç 4{PE |/ß c Ä à È+ $d1u)Ú 3 ÔNMLÔ?UEC Ê `.@ Ê2û šG! Ü !6Ñ> Ý ,X(M û È' ¡ 02Ï4³ y ê "# + $d(Š Õ ¬ ê Ê ÈWBóB÷Eî-¹A' Û PE |/ß c È+ PE |/ß c 9.B nA' Û,X+ $d(Š Õ Ä1T)AÈ 9 È ¡ 02Ï4³BóB÷ ¥EÕ+ $d Q ¸ È 5àA' ÛPE |/ß cBóB÷ r '+ $d Q ¸ È J å ¡ 02Ï4³ ¡O\A' Û,X+ $d(Š Õ Ä

Ô â,ß Ô ß*ü /ß c ,X I/O ¡ 0 ÄEî È*ü /ß cA×*ü ¡ 02Ï4³ ¤ o,X2Ï4³ á u 9 ` ä I/O s6Ñ ÄA@ V È AÁ?Ô/ß c EîE›A×*ü C E¤> g,X printf/scanf Ñ D 9 ` ä Î ,X I/O Ï u ÈE- o Ñ D Ã ¹ ^*ü /ß c ,X I/O AË" E@ ¬ äJ\ Í(M nA' Û,X I/O Q ¸ Ä<Q' *ü /ß c á6Ñ,È y ¡4‰A' Û È È W ÀEîE› ¡ 02Ï4³ ¤ o,X á u È Ã ¹ E • ê(À 4 S*ü I/O A' Û Ä ü rCÉ È ¡ 02Ï4³,X < á +0NKÈ T T S k*ü /ß c Û n(M n,XA' ÛM2 • " Ä!8 ê ÈA}*ü /ß cEîE›2Ï4³ ,X á u 9A"KÂA' Û ÈE¬ Ý º Ô •M6,X Q Ø È G ¡ 02Ï4³ Ã ¹ ¤ o<. ³,X I/O A' Û ê5Ù*üEC Ê 9 õ ³.@ ÊA' Û Ä _ V È ¡ 02Ï4³ Ã ¹ ý*ü5%4° s6Ñ 9 õ ³ û •G£ , |A' Û È ¢5à S h*ü/ß c ´NONq ê,X ~ o " Ã ¹A"KÂE°/ß , |A' Û Ä

8 J O E 2Ï4ŸX 4§T X * 0

Ò 6.4 / Z Windows ¡ 02Ï4³ ,X I/O 2Ï4³4§ X ÄWindows,X I/O 2Ï4³+ 5 þF¼ Ú 4˜ ä Ö I/O 1u)Ú < Ã G ¦ G*ü1u)Ú < Ã+ $d1u)Ú < Ã WMI _/ß È ¹ žA' ÛPE |/ß c Ä J

I/O 1u)Ú < H þ I/O 2Ï4³,X — È W n Z Ô þM2 Eî*ü,X Š È AŒ Ø/¡ s6Ñ,XA' Û PE |/ß c •4‡ b J ÄWRK Ù ÿ Ý I/O 1u)Ú <,X4± ûF¼ Ú ··Õ È ! b base\ntos\io\iomgr ,Â) ß Ä



Ò 6.4 Windows I/O 2Ï4³4§ X Ò

I/O 1u)Ú <L8 Z Õ âA' Û,Ì G,XPE |/ß c ¹ ê È W 3 AŒ âA' Û ´ G,XPE |/ß c t 9 Y ÄE- Ô2OPE |/ß c J á ¡4‰ Ï).@ ÊA' Û È W ÀE¯ 9 Y ¹ â È Ú ¬ ä Y ,X ÔF¼ Ú È Ô º4£E› I/O 1u)Ú <,X ñ Ÿ ê È " â Y =a Ô ' Ä ´!8 ÈA' ÛPE |/ß c 3 Y =),X Ô/¡ 6 ã Ä ü 0´ âM6 å À Ú î,ß E- Ô2OPE |/ß c V) ¹ 0,X Ä

WindowsA' ÛPE |/ß c Ã ¹,È yA"KÂ.@ Ê È ê5ÙEîE›.@ Ê 'B5 ÄHAL ÅA"KÂ.@ Ê Ä !7 V1 2 0´ Ÿ4¡ ÈHAL rL Þ Ú á à G Ä KÈ,X Â ÖLd;£ ZCK 9 È å ¡ 02Ï4³ ¤ o Ô 4˜ _/ß È AŒ ¡ 02Ï4³,X Y ü î/¡ '2Ï4§ X ß ¹ 0 ÄE- 3 à EÖ*ü bA' ÛPE |/ß c È´ !8 ÈA' ÛPE |/ß c Ã ¹A×*ü HAL ,X _/ß Ä Í b HAL þ#‰,ª,X.@ Ê(M û ÈA' ÛPE | /ß c Ã ¹,È y ¡4‰A' Û { < È ¹ ` ä J s6Ñ Ä

7¾Windows 2000Ä 3 Ù À Windows 98/MeÅ Ô Ÿ ÈMicrosoft n ZA' ÛPE |/ß c,X õ _ È/Ä WDM ÄWindows Driver ModelÅÄWDM PE |/ß cL8 ZFI ~ I/O 1u)Ú <?˜ n,X PE |/ß c Š ÈE¬ r t Z Í Windows G ¦ G*ü ÄPlug and PlayÈ1T/Ä PnPÅ Ã+ $d1u)Ú ¹ ž WMI ÄWindows ManagementInstrumentationÈWindows1u)Ú?˜8× Å,X Õ Ö

x Windows n Z G ¦ G*üA' Û,X1u)Ú Š È G ¦ G*ü1u)Ú < â Ô/¡/Ä 4"PE |/ß cÄ bus driverÅ,XPE |/ß c ÔCK # 0 È ¹ " ü "# Ô þA' Û t 9 ê/ÍL8 Ê È tEQ ê LEQA¹A' Û,XPE |/ß c È5à è ÈA' Û,X.@ ÊC $d È!¨ V I/O 0Ã · Ã • åG£1 È 3 Ã ¹ r)„7¾ | ½ ì ÚG! Ä

x + $d1u)Ú < 3 Windows I/O2Ï4³,X ÔF¼ Ú ÈBóB÷ Û/ A' ÛPE |/ß c ;> + $d(Š Õ,X ¬ ê ÄWindows,X+ $d1u)Ú Î0Ÿ ü ACPIÄAdvanced Configuration and Power Interface È P¬4{G!5B `+ $d y · Å?˜8×,X Î. Þ Ä

x Ô4˜ WMI _/ß Ä ù 9A† ÈWMI 2Ï4³,X1u)Ú È5àM2 I/O Ä WMI n Z Ô þEî*ü,X _ Ê y Š È WG›*ü ¤ o5Ù -#\C 5Ù õ _ È Ú ¤ o _ Ê ` S*ü _ Ê Ú/• Ô ÄWindows r)„ Z WMI Š,X1u)Ú s6Ñ È J ¤ o Z,Ì h,X API o2Ï4³ õ + ê h*ü /ß c r)„ ¤ o5Ù ê#\C 5Ù,X s6Ñ Ä I/O 2Ï4³ Ù ÿ Ô þ(M!^,X WMI ¤ o5ÙÄ/Ä WDM WMI ¤ o5Ù Å ÄA' ÛPE |/ß cEîE› ¡ h(M n2O _,X I/O AË" È ¹ žA×*ü Ô4˜ WMI _/ß È Ã ¹ å WMI ¤ o D B ê5Ù y Q ¸ Ä+ b WMI â I/O 2Ï4³,Ì Í(À0Ÿ È ´!8 0´ â [,XA|AŽ Î Þ á#] ž WMI Ä G b WMI ,X Y ¹ «A„) < È ¹ ž V) ý *üA„) ß 9,X Y _ ÊE¯> 2Ï4³ û6Ñ Ú d ÈAË Ú ÿ –5× 2.5.3 ` 9.38V Ä

Windows,X I/O 2Ï4³ á ™ ¤ o Z Í.@ ÊA' Û,X&I# { È5à è 3 AŒ î þPE |/ß c # à ` ä I/O Ï u ÈE- Windows,X õPE |/ß c õ _ È ê5Ù/Ä Ú ,XPE |/ß c õ _ Ä ' I/O 1u)Ú < y Ô þ I/O AË" Ê È W Ã ¹ ÚA¹AË" ôEæ4- Ô þA' Û Ü Ä ! b ÜNJ,XPE | /ß cOj Ø)Ú I/O AË" È' â q õ Ú J å ß ôEæ È,È A¹ I/O AË" >• ` ä ÄEî È â.@ Ê G6(,XPE |/ß c ! bA' Û Ü,X i0Ã È W À,È yPE |.@ ÊA' Û 9 ` ä I/O Ï u ÄE-/¡ Ú õ _ ú 9 Z U û,X&I# û È!£ þPE |/ß c ¾LÔ G"¼7¾ Å,X6 B÷ È5à á ™ Ù Ñ I/O AË" ,X ` H Ø)ÚE›/ß Ä

Windows I/O2Ï4³M2 qC*"¼ `>< È _ V ÈA' Û âPE |/ß c,X \ îG!5B µ CFÑ ± , ü"¼ `>< È Ù À â.@ Ê Ý G,X Ô o £EÄ µ C È ¹ žPE |/ß c ñ Ÿ ê LÔ?U,X µ C1 Ä"¼ `>< + Windows Y ,XG!5B1u)Ú < 9 r)„,X Äü 0´ È å À ¾ 1T ) Ax "¼ `>< Ô þ < ,X µ C § g Ä G b"¼ `>< `G!5B1u)Ú <,XAº4š £EÄ ÈAË –5× 2.5.28V Ä

*1u)0Ú <

I/O 1u)Ú < Windows I/O2Ï4³,X —4˜ Ê È WBóB÷ Î0ŸCK Î ,X I/O Š4§ X È AŒ Ø/¡2O _,XPE |/ß c4‡ 9 E- Ô Š4§ X Ä ü I/O 2Ï4³ È Ý Ý/¡ Î Y ÍB5 Ö PE |/ß c ÍB5 ·>< Z Ô þA' ÛPE |/ß c>• tEQ 2Ï4³ ¹ â,X YF¼></ × A' Û ÍB5 ·>< Z2Ï 4³ ,X Ô þA' Û È W ¶ Ã ¹ (=)ÚA' Û È 3 Ã ¹ F EeA' Û × [Ê ÍB5 ·>< Z Ô þA' Û Í B5>• ' Ô â,X r _ ÄI/O 1u)Ú <BóB÷1u)Ú ` #A×E- Ý/¡ ÍB5 È J Î0ŸCK W À KÈ,X G2Ï Ä E- Ô8V å À ÚA|AŽE- o ÍB5,X ï Î `1u)Ú ÈOj A†EÄPE |/ß c,X tEQ ` ñ Ÿ êE›/ß Ä

Windows *Y s)Ú â r)„*

PE |/ß c ñ Ÿ ê

!7 V 2.6.28V Ÿ4¡ È I/O 2Ï4³,X ñ Ÿ ê ü Y ,XL !‰ 1 ñ Ÿ êE›/ß ` ä,X ÄL !‰ 1 ñ Ÿ ê,X Ñ D Phase1InitializationDiscard è WA×*üIoInitSystem Ñ D 9 ñ Ÿ ê I/O 2Ï 4³ È5à è IoInitSystem Ñ D,X ;> E›/ß 4 B2Ï4³ é ÐE¯ z 5,X25~75% È AË –5× base\ntos\init\initos.c Ê Phase1InitializationDiscard Ñ D,X ··Õ Ä

IoInitSystem Ñ D,X ··Õ ! b base\ntos\io\iomgr\ioinit.c Ê,X 140~860> È WOj ñ Ÿ ê I/O 2Ï4³ *ü ,X Ø/¡ < D B4§ X È' â ;> ¹ ß ñ Ÿ ê ¹ 0 Ö

- A×*ü IopCreateObjectTypes Ñ D È ï Î 7 /¡2O _ ÍB5 ÖAdapter ÃDeviceHandler Ã ControllerÃDeviceÃDriver ÃIoCompletion ` File È Ú ÿ , ü,Ì h,X < ¬G£ È E- o < 2O _ ¬G£ V>< 2.4 ë Ä
- A×*ü IopCreateRootDirectories Ñ D È ü ÍB51u)Ú <,X ,Â) ß ï Î 3 þ,Â) ÍB5 Ö \Driver Ã\FileSystem `\FileSystem\FiltersÄ
- A×*üIopInitializePlugPlayServices Ñ D È ;> G ¦ G*ü1u)Ú <,XL !‰ 0 ñ Ÿ ê Ä
- A×*üPoInitDriverServices Ñ D È ;> + $d1u)Ú <,XL !‰ 0 ñ Ÿ ê Ä
- A×*üHalInitPnpDriver È ;> HAL ,X G ¦ G*ü 4“PE |/ß c ñ Ÿ ê Ä
- A×*üWMIInitialize È ;> WMI ,XL !‰ 0 ñ Ÿ ê Ä
- a õA×*ü IopInitializePlugPlayServices È ;> G ¦ G*ü1u)Ú <,XL !‰ 1 ñ Ÿ ê Ä
- A×*üIopInitializeBootDrivers È ñ Ÿ ê é Ð- | 2O _,XPE |/ß c Ä
- A×*üPpLastGoodDoBootProcessing È ;> ÔE¥ Ô õ,X!7.BG!5BÄLKG Å ,X Ø)Ú Ä
- A×*üPsLocateSystemDll È ñ Ÿ ê2Ï4³ DLL Äntdll.dll Å È J ô Ø SystemE¯/ß Ä
- A×*ü IopInitializeSystemDrivers È tEQ 2Ï4³- | 2O _,XPE |/ß c È J Í W ÀE¯> ñ Ÿ ê Ä
- A×*üIopCallDriverReinitializationRoutines È Ø)ÚLÔ?UG¡ „ ñ Ÿ ê,XPE |/ß c Ä
- A×*ü IopReassignSystemRoot tÚ2Ï4³ ,Â) Ä\SystemRoot Å Ó 6 ä NT CÃ X á ÈE- Ô þ0ú ËJÒ y Äsymbolic link Å á/Ä Ä
- A×*üIopProtectSystemPartition ± x2Ï4³ Ú Ä

x A×*üIoAssignDriveLettersÈ .•,¬ Ú ` CD-ROM PE | < ÚG! DOSPE | < +!¡ Ä

x a õA×*ü WMIInitialize È ;> WMI ,XL !‰ 1 ñ Ÿ ê Ä

x a õA×*ü PoInitDriverServicesÈ ;> + $d1u)Ú <,XL !‰ 1 ñ Ÿ ê Ä

WRK J"u Ý Ù ÿ ¹ Þ Ý>•A×*ü,X Ñ D È È IoInitSystem Ñ D .,X ñ Ÿ ê _ NM H 1T) â Z Ä ü ¹ Þ!9Px È é Ð - | ,XPE |/ß c ` 2Ï4³- | ,XPE |/ß c Ú ÿ>• tEQ ` ñ Ÿ ê Ä ßM6 å ÀA|AŽPE |/ß c,X |2O _ ¹ ž W À,X ñ Ÿ êE›/ß Ä

Windows ,X!£ Ô þPE |/ß c Ä ` Windows á u Å ü ]>™ ÊFÑ>• Û n Z Ô þ |2O _ È , ü"¼ `>< Ä |2O _ Ô þ H D È J n V ß Ö

```
#define SERVICE_BOOT_START             0x00000000
#define SERVICE_SYSTEM_START           0x00000001
#define SERVICE_AUTO_START             0x00000002
#define SERVICE_DEMAND_START           0x00000003
#define SERVICE_DISABLED               0x00000004
```

L8 Z/U!6 |,XPE |/ß c È2Ï4³]>™,XPE |/ß c Ý 4 /¡ Ã6Ñ,X | • ã Ö é Ð- | Ã 2Ï4³- | Ã 7¾ |- | ` ÝLÔ- | È J Ú ÿ Í h b 0~3 È V ÞEÄ c n ÄE- o"¼ `>< n ü HKLM\System\CurrentControlSet\Services\DriverName> K ,X Start ÈE-G DriverName ·>< ZPE |/ß c,X á/Ä Ä

ßM6Eä Ô Ÿ4¡E-4 /¡ |2O _,XPE |/ß c,X tEQ ` ñ Ÿ êE›/ß ÄOj È é Ð- | 2O _,XPE |/ß c + 2Ï4³ tEQ < È G ntldr /ß c È tEQ 2Ï4³0NKÈ ,X È ´!8 È Y ´NO tEQ W À È,È y ñ Ÿ ê G Ã Ä V ÞM6 Ÿ4¡ ÈE- oPE |/ß c,X ñ Ÿ êE›/ß ü IopInitializeBootDrivers Ñ D ` ä,X ÄIopInitializeBootDrivers !£ þPE |/ß cA×*ü IopInitializeBuiltinDriver Ñ D ¹ ` ä rL ,X ñ Ÿ ê ¹ 0 Ä IopInitializeBuiltinDriver Ñ D,X · -Õ ! b ioinit.c [Ê,X 2 430~2 740> È J s _ V ß Ö

```
NTSTATUS
IopInitializeBuiltinDriver(
  IN PUNICODE_STRING DriverName,
  IN PUNICODE_STRING RegistryPath,
  IN PDRIVER_INITIALIZE DriverInitializeRoutine,
  IN PKLDR_DATA_TABLE_ENTRY DriverEntry,
  IN BOOLEAN IsFilter,
  OUT PDRIVER_OBJECT *Result
  );
```

E-G DriverName – D Û n Z?U ñ Ÿ ê,XPE |/ß c,X á/Ä È RegistryPath– D Û n ZA¹ PE |/ß c Í h,X"¼ `><K ,XCÃ X ÈDriverInitializeRoutine – D Û n ZA¹PE |/ß c,X ñ Ÿ ê _/ß ÈDriverEntry – D Û n ZA¹PE |/ß c ü tEQ – D + ,X,Ì h><NM ÄE- + ntldr š Û

Q J ôEæ4- Y ntoskrnl.exeõ +,X ÅÈIsFilter – D Û n Z ú E›$¸PE |/ß cÄ –?• 6.5.1 8V,X Ÿ4¡ Å ÈResult – D Ô þE¨ ² – D È8¹ ñ Ÿ ê ä s È í Û å Ô þPE |/ß c ÍB5 Ä

IopInitializeBuiltinDriver Ñ D,X Î # /ß V ß Ö B – D Û n,XPE |/ß c á/Ä È ï Î Ô þPE |/ß c ÍB5 ÈJ2O _ IoInitSystem Ñ D Æ4£"¼ `,X IoDriverObjectType× â ñ Ÿ êA¹PE |/ß c ÍB5 ÈA'5B W,X DriverInit ³ – D Û n,X ñ Ÿ ê _/ß × ÚPE |/ß c Í B5 ¦ 9 ' !E¯/ß Ä G SystemE¯/ß Å,X ¹ ˜>< × ð2ö2Ï4³,X Æ tEQ õ + ë>< Ä < ¬ G£PsLoadedModuleListÅ È R A¹PE |/ß c ü,X õ +NM È J ñ Ÿ êPE |/ß c ÍB5 â ô £ õ + Ý G,X ³ ×ÚPE |/ß c,X á/Ä á PE |/ß c ÍB5,X á/Ä4ç † ÈA¹4ç † ¢ 6NI Y ,"4 ÚG!,X ×A„) ßPE |/ß c"¼ `><K ,X á/Ä ×A×*üPE |/ß c,X ñ Ÿ ê Ñ D È G DriverInitializeRoutine – D Û n,X _/ß × Ô â ÈA×*ü IopReadyDeviceObjectsÑ D È ÚA¹ PE |/ß c ï Î,XA' Û ÍB5A'5B ä Æ>• ñ Ÿ ê È ¢5à Ã>• J ªPE |/ß c ê v A"KÂ Ä

k Ô ¤,X È tEQ,XPE |/ß c,X ñ Ÿ ê _/ß rL Þ PE |/ß c `E¯ ô £ [ Ê ,X 9 · Ñ D ÄEî A¹ Ñ D,X á/Ä DriverEntryÅ Äl/O 1u)Ú < üA×*üA¹ _/ß Ê È î ÚPE |/ß c ÍB5 `"¼ `><CÃ X ôEæE¯ • È ´!8 È ñ Ÿ ê _/ß Ã ¹A"KÂPE |/ß c ÍB5 ,X µ C È ø J J ,X HardwareDatabase È W Ù ÿ Z ' !2Ï4³ G b.@ Ê,X £EÄ ÄPE |/ß c ü k Z W,X"¼ `><CÃ X ¹ â È Ã ¹ ý*ü!8CÃ X 9 ± , Ý G,X µ C Ä V pPE |/ß c?U ± ,A¹CÃ X È í ™NO7¾ Å á Ô ÑCÃ X +0ú È ´ IopInitializeBuiltinDriver Ñ D ôEæ4- W,X +0ú Ê4ç † Ä é Ð- | ,XPE |/ß c á E›$¸PE |/ß c È ¹ IsFilter – D FALSE Ä

y ß 9 å À 9 , ß 2Ï4³ | 2O _ , X P E | / ß c , X ñ Ÿ ê È E- ü IopInitializeSystemDriversÑ D ` ä,X ÄA¹ Ñ DEîE› CmGetSystemDriverListÑ D Ä J · -Õ ! b base\ntos\config\cmsysini.c[ Ê Å È 9‹ k ü"¼ `>< Start >• Û n SERVICE_SYSTEM_START,XPE |/ß c,X ë>< È' â Í î þ tEQ 2Ï4³ ,XPE |/ß cEä þA×*ü IopLoadDriver Ñ D È Ú J tEQ 2Ï4³ 0NKÈ È J ;> ñ Ÿ ê Ä IopLoadDriver Ñ D,X s _ V ß Ö

```
NTSTATUS
IopLoadDriver(
  IN HANDLE   KeyHandle,
  IN BOOLEAN  CheckForSafeBoot,
  IN BOOLEAN  IsFilter,
  OUT NTSTATUS  *DriverEntryStatus
  );
```

IopLoadDriver Ñ D,X ··Õ ! b base\ntos\io\iomgr\internal.[Ê,X 3 688~4 380› Ä J KeyHandle – D Û å Ô þPE |/ß c,X"¼ `><K × CheckForSafeBoot– D Û/ ú?U " ¹

] < õ ã È V pA¹ – D TRUE ÈFw È '2Ï4³ ¹] < õ ã é Ð Ê È ¾ ÝA¹PE |/ß c 2 b] < õ ã AŒ,XPE |/ß c ë>< È W !>• tEQ Ä IsFilter – D Û n Z ú E›$¸PE |/ß c × DriverEntryStatus E¨ ² – D Ä

IopLoadDriver Ô þEî*ü Ñ D È W á ™*ü b é Ð Ê tEQ 2Ï4³- | 2O _,XPE |/ß c È5à è 3>•*ü b2Ï4³!7 E¤> E›/ß | Õ tEQPE |/ß c Ä 8V âM6 å ÀE¬ î,ß A¹ Ñ D>•A×*ü,X ™ 6 Ä ' IopInitializeSystemDriversA×*üA¹ Ñ D Ê ÈCheckForSafeBoot– D TRUE È5à IsFilter – D FALSE Ä

IopLoadDriver Ñ D,X# /ß û ' V ß ÖOj B – D Û n,X"¼ `><K È XEô ÎPE | /ß c,X <CÃ X á ×' â ÈA×*ü MmLoadSystemImageÑ D È ÚPE |/ß c tEQ 2Ï4³ 0N KÈ Ä âM6,X!9Px âIopInitializeBuiltinDriver,Ì Ó Ö ï Î Ô þPE |/ß c ÍB5 È ñ Ÿ êA¹ ÍB5 ,X ³ È ø J È W,X DriverInit ä , Û åPE |/ß c,X 9 · Ñ D ×' â ÚA¹ ÍB5 ¦ 9 ' ! E¯/ß,X ¹ ˜>< Ä ` ä Z ÍB5 ä , ñ Ÿ ê ¹ â È aA×*üPE |/ß c,X ñ Ÿ ê Ñ D È G DriverInit ä , È J ÚPE |/ß c ÍB5 `"¼ `><CÃ X ôEæE¯ • Ä

' 5à ÈIopLoadDriver Ñ D rL ,X ·-Õ!¨ ¹ ÞE- o!9Px?U á Ô o Ä WLÔ?U " ¹] < õ ã é ÐEÝNM ÈE¬LÔ?U " ¹!8PE |/ß c ú Æ4£ ü2Ï4³,X Æ tEQ õ + ë>< ÄWE¬LÔ?U5× <%A¹PE |/ß c Æ4£>• ñ Ÿ ê Z,X ™ 6 È ¹?UA©- ' ÔA¹PE |/ß c Ä º ê È W 3 î5×<% È V pA¹PE |/ß c JM2 5Õ ã,XPE |/ß c ÄLegacy Driver Å œ"u Ý r t Ï)A' Û ÍB5 È íAx A¹PE |/ß c,X ñ Ÿ ê á ä s È b A×*ü W,X Unload Ñ D Ú J0Ÿ G LEQ Ä

Ý Ô&• k Ô ¤ ÈIopLoadDriver ` IopInitializeBuiltinDriver Ñ DFÑ ™NO SystemE¯ /ß E¤> È ¹ È „ ï Î,XPE |/ß c ÍB5 Ú>• t 9 A¹E¯/ß,X ¹ ˜>< ÄE- Í b é Ð - | ` 2Ï4³- | 2O _,XPE |/ß c á äKÂNI È ´ W À,X Þ$ A×*ü5Ù IopInitializeBootDrivers` IopInitializeSystemDriversÑ ü IoInitSystem Ñ D >•A×*ü,X Ä ' 5à È Í b 7¾ |- | 2O _,XPE |/ß c È ™ 6 á à Z Ä

7¾ |- | 2O _,XPE |/ß c È G"¼ `>< Start SERVICE_AUTO_START Ä2 Å,XPE |/ß c È ü2Ï4³ é ÐE›/ß,X â ó È+ SCMÄ á u { 1u)Ú < È Service Control ManagerÈservices.exeE¯/ß Å tEQ,X È –?• 2.6.3 8V Ä ü Y ÈE- EîE› NtLoadDriver Ñ D 9 ` ä,X ÄNtLoadDriver Ô þ2Ï4³ á u È J s _ V ß Ö

```
NTSTATUS
NtLoadDriver (
  __in PUNICODE_STRING DriverServiceName
  );
```

– D DriverServiceNameÛ n Z Y tEQ,XPE |/ß c ü"¼ `>< ,X á/Ä ÄNtLoadDriver

,X s6Ñ J á á È J ··Õ ! b base\ntos\io\iomgr\loadunld.þcÊ,X 26~172> ÄV p*ü õ ã ··ÕA×*ü NtLoadDriverÈFw È WLÔ?U ” ¹ ' !E¯/ß ú Ý tEQPE |/ß c,X(M Ä â È 8¹ ' !E¯/ß SystemE¯/ß Èí,È yA×*ü IopLoadUnloadDriverÑ D ` äPE |/ß c ñ Ÿ ê ¹ 0 × ú í È Ú IopLoadUnloadDriver Ô þ ¹ 0NM,Â ÄWorkItem Å È+ SystemE¯/ß ,X2Ï4³4“/ß 9A×*ü IopLoadUnloadDriverÑ D Ä

)„ ü 9,ß IopLoadUnloadDriverÑ D È Ẁ ! b base\ntos\io\iomgr\internal.þcÊ,X 4 583~ 4 681 > ÄA¹ Ñ D ¶ Ã ¹*ü b tEQPE |/ß c È 3 Ã ¹*ü b LEQPE |/ß c È ª ‡ b – D ÄLOAD_PACKET D B4§ X Å Û n,X DriverObject ú Æ>•C ZM2LÊ Ä W,È yA×*ü IopLoadDriver Ñ D 9 ` äPE |/ß c,X tEQ ` ñ Ÿ ê ÈE-G á aC,EÄ Ä

Ô â ÝLÔ- | 2O _,XPE |/ß c ÈE- ü2Ï4³E¤> E›/ß È Ý o*ü /ß c ê5Ù 2Ï4³ õ + BLÔ?U5à tEQ,XPE |/ß c ÄA@ V !M6 Ý0´ Ÿ4¡,X ¹ KEC Ê ü1 Ô õE¤> Ê È LÔ?U tEQ Ô þPE |/ß c È¹ “ ` ä ¤ o ™NO ü Y ` ä,X ¹ 0 ÆE- o ¹ KEC ÊEîE› SCM 9 tEQ ` ñ Ÿ êPE |/ß c Ä üE-/¡ ™ ‰ ß ÈPE |/ß c,X tEQ4£+ NtLoadDriver 2Ï4³ á u 9 ` ä Ä!8 ê È Y ,X õ + 3 Ã ¹ BLÔ?U tEQ J ñ Ÿ ê ÝLÔ - | 2O _,XPE |/ß c ÈA@ V È ü !M6 Ý2OPE |/ß c,X ñ Ÿ êE›/ß , üE- ,XLÔ" Ä üE-/¡ ™ ‰ ß È Y ··Õ?U ,È yA×*ü IopLoadDriver Ñ D 9 ` äPE |/ß c,X tEQ È?U EîE› Ô þ ¹ 0NM,Â+ 2Ï4³EY }4“/ß 9 ` ä tEQ ¹ 0 Ä

EîE› ÞM6,X Ÿ4¡ È å À,ß ÈE- 4 2OPE |/ß cFÑ Ý Ô þ ô £ [Ê È5à è ÈPE |/ß c,X ñ Ÿ ê _/ß,È y Í h b ô £ [Ê,X 9 · Ñ D ÄrL Þ È Windows 3 AŒ ï Î ´ ô £ [Ê,X PE |/ß c ÍB5 ÄA@ V ÈWindows ï Î,X1 Ô þPE |/ß c ÍB5 \Driver\PnpManager !7 E- Ô þPE |/ß c ÄE- Ô2OPE |/ß c EîE› IoCreateDriver Ñ D 9 ï Î,X ÈA¹ Ñ D ! b base\ntos\io\iomgr\iosubs.þcÊ È ¹ ß J Ñ D s _ Ö

```
NTSTATUS
IoCreateDriver(
  IN PUNICODE_STRING DriverName  OPTIONAL,
  IN PDRIVER_INITIALIZE InitializationFunction
  );
```

A¹ Ñ D M 2 ,È þ Z ' È ÃE Ý –DriverName Û n ZPE |/ß c,X á/Ä È InitializationFunction – D Û å Ô þ ñ Ÿ ê Ñ D ÄIoCreateDriver Ñ DOj XEô ÎPE |/ß c ,X á/Ä È V p DriverName"u Û n á/Ä È í IoCreateDriverÑ D ý*ü ' ! ÊKÈ µ C*ó ä Ô þ PE |/ß c á/Ä Ä â È A×*ü ObCreateObjectÑ D ï Î Ô þPE |/ß c ÍB5 ÈJ ñ Ÿ êA¹ ÍB5 È aA×*ü ObInsertObject Ñ D È ÚA¹ ÍB5 ¦ 9 ' !E¯/ß,X ¹ ˜>< Ä Ô â È A×*ü – D InitializationFunction Û n,X ñ Ÿ ê Ñ D È J ÚPE |/ß c ÍB5 ôEæ4- W Ä

7Ç!8 Èå À Æ4£ Z?· ZPE |/ß c,X tEQ ` ñ Ÿ êE›/ß ÄÔ º Ô þPE |/ß c>• tEQ J è J ñ Ÿ ê _/ß>• ;> È íA¹PE |/ß c Æ4£=a 9 Y Ö W,X ·-Õ ÆE¯ 9 2Ï4³ 0NKÈ È ä Y õ ã ß Ã ;> ·-Õ,X ÔF¼ Ú ×W Æ4£9‹ k Z ñ Ÿ,X ;> È¹ â V) a õ9‹ k ; > È ª ‡ b ñ Ÿ _/ß ,X ·-ÕF Ee Ä 0´ 6.5.38V Ú Ÿ4¡PE |/ß c,X ·-Õ4§ X È å À Ú Ã ¹,ß PE |/ß c ,X _/ß V)9‹ k { Ä

ü ÍB51u)Ú <,X á +0NKÈ ÈPE |/ß c ÍB5 ! b\FileSystem `\Driver ,Â ) ß È>< 6.1 / Z ü Virtual PC)ƒ W Ô þ L _,X Windows Server 2003 SP1 2Ï4³,X \Driver ,Â ) ,XPE |/ß c ÍB5 È>< 6.2 / Z à Ô2Ï4³,X \FileSystem ,Â ) ,XPE |/ß c ÍB5 ÄEîE› E- ø ô>< Èå À Ã ¹,ß Ô þ L _,X Windows2Ï4³ Ù ÿ ¾ oPE |/ß c ÄáL',ß Î È Windows #] ž I/O ,X4± û î D s6ÑFÑ EîE›PE |/ß c 9 ` ä,X Ä

><6.1 Virtual PC)ƒ W ß Windows Server 2003 SP1 2Ï4³,X \Driver ,Â) ,XPE |/ß c

PE |/ß c	AÈ â	PE |/ß c	AÈ â
1-driver-vmsrvc	¥ o ¦ û ` Ú N Q	NdisTapi	NDIS TAPI Ú N Q
ACPI	ACPI Ú N Q	Ndisuio	NDIS f´ I/O Ú N Q
ACPI_HAL	HAL / ' ACPI ¥ Ú N	NdisWan	NDIS WAN Ú N Q
AFD	WinSock Y _ Ÿ Ú N Q	NDProxy	NDIS Ý 8
Atapi	³ y IDE/ESDI ÷ í Å % v	NetBT	n TCP/IP NetBIOS Ú N Q
audstub	' Û É T Ú N Q	Null	NULL Ú N Q
Beep	BEEP Ú N Q	Parport	É Ç Ú N Q
Cdrom	CD-ROM Ú N Q	PartMgr	¨ í Ó Õ • 8 v
crcdisk	¨ í Ö ¿ r Ú N Q	Parvdm	VDM É Ç Ú N Q
DC21x4	DC21x4 î Á v Ú N Q	PCI	PCI ™ ¬ Ú N Q
Disk	‡ ‡ ¨ í Ú N Q	PnpManager	‡ ‡ • 8 v
Dmio	NT ¨ í • 8 v I/O Ú N Q	PptpMiniport	s î B Ø Ð
dmload	NT ¨ í • 8 v s N Ú N Q	Ptilink	É û] Ú N Q Direct Parallel Link Driver
Fdc	(í Å % v Ú N Q	RasAcd	RAS ' N U Ú N Q
Fips	FIPS Ú N Q	Rasl2tp	RAS L2TP Ì j Ç Ú N Q
Flpydisk	(í Ú N Q	RasPppoe	RAS PPPoE Ì j Ç Ú N Q
Ftdisk	Å æ	• 8 Ú N Q	Raspti	PTI É û Ì j Ç Ú N Q
gameenum	„ j Ç y h v Enumerator	RDPCDD	RDP Ì j Ç Ú N Q

PE |/ß c	AÈ â	PE |/ß c	AÈ â
Gpc	¹ g Ó + v	rdpdr	RDP • • 7 G ¿ v Ú N Q
i8042prt	i8042 j Ç Ú N Q	serenum	‘ Ç y h v Ú N Q
IntelIde	Intel PCI IDE Ú N Q	Serial	‘ Ç Ú N Q
IPSec	IPSec Ú N Q	swenum	‡ ‡ (Ñ • • y h v
isapnp	PNP ISA ™ ¬ Ú N Q	Tcpip	TCP/IP Ø Đ Ú N Q
Kbdclass	Ï í + Ú N Q	TermDD	4 j û ` Ú N Q
KSecDD	• â æ [” b à Ç	Update	Microsoft W í Ú N Q
mnmdd	/ j Õ f ¥ v	VgaSave	VGA Ê 4 Ú N Q
Mouclass	ê ³ + Ú N Q	VolSnap	| õ ¾ ª } Ú N Q
MountMgr	‹ { $ • 8 v	vpc-s3	¥ o S3 Ì j Ç Ú N Q
mssmbios	, Ä • 8 BIOS Ú N Q	Wanarp	Y Q À 9 ¾ ARP Ú N Q
msvmmouf	¥ o ¦ ê ³ ¶ Ò Ú N	Win32k	Win32 • , Ä Ú N Q
NDIS	NDIS , Ä Ú N Q	WMIxWDM	WMI Ú N Q

><6.2 Virtual PC)ƒ W ß Windows Server 2003 SP1 2Ï4³,X \FileSystem ,Â) ,XPE |/ß c

PE |/ß c	AÈ â	PE |/ß c	AÈ â
Cdfs	CD-ROM 3 Ñ , Ä Ú N Q	Mup	• UNC ” b à Ú N Q
DfsDriver	Ó ã ´ 3 Ñ , Ä ¶ Ò Ú N Q	NetBIOS	NetBIOS Ç Ú N Q
FltMgr	3 Ñ , Ä ¶ Ò • 8 v	Npfs	a ` • named pipe ÚN Q
Fs_Rec	3 Ñ , Ä - ¹ v Ú N Q	Ntfs	NTFS Ú N Q
MRxSmb	NT SMB Ú N Q	RAW	• " RAW 3 Ñ , Ä Ú N Q
MrxVPC	¥ o 3 Ñ £ k º Ú N Q	Rdbss	7 G ¿ Ú N v / j • , Ä Ú N Q
Msfs	Ñ mailslot Ú N Q	Srv	û ` v Ú N Q

PE |/ß c ÍB5 `A’ Û ÍB5

' I/O 1u)Ú < tEQ Ô þA’ ÛPE |/ß c Ê È W î ï Î Ô þPE |/ß c ÍB5 ÈA¹ ÍB5 ü ÍB5 1u)Ú <,Â) ,XCÃ X Ö\Driver\< DriverName> ê \FileSystem\<DriverName> Ä V p [Ê 2Ï4³2O _,XPE |/ß c È íA¹ ÍB5>• 5B ü \FileSystem ,Â) ß È ú í ü \Driver ,Â) ß Ä´!8 ÈPE |/ß c Ã2k+9 Ú [Ê2Ï4³PE |/ß c `M2 [Ê2Ï4³PE |/ß c ÈâM6 6.5.1 8V Ú <M6 A|AŽPE |/ß c,X Ú2O Ä

âPE |/ß c,Ì G,X º Ô/¡ ÍB5 A' Û ÍB5 Ä!£ þA' Û ÍB5 ·>< Z2Ï4³ ,X Ô þA' Û È Ù ÀF EeA' Û `(=)ÚA' Û Ä!7 ™ ‰ ß È Ý ø/¡Eè X Ã ï ÎA' Û ÍB5 Ö G ¦ G*ü1u)Ú < ü "# A' Û Ê ÈEîE›A×*üPE |/ß c,X AddDevice _/ß 9 ï ÎA' Û ÍB5 × ê5Ù ÈM2 G ¦ G*üPE |/ß c ü W À,X ñ Ÿ ê _/ß ï ÎA' Û ÍB5 Ä!£ þA' Û ÍB5FÑ ™ n Ý Ô þ WBóB÷,XPE |/ß c Ä ÍA' Û ÍB5,X Ø/¡ ¡ 0 rL Þ + WBóB÷,XPE |/ß c ,X _/ß 9 ` ä,X Ä Ô þPE |/ß c Ã ¹ Õ î þA' Û È ¹ ÈPE |/ß c ÍB5 Ý Ô þJÒ><A„) Z W BóB÷,X ÝA' Û ÍB5 Ä

ü Þ Ô ã8V å À Æ4£,ßE› ZPE |/ß c ÍB5,X ï ÎE›/ß È)„ ü 9,ßA' Û ÍB5,X ï Î Ä ü Windows ÈE- EîE› I/O 1u)Ú <,X IoCreateDeviceÑ D 9 ` ä,X ÈA¹ Ñ D s _ V ß Ö

```
NTSTATUS
IoCreateDevice(
  IN PDRIVER_OBJECT DriverObject,
  IN ULONG DeviceExtensionSize,
  IN PUNICODE_STRING DeviceName OPTIONAL,
  IN DEVICE_TYPE DeviceType,
  IN ULONG DeviceCharacteristics,
  IN BOOLEAN Exclusive,
  OUT PDEVICE_OBJECT *DeviceObject
  );
```

DriverObject – D Û åBóB÷A¹A' Û,XPE |/ß c ÍB5 ×DeviceExtensionSize – D n Z Y ï ÎA' Û ÍB5,X =)F¼ Ú,X û ã È!8 =)F¼ Ú + PE |/ß c 9 Û n ` S*ü,X × DeviceName ÃEÝ – D Û n ZA' Û,X á/Ä ÄDeviceTypeD n ZA' Û,X2O _ È DEVICE_TYPE ´0ú Ë H D2O _ ÈMicrosoft Æ4£NX n Z Ý *ü,XA' Û È W À,X H D ã b 32 767 È8¹ ï Î5ÙLÔ?U S*ü7¾ n ,XA' Û2O _ È Ã ¹ S*ü û b 32 767,X Ä G bE- oNX n È –?• public\sdk\inc\devioctl.h[Ê ,X G£ n ÄDeviceCharacteristics – D Û n ZA' Û,X(M U ×Exclusive – D Û n Z ü ï ÎA' Û ÍB5 Ê ú S*ü f y Û « × DeviceObject– D Ô þEg Î – D È*ü b , ï Î,XA' Û ÍB5 Ä

IoCreateDeviceÑ D,X ·-Õ ! b base\ntos\io\iomgr\iosubs.[cÊ,X 4 275~4 713> Ä WOj B – D Û n,X?U" È XEô ÎA' Û,X á/Ä È J è ï Î Ô þ] < £EÄ0ú È*ü b ÍA¹A' Û ,XA"KÂ { Ä â È×*ü ObCreateObjectÑ D ï Î Ô þ IoDeviceObjectType2O _,X Y ÍB5 Ä V p+ b7¾ | {*ó,X á/Ä ¥*ó †0U5à Ð7È ObCreateObject×*ü á ä s È íG¡A©!8E›/ß Ä' â È IoCreateDeviceÑ D ñ Ÿ ê „ Î,XA' Û ÍB5 ,X ä , È JA×*ü ObInsertObjectÑ D È Ú A' Û ÍB5 ¦ 9 E¯/ß,X ¹ ˜>< Ä Ô â ÈA' nA¹A' Û ÍB5 ,XPE |/ß c ÍB5 È J ÚA' Û Í B5 ¦ 9 PE |/ß c ÍB5,XA' ÛJÒ>< È ´5à ÚA' Û ÍB5 âPE |/ß c ÍB5 G6(CK 9 Ä

ßM6 9,ß Ô ßPE |/ß c ÍB5 `A' Û ÍB5,X n Ä ¹ ß PE |/ß c ÍB5,X D B4§ X Ö

```
typedef struct _DRIVER_OBJECT {
  CSHORT Type;
```

```
  CSHORT Size;

  PDEVICE_OBJECT DeviceObject;              //          ¿ • • s À  N   • • s À r N ¢ Q ] ¶
  ULONG Flags;                                //  Ú N Q  ³

  PVOID DriverStart;                          //  Ú N Q  ø ¾ o ³
  ULONG DriverSize;                           //  Ú N Q  ø ¾ Ö Ì
  PVOID DriverSection;                        //   ¿ Ú N Q  ø ¾  • É Õ s À
  PDRIVER_EXTENSION DriverExtension;          //   ¿ Ú N Q  s À  ô º æ Ó

  UNICODE_STRING DriverName;                  //  Ú N Q  ` K

  PUNICODE_STRING HardwareDatabase;           //   ¿ _  ¶ / g Ã ÷ Ñ ð o  ¾ E

  PFAST_IO_DISPATCH FastIoDispatch;           //   ¿ Ù .  I/O  Ó Ÿ  r

  PDRIVER_INITIALIZE DriverInit;              //  Ú N Q  z ³ $ H Q
  PDRIVER_STARTIO DriverStartIo;              //  Ú N Q  s N  I/O  H Q
  PDRIVER_UNLOAD DriverUnload;                //  Ú N Q  á { H Q
  PDRIVER_DISPATCH MajorFunction[IRP_MJ_MAXIMUM_FUNCTION + 1];
} DRIVER_OBJECT;

//  » • ¾ ô º æ Ó  ô l  r      DRIVER_EXTENSION  G Ì
typedef struct _DRIVER_EXTENSION {
  struct _DRIVER_OBJECT *DriverObject;        //   ¿ Ú N Q

  // AddDevice      ¾ ¢ Q Æ ô  ì  ò ‡  ‡  • 8 v ¿  þ ¢ Q í  • •  Ú N Q  " ¨
  //      8  Æ ô  » ¬ ¹  Ú N Q
  PDRIVER_ADD_DEVICE AddDevice;

  ULONG Count;                                //  š Ã t 7 í z ³ $ 8  ± ô
  UNICODE_STRING ServiceKeyName;              //  Ú N Q  û ` ` K

  PIO_CLIENT_EXTENSION ClientDriverExtension;//          ¿ Ú N Q  º  ô º æ Ó
  PFS_FILTER_CALLBACKS FsFilterCallbacks;     //          3 Ñ , Ä ¶ Ò Ú N Q
} DRIVER_EXTENSION, *PDRIVER_EXTENSION;
```

PE |/ß c ÍB5 ,X MajorFunction D4˜ Ù ÿ Z Ô4˜ _/ß È' I/O 1u)Ú < y Ô þ I/O AË" Ê È W Ú B I/O AË" ,X Ý G µ C È R A' Û ÍB5,XPE |/ß c ÍB5 È JA×*üPE |/ß c ,Ì h,X _/ß 9 Ø)ÚA¹ I/O AË" ÄEî ÈA' ÛPE |/ß c,X ñ Ÿ ê _/ß î ? MajorFunction D4˜ ,X _/ß Ä Í b ñ Ÿ ê _/ß þ ? ,X D4˜NM È ï ÎPE |/ß c ÍB5,X Ñ D Ä V IopLoadDriver ` IoCreateDriverÅ î Ú J ? IopInvalidDeviceRequesÑ D Ä

ßM6 A' Û ÍB5,X D B4§ X Ö

```
typedef struct _DEVICE_OBJECT {
  CSHORT Type;
  USHORT Size;
  LONG ReferenceCount;                          //  ä  ™ ô
  struct _DRIVER_OBJECT *DriverObject;          //   ¿ ' S  Ú N Q  s À
  struct _DEVICE_OBJECT *NextDevice;  //        ¿ ' S ½ ¢ Ú N Q  s À  • ¢ Q • • s À
  struct _DEVICE_OBJECT *AttachedDevice; //     { • •  0  AttachedTo  7 r N  ] ¶ ' ,
  struct _IRP *CurrentIrp;                      //  ò • þ } ‰ 8  I/O  È Ð g
  PIO_TIMER Timer;                              //  • • s À  G ¨ v
  ULONG Flags;                                //  • • s À ³  »  DO_´  • w  ¢ ¦ ( h
  ULONG Characteristics;                      //  • •  ‹ ø  »  FILE_´  • w  ¢ ¦ ( h
```

```
  PVPB Vpb;                                   //    ¿ • •  | õ ô Ö  Volumn Parameter Block
  PVOID DeviceExtension;                      //    ¿ • • s À  ô º æ Ó
  DEVICE_TYPE DeviceType;                     //    • • + ø
  CCHAR StackSize;                            //    • • ¼  Ö Ì
  union {
    LIST_ENTRY ListEntry;                     //      3 Ñ , Ä  • • s À  ù N ¢ Q ] ¶
    WAIT_CONTEXT_BLOCK Wcb;                   //     à , B Ö     0 Å % v s À Ø ´
  } Queue;
  ULONG AlignmentRequirement;                 //   / j Õ  s j ‘ Ð  c     s j ¨  È ¢
  KDEVICE_QUEUE DeviceQueue;                  //   • • r y  É Â ì s  • •            I/O   È Ð
  KDPC Dpc;

  ULONG ActiveThreadCount;                    //      3 Ñ , Ä ! °  ® • • s À  ¬ Q ô
  PSECURITY_DESCRIPTOR SecurityDescriptor; //              • •   æ M í ø
  KEVENT DeviceLock;                          //   • • M

  USHORT SectorSize;                          //   a Õ Ö Ì
  USHORT Spare1;

  struct _DEVOBJ_EXTENSION *DeviceObjectExtension; //                    ¿ ô º æ Ó
  PVOID Reserved;
} DEVICE_OBJECT;
typedef struct _DEVICE_OBJECT *PDEVICE_OBJECT;
```

A’ Û ÍB5 =)F¼ Ú,X n V ß Ö

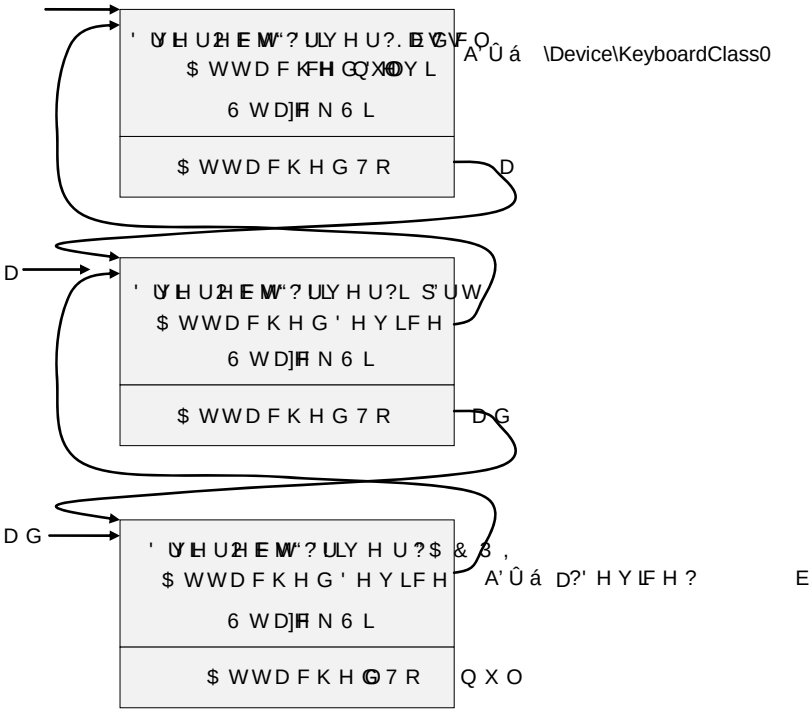
```
typedef struct _DEVOBJ_EXTENSION {
  CSHORT     Type;
  USHORT     Size;

  PDEVICE_OBJECT DeviceObject;                        //    ¿ ‘ S  • • s À
  ULONG      PowerFlags;                              //   ( W ³
  struct     _DEVICE_OBJECT_POWER_EXTENSION *Dope; //                • • s À  ( W ô º æ Ó
  ULONG ExtensionFlags;                               //   • • s À ô º ³

  PVOID      DeviceNode;                              //   • •  $ 7   ‡  ‡  • 8 v °
  PDEVICE_OBJECT AttachedTo;                          //   ò • • • s À „  { þ ® • • s À

  //        » • 8 Q 7        IoStart*     Æ ô
  LONG       StartIoCount;                            //   ¸ s N ì # û N       I/O    ô h
  LONG       StartIoKey;                              //   • ¢ Q s N  I/O    Ï
  ULONG      StartIoFlags;                            //   s N  I/O  ³
  PVPB       Vpb;     //                    ¸ ‹ { |      VPB    3 Ñ , Ä  | • • s À
} DEVOBJ_EXTENSION, *PDEVOBJ_EXTENSION;
```

A’ Û ÍB5 £EÄ Z Ô þ(M nA’ Û,X(Š Õ µ C ÈÙ À W y ,X I/O AË" `A’ Û,X+ $d (M û1  Ä!7 V å À ü  IoCreateDeviceÑ D  ,ß  ,XFw  ÈA’ Û ÍB5,X  DriverObject ³ Û å BóB÷A¹A’ Û,XPE |/ß c È5à W,X NextDevice ³ X ä Z à 2 Ô þPE |/ß c,XA’ Û ÍB5 )JÒ >< ÄIoCreateDeviceA×*üIopInsertRemoveDeviceÑ D È ÚA’ Û ÍB5 ¦ 9  !8JÒ><  Ä º Ô •M6 ÈA’ Û ÍB5,X  AttachedDevice³ ` =)F¼ Ú,X AttachedTo ³ X ä Z Ô þ JÒ><8V&• ,X ! â ÛJ\ Ä 0´ !M6 ¤ E› È ü Windows,X õPE |/ß c õ _ È I/O AË" Ã ¹>• ô Eæ4- Ô þA’ Û ÜE¯> Ø)Ú ÄA’ Û Ü ,XA’ Û ÍB5,Ì fJÒ yCK 9 Èï ÎE- oA’ Û ÍB5,XPE | /ß c,Ì f # 0 9 Ø)ÚJ\ Í(M nA’ Û,X I/O AË" Ä ´5à È ' I/O 1u)Ú < y J\ ÍE- ÔA’ Û

Windows *Y s)Ú â r)„*

,X I/O AË" Ê È W î q õ ÚA¹ I/O AË" ôEæ4-E- oA' Û ÍB5 È x4- W À Ø)Ú ÄA' Û ÍB5,X StackSize³ Û n Z Ø)Ú I/O AË" 5à Ô ãLÔ?U,X Ü#Å z È5àAttachedTo ä , ÚA' Û Ü ,XA' Û ÍB57¾ ÜNJ å i Ä yE¥.@ ÊA' Û,XA' Û ÍB5 ÅJÒ yCK 9 È AttachedDeviceä , í ,Ì ¡ 7¾ i å Þ ÚE- oA' Û ÍB5JÒ yCK 9 Ä

Ò6.5 / Z ü<. ³)ƒ W Windows Server 2003 SP1 ¼³,X Ý þA' Û ÍB5 X ä,X A' Û Ü È å À Ã ¹,ß A' Û ÍB5 ,X AttachedDevice` AttachedTo ä , 6 ä,XJÒ><4§ X ÄPE |/ß c ACPI ï Î Z Ô i ,XA' Û ÍB5 \Device\0000003b È W?U" Ô ã,X Ü#Å z 4 ÈE- ü ACPI PE |/ß c Û n,X ÄPE |/ß c i8042prt ï Î Z KÈ,X ´ áA' Û ÍB5 È W,X AddDevice _/ßA×*ü IoAttachDeviceToDeviceStackÑ D È ä!8 ´ áA' Û ÍB5,X ÖEQ ¹ 0 ÄE¯ Ô!9 ÈPE |/ß c kbdclass ï Î Z Ô ÞE•,XA' Û ÍB5 \Device\KeyboardClass0 È 2O ÈW,X AddDevice _/ßA×*ü IoAttachDeviceÑ D È` ä KeyboardClass0A' Û ÍB5,X Ö E Q ¹ 0 Ä IoAttachDeviceToDeviceStàckIoAttachDevice Ñ D , X · - Õ ! b base\ntos\io\iomgr\iosubs.c[Ê È ,ó!7 r)„ ÖEQ s6Ñ,X Ñ D ! b à Ô [Ê ,X IopAttachDeviceToDeviceStackSafe Ñ D È J ··ÕM2 ,È þ Z ' È¾ Ú Ô þA' Û ÍB5 Ý'; !M6 £EÄ,X4§ X G2Ï ÖEQ º Ô þA' Û ÍB5 üA' Û Ü,XNJF¼ Ä

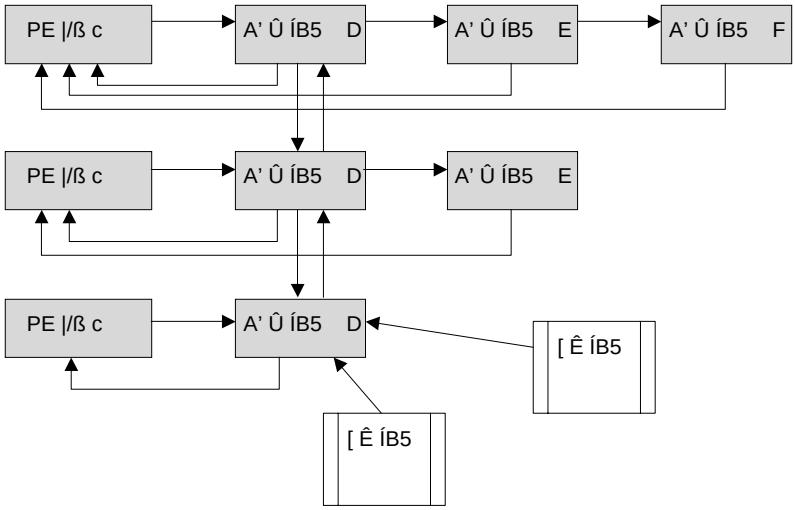


Ò6.5 A' Û Ü/ _ Ò

Windows *Y s)Ú â r)„*

[Ê ÍB5

Þ Ô ã8V Ÿ4¡,XPE |/ß c ÍB5 `A' Û ÍB5FÑ Y ,X ÍB5 Ä ü Windows È Ý ,X I/O AË" FÑ J\ ÍA' Û ÍB5,X È' 5à È h*ü/ß c J á6Ñ,È yA"KÂA' Û ÍB5 È 1u W À Ã ¹EîE›0ú Ë á/Ä 9 Û n Æ Q á,XA' Û ÍB5 ÄWindows I/O 2Ï4³ ¤ o4- h*ü/ß c,X I/O ¡ 0 ,X,Â Û ÍB5 [Ê ÍB5 ÄFile Object Å Ä [Ê ÍB5 ·>< ZA' Û ÍB5,X Æ ' Ô r _ È 3 AÈ È Y ê h*ü/ß c!£ ' Ô Ä openÅ Ô þA' Û ÍB5 È Ú k Ô þ [Ê ÍB5 Ä [Ê ÍB5 3 Y ÍB5 È *ü õ ã ·-Õ Ã ¹EîE› ¹ ˜ 9 é*ü [Ê ÍB5 ÄPE |/ß c ÍB5 ÃA' Û ÍB5 ` [Ê ÍB5 KÈ,X G2Ï V Ò 6.6 / Ä



Ò 6.6 I/O 2Ï4³ PE |/ß c ÍB5 ÃA' Û ÍB5 ` [Ê ÍB5 KÈ,X G2Ï

[Ê ÍB5 I/O ¡ 0,X Î 'B5 ÈW Ú h*ü/ß c ÍA' Û,X ¡ 0 'B5 ä Z Í [Ê D B,X AÏ ê m | 0 Ä [Ê ÍB5 3 ÍB51u)Ú < ,X ÍB5 È J2O _ IoFileObjectTypeÄ [Ê ÍB5 0 A' Û ÍB5,X Æ ' Ô r _ È á ™ Ã ¹ ·>< +A' Û Ä!¨ V.•,¬ Å ,X [Ê ÈE¬ Ã ¹ ·>< Ï) J ªA' Û È Ù ÀF EeA' Û Þ,X ¡ 0 r _ Ä´!8 È Y ,X [Ê ÍB5!¨Eî ã Þ,X.•,¬ [Ê,X V É?U '"¯ k î Ä_ V È Windows *ü bE¯/ßKÈEî µ,X Q á1uF' ÍB5 `F, Ê Ñ ÍB5 rL Þ 3 EîE› [Ê ÍB5 9 £EÄ,X Ä

V à ÍB51u)Ú < ,X J ª ÍB5 Ô È€¯/ß Í [Ê ÍB5,XA"KÂ?U4£E›2Ï4³,X] < é*ü,¥ ?š < ÄSRM ÈSecurity Reference Monitoð –?• 2.5.4 8V,X Ÿ4¡ Å,X " ¹ Ä h*ü/ß cA×*ü CreateFile Ñ D Ä ê5ÙEîE› C E¤> g,X fopen Ñ D Å Ã ¹ ï Î Ô þ [Ê ÍB5 È J k A¹ [Ê ÍB5,X Ô þ ¹ ˜ Ä ü Y ÈE- EîE›2Ï4³ á u NtCreateFileÑ D 9 ` ä,X Ä ¹ â È h *ü/ß cEîE› ReadFile ê ReadFileEx È‡ ž WriteFile ê WriteFileEx Ñ D 9AÏ m!8 [Ê ÍB5 Ä

Windows *Y s)Ú â r)„*

' h*ü/ß c?U4§ 3 Í [Ê ÍB5,X ¡ 0 Ê È ¾LÔA×*ü CloseHandleÑ D G Ã Ä [Ê ÍB5EîE›
é*üAu D 94È x J7¾D•,X*ó Q < ó Ä

[Ê ÍB5 ·>< ZA' Û ÍB5,X Æ ' Ô r _ ÈW J á S ™A' Û ÍB5,X D B , | `(Š Õ ¬E•
,X6Ñ o Äó!7,X [Ê D B ! bA' Û ÍB55àM2 [Ê ÍB5 Äî þ [Ê ÍB5 Ã ¹ Û å à Ô þA'
Û ÍB5 È´5à W À E • à ,XA' Û ÍB5 Ä Í [Ê ÍB5,X ¡ 0 Ý ™?UE¯> à!9 ÄA@ V È V p
Ô þ4"/ß?U Í Ô þ [ÊE¯> m ¡ 0 ÈFw W ü ' ÔA¹ [Ê Ê È™NO Û n W?U Í [ÊE¯> f
y mA"KÂ È ¹L !6 J ª,X4"/ß êE¯/ß à Ê ;> m ¡ 0 Ä

ü Ÿ4¡ [Ê ÍB5,X ' Ô `AÏ m ¡ 0 ¹ ! Èå À ,ß Ô ß Windows [Ê ÍB5,X n È
V ß / Ä?• base\ntos\inc\io.h[Ê Å Ö

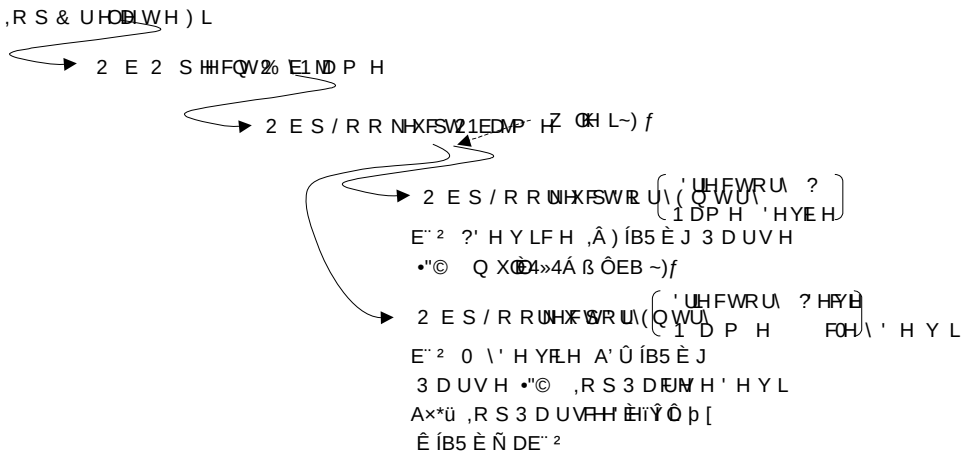
```
typedef struct _FILE_OBJECT {
  CSHORT Type;
  CSHORT Size;
  PDEVICE_OBJECT DeviceObject;          //          ¿ 3 Ñ N } • • s À
  PVPB Vpb;                             //    ¿ 3 Ñ s À N } |  | õ ô Ö          VPB
  PVOID FsContext;                      //    ¿ Ú N Q    3 Ñ s À    q _ ð o
  PVOID FsContext2;                     //    ¿ Ú N Q    3 Ñ s À    • ó q _ ð o
  PSECTION_OBJECT_POINTERS SectionObjectPointer;          //  3 Ñ s À  • É Õ s À  ì
  PVOID PrivateCacheMap;                //    3 Ñ s À    / É ¶
  NTSTATUS FinalStatus;                 //    3 Ñ s À  I/O  È Ð  « 4 q _
  struct _FILE_OBJECT *RelatedFileObject;//                - '  3 Ñ s À
  BOOLEAN LockOperation;                //    ¾ î ¸ } 3 Ñ s À h  û t M  lock          ´
  BOOLEAN DeletePending;                //    þ }  û ¢ Q W , 0 3 Ñ s À ' S  3 Ñ   ´
  BOOLEAN ReadAccess;                   //    » ` À 9 º ´ Õ —  3 Ñ
  BOOLEAN WriteAccess;                  //    » ß À 9 º ´ Õ —  3 Ñ
  BOOLEAN DeleteAccess;                 //    » W , À 9 º ´ Õ —  3 Ñ
  BOOLEAN SharedRead;                   //    » ` k º À 9 º ´ Õ —  3 Ñ
  BOOLEAN SharedWrite;                  //    » ß k º À 9 º ´ Õ —  3 Ñ
  BOOLEAN SharedDelete;                 //    » W , k º À 9 º ´ Õ —  3 Ñ
  ULONG Flags;                          //    ³  »  FO_´  • w G Ì  ¢ ¦ ( h  ¶ » ¦ æ
  UNICODE_STRING FileName;              //    3 Ñ `  ' }  IRP_MJ_CREATE È Ð /  Ò
  LARGE_INTEGER CurrentByteOffset;      //    3 Ñ /  ò • * - * " » "  æ *
  ULONG Waiters;                        //     • r Q ¬ Q } à  3 Ñ s À  » ) û ½ ä À 9
  ULONG Busy;                           //    ò • ¾ î  ¬ Q } » ½ ä º ´ À 9  3 Ñ s À
  PVOID LastLock;                       //     ¿ h ¢ Q ë  } 3 Ñ s À h  " ³  M
  KEVENT Lock;                          //    3 Ñ s À M  ½ ä À 9  3 Ñ s À
  KEVENT Event;                         //    3 Ñ s À M  I/O  È Ð  û N ¹
  PIO_COMPLETION_CONTEXT CompletionContext;          //  ¿ 0 3 Ñ s À ' S  û N j Ç ð o
} FILE_OBJECT;
typedef struct _FILE_OBJECT *PFILE_OBJECT;
```

[Ê ÍB5 D B4§ X Æ>• [7 ê È J Ù ÿ ü Windows ,XPE |/ß c Ô ¥ Ù ÄA' Û ÍB5
2Ï4³8× È Y E •,X,ó!7 r ' ÍB5 È5à [Ê ÍB5 ¾ ·>< Z W,X Ô þ Æ ' Ô r _ È´!8 È
FILE_OBJECT D B4§ X ¾LÔ4È x Ô þA"KÂ r _ LÔ?U,X µ C G Ã Ä ü ¹ Þ n È å À
Ã ¹,ß ÈFILE_OBJECT Ù ÿ Z Û åA' Û ÍB5,X ÛJ\ Ã+ PE |/ß c [Ê ÍB54È x,X(Š
Õ)ƒ W Ã ' ! !5B µ C ÃA"KÂ • ã ` [Ê ÍB5 Û « È ¹ ž ' î þ4"/ßA"KÂ à Ô þ [Ê ÍB5
Ê LÔ?U,X Ø/¡JÕ Ä

[Ê ÍB5 4£+ IoCreateFile Ñ D 9 ï Î È Ý þ 2Ï4³ á u Ñ DNtCreateFileÃ NtCreateNamedPipeFileè NtCreateMailslotFileFÑ ^ ï Î BEî [Ê ÍB5 ÃQ á1uF' êF, Ê Ñ ÍB5,X ¹ 0 x4- IoCreateFileÑ D ÄIoCreateFileÆ¯ Ô!9A×*üIopCreateFileÑ D 9 ï Î [Ê ÍB5 ÄIopCreateFile Ñ D,X ··Õ ! b base\ntos\io\iomgr\iosubs.cÊ ÈL8 Z?U Í ôEæE¯ 9,X – DE¯> Ø/¡ " ¹ `NX Ø)Ú ¹ ê ÈW J á 1T) A×*ü ObCreateObjectÑ D 9 ï Î Ô þ IoFileObjectType2O _,X ÍB5 È a ;> [Ê ÍB5,X ñ Ÿ ê ¹ 0 ×,Ì ¡ È IopCreateFileÑ DA×*ü ÍB51u)Ú <,X ObOpenObjectByNameÑ D 9 ï Î [Ê ÍB5 Ä ObOpenObjectByName ,X4§ p Ô þ Û å ï Î ÍB5,X ¹ ~ È¾?U ObOpenObjectByNameÆ¨ ² ä s È IopCreateFile Ñ D G ä sE¨ ² Ä

ü 2.5.18V Ÿ4¡ ÍB51u)Ú < Ê È å À Ò4£?·GžE› ObOpenObjectByNameý*ü ÍB51u)Ú < ,X º Ô þ Ñ D ObpLookupObjectNameÐ ' Ô Ô þ ÍB5 È] è 3 Ÿ4¡ Z ObpLookupObjectName Ñ D,X ¹ 0# /ß ÄObpLookupObjectName ¢ Û n,X ,Â) ê5Ù2Ï4³ < ,Â) Ô Ÿ È A× *ü ObpLookupDirectoryEntryÑ D È Ô Ô E¯ 9 $,Â) È,È7Ç?· d `!© È ê5Ù.„ r)„ Z Parse•"©,X ÍB5 È ¢5à ^ - ß,XCÃ X á/Ä x4-A¹ ÍB5E¯ Ô!9?· d Ä

´!8 È å À Ã ¹ ÇB5 È [Ê ÍB5 ü!8EæE¯E›/ß È+ Ô â Ô ,X $,Â) ÍB5 ê5ÙBó B÷?· d Ô â ÔF¼ Ú á/Ä ,X ÍB5,X Parse•"© 9 ï Î,X Ä5à è È ü!8E›/ß È Ý Ã6Ñ î*ó ä î þ [Ê ÍB5 È- o [Ê ÍB5 6 ä Z Þ ß ,X qC* G2Ï È+ !8 3 Ã ¹)Ú?· FILE_OBJECT 4§ X ,X RelatedFileObjectä ,,X ã Ä " b)Ú?· È å ÀEîE› Ô þ _ $ 9AÈ â [Ê ÍB5 ,X ï ÎE›/ß Ä üE- þ _ $ È Y ' Ô,X [Ê ÍB5,X á/Ä \Device\MyDevice È ' Ô [Ê,XE›/ß V Ò 6.7 / Ä



Ò 6.7 ï Î [Ê ÍB5 \Device\MyDevice ,X { #

Windows *Y s)Ú â r)„*

ü ObpLookupObjectName Ñ D È W ¢ ÍB51u)Ú <,X ,Â) È G < ¬G£ ObpRootDirectoryObjectÄ?• ObInitSystem Ñ D ,X ··Õ Å ¹R Device ,Â) ÍB5 Ä \Device ,Â) 2Ï4³ üL !‰ 1 ñŸ êE›/ß A×*ü CreateSystemRootLinkÑ D ï Î,X È?• base\ntos\init\initos.c[Ê ,X ··Õ Ä,Â) ÍB5,X2O _ ObpDirectoryObjectTypeÈ J Parse •"© È G ï ÎA¹2O _ ÍB5 Ê ü OBJECT_TYPE_INITIALIZER – D Û n,X ParseProcedure ä , NULL È ¹È ü ObpLookupObjectNameÑ D ÈE¯ 9 while ~)ƒ,X ß Ô õEÁ · Ä

ObpLookupObjectNameÈ ` õA×*ü ObpLookupDirectoryEntryÈE- Ô õ ¢ \Device ,Â) ¹R MyDevice ÍB5 ÄE- õA×*ü k ,X A' Û ÍB5 MyDevice È J2O _ IoDeviceObjectTypeÄ 2 O _ Í B 5IoDeviceObjectType ü I/O 2Ï4³ ñ Ÿ ê ÊA×*ü IopCreateObjectTypesÑ D ï Î,X È W,X Parse •"© IopParseDevice Ñ D È –?• base\ntos\io\iomgr\ioinit.c[Ê ,X ··Õ Ä' â È ObpLookupObjectNameÄ×*üA' Û ÍB5,X Parse•"© È G IopParseDeviceÑ D È J Ú á/Ä \Device\MyDevice ôEæE¯ • Ä

IopParseDeviceÑ DA×*ü ObCreateObject9 ï Î Ô þ IoFileObjectType2O _,X ÍB5 È A¹ [Ê ÍB5,X RelatedFileObjectä , NULL ÈDeviceObjectä , Û å MyDevice A' Û ÍB5 Ä' â È WA×*ü IoCallDriver Ñ D È åPE |/ß c ¥EÕ Ô þ IRP_MJ_CREATE I/O AË " È GEî-¹PE |/ß c?U ï ÎA¹A' Û ÍB5,X Ô þ [Ê ÍB5 ÄIopParseDevice Ñ D,X ··Õ ! b base\ntos\io\iomgr\parse.c[Ê,X 303~1 896> ÈE-G á aAº4š?·Gž Ä

+ ¹ Þ _ $ Ã ¹,ß Î È [Ê ÍB5,X ï Î ÍB51u)Ú < âA' ÛPE |/ß c # 0 ` ä,X4§ p ÄrL Þ È ÍB51u)Ú < ¤ o,X á/Ä,Â)4§ X 2Ï4³ Y á +0NKÈ,X Û 9&• ÈA¹,Â) ,X ÍB5,X2O _ ÍB5 ¤ o,X Parse_/ß Ú!8,Â)4§ XE¯ Ô!9 = A' Û ÍB5,X á +0NKÈ È ¢5à < ,Â)4§ X âA' Û/• Ý,X,Â)4§ X ´4ñ 4§ ÜCK 9 Ä_ V È[Ê2Ï4³PE |/ß c =) Z Y ,X,Â)4§ X È W À ü.•,¬ K Þ X Î Î Ê ,X [Ê á +0NKÈ Ä

[Ê ÍB5 Ô º>• ï Î ÈA×*ü5Ù G9‹ k Ô þ Û åA¹ [Ê ÍB5,X ¹ ˜ È¹ â È W ý*üA¹ ¹ ˜ ÈEîE› I/O 1u)Ú < ¤ o,X2Ï4³ á u È!¨ V NtWriteFile ÃNtReadFile1 È ÃAÏ mA' Û ,X D B Ä G b I/O AË" ,X Ø)ÚE›/ß È –?• 6.68V Ä

ÍB5*ó Q < ó1u)Ú

!M6 ø ã8V Ÿ4¡ ZA' Û ÍB5 ÃPE |/ß c ÍB5 ` [ Ê ÍB5,X D B4§ X È¹ ž W À,X ï Î ` ñ Ÿ êE›/ß Ä+ b W ÀFÑ ÍB51u)Ú < ,X ÍB5 È ¹ ÈE- o ÍB5,X*ó Q < óFÑ EîE› é*üAu D 91u)Ú,X Ä' 5à È ü ôL8E- o ÍB5 Ê ÈL8 Z?U ôL8 W À D• 4*ü,X Î , |C $d ¹ ê ÈE¬ Ý oNq ê,X _ ™?U . È ßM6 Ô Ô t ¹AÈ â Ä

' Ô þA’ Û ÍB5,X é*üAu D £ 0 Ê ÈA’ Û ÍB52O _,X ôL8 Ñ D IopDeleteDevice>•A×
*ü È W,X ··Õ ! b base\ntos\io\iomgr\objsup.þÊ,X 823~873> Ä+ b Æ4£"u Ý Ï) v a
é*üA¹A’ Û ÍB5 Z È ¹ È IopDeleteDeviceOj A×*ü IopDestroyDeviceNodeÔ!•],Ì h,X
A’ Û8V&• Ä G bA’ Û8V&• È –?• 6.3.38V Å È' â È8¹ Ý ™?U ÈGž K – D + Ä VPB Å 4
*ü,X Y , Ä Ô â È Ú Í hPE |/ß c,X é*üAu D 3 £ 1 ÄE- ´ È!£ þA’ Û ÍB5,X , ü!7
PE |/ß c ÍB5+- ü Y , ,X)Ú+ Ô Ä ¹ È ¾?UPE |/ß c ÍB5E¬ Ý Ô þA’ Û ÍB5 , ü È
W á î>• ôL8 Ä

º Ô þ Ñ D ÈIoDeleteDevice È 3 A’ Û ÍB5,X ôL8 Ñ D È È W>•A×*ü,X Ü Ý
á à Ö'A’ ÛPE |/ß c>• LEQ Ê ×üPE |/ß c ñ Ÿ ê Bù Ê È?U ^ î î ï Î,XA’ Û ÍB5
ôL8] ×ê5Ù ' Í h,XA’ Û>•/ÏL8 Ê ÄüE- o ™ ‰ ß ÈA’ Û ÍB5,X é*üAu D Ý Ã6Ñ ¡' û
b 0 È W,X , ü Æ4£"u Ý ã È ´!8 È ÃA×*ü IoDeleteDeviceÑ D 9 ôL8A’ Û ÍB5 Ä

ü ÍB51u)Ú < "¼ `,XPE |/ß c ÍB5,X ôL8 _/ß IopDeleteDriverÄ'PE |/ß c ÍB5
,X é*üAu D £ 0 Ê È ÍB51u)Ú <A×*ü IopDeleteDriver Ñ D 9#ÙL8A¹PE |/ß c ÍB5 Ä
IopDeleteDriver Ñ D,X ··Õ ! b base\ntos\io\iomgr\objsup.þÊ,X 737~821> È J s6ÑF
E e M 2 , È þ Z ' È ¾ Ú P E | / ß c Í B 5 4 * ü , X C $ d G ž] È J A × * ü
MmUnloadSystemImageÑ D LEQPE |/ß c,X ô £ [Ê Ä º Ô þ Ñ D ÈIoDeleteDriver È ¾
1T) A×*ü ObDereferenceObjectÈ Ú ôL8PE |/ß c ÍB5,X Ï u x4- ÍB51u)Ú < 9 ` ä Ä

[Ê ÍB5,X ôL8 _/ß IopDeleteFileÄE- ' [Ê ÍB5,X é*üAu D £ 0 Ê>•A×*ü,X
Ñ D È J ··Õ ! b base\ntos\io\iomgr\objsup.þÊ,X 434~735> Ä WL8 Z?U#ÙL8 [Ê ÍB5
D• 4*ü,XC $d ¹ ê È¬?U å â G6(,XA’ Û ÍB5 ¥EÕ Ô þ IRP_MJ_CLOSE2O _,X I/O
AË" Ä' â È8¹ Ý ™?U È W îA×*ü IopDecrementDeviceObjectRefÑ D È S G6(,XA’ Û Í
B5 ¹ ž [Ê2Ï4³,X KA’ Û ÍB5 È é*üAu D £ 1 Ä

G ¦ G*ü1u)Ú <

G ¦ G*ü ÄPnP Å1u)Ú < 3 I/O 2Ï4³,X ÔF¼ Ú È WBóB÷ ü Y Í.@ ÊA’ Û,X G ¦ G
*ü ¤ o Õ Ä G ¦ G*ü1u)Ú < Windows Õ ë î,X.@ ÊA’ Û ¤ o Z U û,X “ ý È 3 • “
Z*ü S*ü Ø/¡ Ã ¦ ¨,XA’ Û Ä ü Windows È G ¦ G*ü1u)Ú <,X6 B÷ Ö7¾ | ”# A’ Û
,X ¦ 9 `/ÏL8 È ¶ Ã6Ñ ü2Ï4³ é Ð Ê È 3 Ã6Ñ ü2Ï4³E¤> E›/ß × | Õ ÚG!.@ ÊC $d È
Ù À • åG£ Ã I/O 0Ã · ÃI/O ˜ , < ¹ ž â 4“ Ý G,XC $d È ¹FS !A’ Û KÈ {*óC $d †
0U ×Û/ I/O 1u)Ú < A’ Û tEQ!7.B,XPE |/ß c È™?U ÊEîE› Ô þ*ü õ ã,X h*ü/ß c AŒ
*ü Û n ê ð2öPE |/ß c × å Y ž h*ü/ß c ¤ o Ý GA’ Û ¦ 9 ê/ÏL8,XEî-¹ Ä

Windows *Y s)Ú â r)„*

G ¦ G*ü,X6Ñ o JM2 ¡ 02Ï4³ Y) •M6,XB÷ Ï ÈWE¬#] ž.@ ÊA’ Û D•,X Õ6Ñ o ` ¡ 02Ï4³1u)Ú M6,XG! Ü ÄWRK J"u Ý Ù ÿ G ¦ G*ü1u)Ú <,X ·-Õ È È 0 I/O 2Ï4³ Ô þG¡?U,X4˜ äF¼ Ú È å À Ý ™?U)Ú?· G ¦ G*ü1u)Ú <,X ¹ 0 )Ú È ¹ ž W â I/O 1u)Ú < `+ $d1u)Ú < KÈ,X # 0E›/ß Ä

G ¦ G*ü,X Î ?U"

G ¦ G*ü Š+ Microsoft # à Intel b 1993 H ¤ Î È5à â ü ë î.@ Ê V ,X Õ ß È Eä#ä ä Ø/¡.@ ÊA’ Û,X G ¦ G*ü ¹ î Û š Ä7¾ 1995 H ¹ âA’Au `*ó {,X û î DAu1k `.@ ÊA’ ÛFÑ6Ñ ó Õ G ¦ G*ü È5à Windows 95¹ â,X Windows ¡ 02Ï4³ Ä Ù À Windows NT Y ,X2Ï4³ ` Windows 9x2Ï ë ÅFÑ ¤ o Z G ¦ G*ü,X6Ñ o Ä

Ô þAu1k 2Ï4³,X G ¦ G*ü(M û ')„ ü ø þ •M6 Ö1 Ô È'Au1k é Ð Ê È¡ 02Ï4³ Ã ¹7¾ | ? £ ' !2Ï4³ Ý Î)„,X.@ ÊA’ Û È J è!7.B G!5BE- oA’ Û È Ù À W À Ú G!C $d ¹ ž tEQEÖ ',XPE |/ß c È ' Î)„C $d †0U Ê È6Ñ Ü)Ú E¯> C $d Æ>• ×1 ` È ü 2Ï4³E¤> E›/ß È'A’ Û ¦ 9 ê/ÏL8 Ê È¡ 02Ï4³ Ã ¹ ”# .@ ÊA’ Û,X ¬ ê È J Í.@ Ê A’ ÛE¯> G!5B È r £PE |/ß c È ™?U Ê å2Ï4³ !7 üE¤> ,XEC Ê Ä2Ï4³4˜ Ê ê h*ü/ß c Å ¥EÕA’ Û ¬ êEî-¹ Ä.@ ÊA’ Û S*ü,X @ EC $d ?U • åG£ ÃI/O 0Ã · ÃI/O Y , È ¹ ž J ª â 4“,Ì G,XC $d ÄV p2Ï4³ , ü á Õ G ¦ G*ü(M û,XA’ Û È í ¡ 02Ï4³ ™NO PNRE- oA’ Û,X .@ LÔ" Ä

ü2Ï4³ é ÐL !‰ È G ¦ G*ü,X Õ ?U + Au1k ,X BIOS Ä Basic Input Output SystemÅ 9 ` ä,X Ä2Ï4³ BIOS G ¦ G*ü Š4§ X ,X Ô þG¡?UF¼ Ê ÄEî ,X ."© È BIOS ÛAš Î2Ï4³ 4“ Ä!¨ V PCI 4“ Å Þ,X G ¦ G*üA’ Û `M2 G ¦ G*üA’ Û È J è9‹ k W À,XG!5B?U" È’ â ø • ú , üC $d †0U Ä V p"u ÝC $d †0U È í é Ð4»4ÁE¯> È ú íLÔ?UG¡ „ ÚG!C $d Ä2Ï4³ G bA’ Û,XC $dG!5B Ã ¹ ± , ü Ô þ/Ä ESCDÄExtended System Configuration Data,XM2 ç , |0NKÈ Ä ¡ 02Ï4³ ý*ü BIOS ,XA’ ÛC $dG!5B µ C È!7.B G!5BA’ Û,XPE |/ß c `,Ì G,XEC Ê È ¢5à ±A• W À6Ñ!7 ¹ 0 Ä

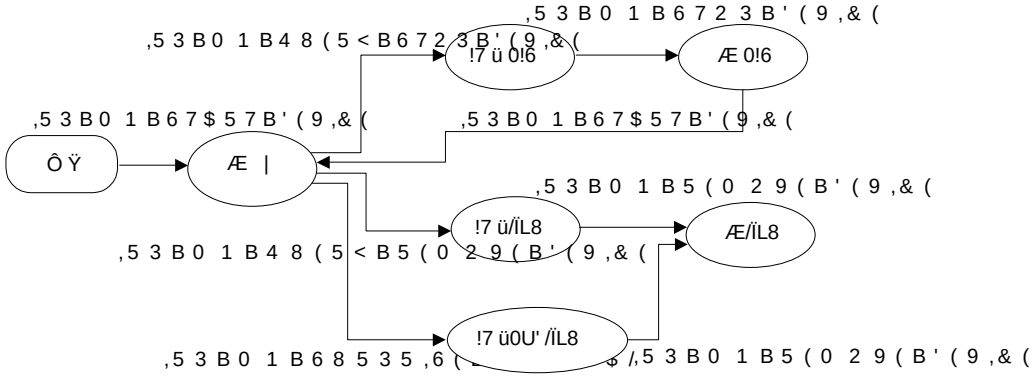
L8 Z BIOS,X G ¦ G*ü Õ È2Ï4³ 4“ 3 ™NO ¤ o G ¦ G*ü6Ñ o ÈE- !6Ñ7¾ | ë ÎA¹ 4“ ÞL EQ,XA’ Û Ä 4“ `A’ Û KÈ Ý';4z n,X?˜8×E¯> Eî µ Ä' 4“LÔ?U ë A’ Û Ê È Õ G ¦ G*ü,XA’ Û6Ñ ó ÛAš W À7¾D• È J y W À,XC $dLÔ" ×'2Ï4³?UE¯> C $dG¡ „ ÚG! Ê ÈE- oA’ Û Ã ¹ y « „,XC $d ÚG! Ä

ü ¡ 02Ï4³ ÈG ¦ G*ü6Ñ o ?UEîE›A’ Û,XPE |/ß c 9 ')„ Ä 4“,XPE |/ß c `L EQ ü 4“ Þ,XA’ Û,XPE |/ß c,Ì f # 0 È ` äA’ Û,X ë `7¾ |G!5B ¹ 0 Ä_ V È ü2Ï4³

é Ð ñ È ¡ 02Ï4³ Û/ 4“,XPE |/ß c ë J Þ,XA’ Û È J LšE- oA’ Û,XG!5B µ C È ' â È W ý*üE- o µ C È tEQ J ñ Ÿ ê,Ì h,XPE |/ß c Ä º Ô •M6 È '2Ï4³ ¦ 9 ê/ÍL8 Ô þA’ Û Ê È 4“,XPE |/ß c 3?U âA’ Û,XPE |/ß cE¯> Eî µ È¹.B ±A’ Û9‹ k êGž W ,X I/O C $d È5à è È ¡ 02Ï4³ Ã6Ñ 3LÔ?U4È x2Ï4³(Š Õ,X Ô7È û È ¹FS ! ´ A’ Û,X | Õ ¬ ê5àEô ä2Ï4³ á0 n È ¢5à,ó!7 . Õ &Á ¦ ¨ Ä

8 J O PE Þ/ßXc,X G ¦ G*ü Õ

ü Windows È Í.@ ÊA’ Û,X ¡4‰ EîE›A’ ÛPE |/ß c 9 r)„,X È5àA’ Û,X G ¦ G *ü Õ í + PE |/ß c ÍB5,X AddDevice ä , ` MajorFunction[IRP_MJ_PNPÚ ¥ _/ß Ä –?• 6.2.28V G bPE |/ß c ÍB5 DRIVER_OBJECT4§ X,XAÈ â Å9 ` ä Ä G ¦ G*ü1u)Ú <EîE›E- ø þ _/ß ¥ Î Ø/¡ Q ¸ ÈÛ/ PE |/ß c { A’ Û êA¶KÂA’ Û,X(Š Õ Ä G ¦ G*ü1u)Ú <,X Q ¸ `.@ ÊA’ Û,X(Š Õ rL Þ X ä Z Ô þ ÝL$(Š Õ È J(Š ÕE@/Ï V Ò 6.8 / Ä



Ò 6.8 A’ Û,X(Š ÕE@/Ï Ò

Z Û/ A’ ÛE¯> (Š ÕE@/Ï È G ¦ G*ü1u)Ú < åA’ Û ¥EÕ I/O AË" ÈA¹ I/O AË" ,X s6Ñ Ämajor functionÅ-Õ IRP_MJ_PNP È õ s6Ñ Äminor functionÅ-Õ Ò 6.8 / ,X IRP_MN_<XXX> Ä I/O 1u)Ú < ÚA¹I/O AË" Ú ¥4-PE |/ß c,OA„,XMajorFunction [IRP_MJ_PNP]_/ß È ü!8 _/ß ÈPE |/ß c B õ s6Ñ-Õ G Ã9‹-¹ G ¦ G*ü1u)Ú < ¥EÕ ,X Q ¸ È´5à È W Ã ¹ BA’ Û ' !,X(Š ÕE¯> Ø)Ú Ä ¢ Ò Ã ¹,ß Î È ' G ¦ G*ü1u)Ú <?U 0!6 Ô þA’ Û Ê È WOj EîE› ¥EÕ IRP_MN_QUERY_STOP_DEVICEQ ¸ ÈA¶KÂPE |/ß c ú Ã ¹ 0!6A¹A’ Û È V pPE |/ß c à ã!8AË" ÈFw È G ¦ G*ü1u)Ú < a ¥EÕ Ô þ IRP_MN_STOP_DEVICE Q ¸ ÈA}PE |/ß c 0!6A¹A’ Û Ä/ÍL8A’ Û,X ¡ 0 3 î4£ Z2O ,XE›/ß ÈE-G á aG¡ á Ä

G b s6Ñ _A’ Û,X(Š ÕE@/ÏE›/ß È Ý ø&• kAÈ â Ö

1. L8 Z0U' /ÏL8 ê5ÙA’ Û Lp,X ™ 6 ¹ ê ÈA’ Û,X 0!6 ê/ÏL8 Ô þ#ý `,X # E›/ß È G ¦ G*ü1u)Ú < ü y *ü ,X 0!6 ê/ÏL8A’ Û,XAË" Ä ü Windows ÈE- EîE› Ô þA’ Û1u)Ú*ü + M6/ß c 9 . ,X ÅÊ ÈîA¶KÂPE |/ß c ÈA}PE |/ß c Ý î ` ä Ô o!7 ü1 Y ê î þ `4§,X I/O Ï u ÄPE |/ß c 3 Ã ¹ ¦4± G ¦ G*ü1u)Ú <,XAË" È !¨ V È ' !E¬ Ý J ª,X v /ß c!7 ü S*ü W,XA’ Û Ä

2. ' G ¦ G*ü1u)Ú <LÔ?UG¡ „ ÚG! Ô þA’ Û,XC $d Ê ÈW Ã ¹ Ý'; Ò ,XCÃ XA}PE |/ß c 0!6A¹A’ Û È' â È ÍA’ ÛG¡ „G!5BC $d È a åPE |/ß c ¥EÕ Ô þ IRP_MN_ START_DEVICE Q ¸ ÈA¹ Q ¸ Ù ÿ Z G ¦ G*ü1u)Ú <,XC $d ÚG! • È ´5àPE |/ß c Ã ¹ Û/ A’ Û ü „,X I/O C $d 5 Ê ß4»4Á ¹ 0 Ä

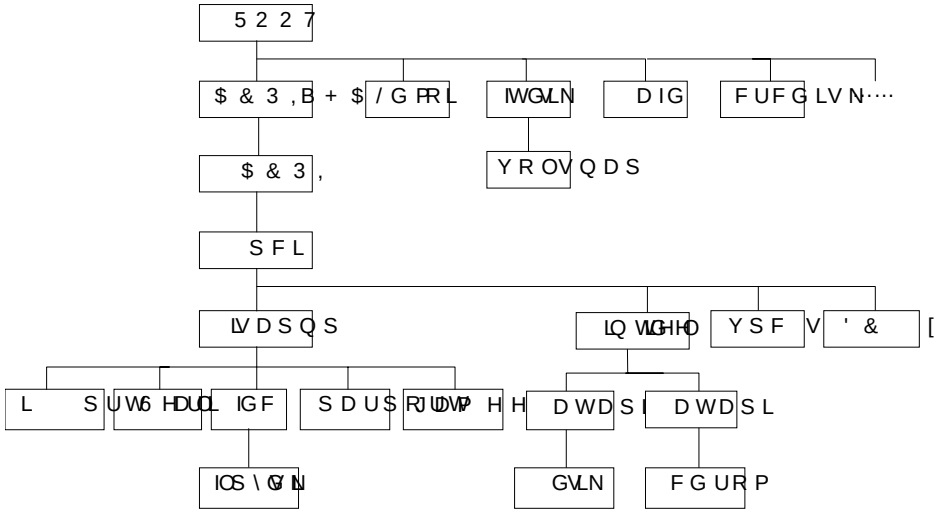
L8 Z Ò 6.8 / ,X IRP_MN_XXX Q ¸ È G ¦ G*ü1u)Ú <EîE› MajorFunction[IRP_MJ_PNP]_/ß ¥EÕ4-PE |/ß c,X rL Q ¸E¬ Ý \ î ÈAË –5× base\ntos\inc\io.h[Ê ,X 156~182> Ä rL Þ È ¢E- o Q ¸ 3 Ã ¹,ß Î G ¦ G*ü1u)Ú < âA’ Û ' xF',X #A, Ä k Ô ¤,X ÈE-4˜ Q ¸ á ™EÖ*ü b s6Ñ _A’ Û È 3EÖ*ü b 4“A’ Û Ä ü Ô þ Õ G ¦ G*ü,X A’ ÛPE |/ß c ÈMajorFunction[IRP_MJ_PNP] _/ß T T Ô þ L _,X(Š Õ r)„ È W B y ,X IRP_MN_XXX Q ¸ 9 ¬A’ Û,X(Š Õ Ä' 5à È (Š Õ EÝ ½ Õ ¾ o Q ¸ ` ¾ o(Š Õ È í Ã6ÑLc- A’ Û,X á à5à Ý á à Ä

A’ ÛPE |/ß c,X º Ô þ ä , AddDevice _/ß G ¦ G*ü1u)Ú < ü y 4“PE |/ß c ¤ o,XA’ Û £EÄ ¹ â ÈJ\ Í 4“ Þ ”# ,X!£ þA’ Û5àA×*ü,X Ä L _,X ™ 6 È'2Ï4³ é Ð Ê È G ¦ G*ü1u)Ú < ™NO ë ÄenumerateÅ Î ' !2Ï4³ Ý,X.@ ÊA’ Û È !8 È WAË" 4“PE |/ß c ¤ o Ý G.@ ÊA’ Û,X µ C È Ù À.@ ÊA’ Û,XC $d?U" È' â È G ¦ G *ü1u)Ú < tEQE- oA’ Û,XPE |/ß c ÈJA×*ü,Ì h,X AddDevice _/ß Äß Ô ã8V å ÀA|AŽ!8 A’ Û ë E›/ß È ¹ ž ü!8E›/ß Î0ŸCK 9,XA’ Û å Ä

A’ Û ë âA’ Û å

A’ Û ë ü I/O 2Ï4³ ñ Ÿ êE›/ß E¯> ,X ÈI/O 2Ï4³ ï Î,X1 Ô þA’ Û ÍB5 + PE |/ß c \Driver\PnpManager r)„,X Ô þ ´ áA’ Û ÍB5 ÄA¹A’ Û ÍB5 ë ,XCK Ÿ&• Ä HAL D• 3>•Ax Ô þ 4“A’ Û È ü Õ ACPI ,X2Ï4³ ÈEîE› HAL A’ Û È Ã ¹E¯ Ô !9 ë ACPI Ä' âE¯ Ô!9 ë PCI 4“ Þ,X Ø/¡A’ Û È Ù ÀEîE› PCI-ISA 9E² y,X A’ Û Ä V!8E¯> ß • È Ý K Ý 4“6Ñ o,XA’ ÛFÑ ¹Eæ &,X • ã ë W À,XA’ Û È,È7Ç Ý,XA’ ÛFÑ>• ë Î 9 Ä

ü ë E›/ß È!£ þ8V&•FÑ EîE› Ô þ2O _ DEVICE_NODE,X ÍB5 9 £EÄ,X ÄLc - ë E›/ß,XE¯> È Ô É ¹ < ¬G£ IopRootDeviceNode 8V&•,X å>• Î0ŸCK 9 Ä 8V &• ·>< ZPE |/ß c \Driver\PnpManager ü ë Ô Ÿ Ê ï Î,X ´ áA' Û ÍB5 Ä!£ Ô þ 4"A' Û ë ,XA' ÛFÑ Ö A¹ 4"A' Û ü8V&•,X ß • È 0 W,X $8V&• Ä ' È DEVICE_NODE D B4§ X4È x Z å,XE² y µ C È¹ ž Û å,Ì hA' Û ÍB5,X ÛJ\ ÄÒ 6.9 ü<. ³)ƒ W ß Ô þ ACPI P •,X Windows Server 2003 SP2Ï4³,XA' Û å È W J"u Ý / Î Ý,XA' Û8V&• ÈE-G / ,X û î D8V&•FÑ âPE |/ß c,Ì Í h Ä ´!8 È Í';>< 6.1 È å À Î Þ Ã ¹)Ú?·E- oA' Û8V&•,X ÿ `*üEè Ä ¢ Ò å À Ã ¹,ß Î È üA¹2Ï4³ È Õ G ¦ G*ü,XA' ÛFÑ EîE› PCI 4" ` PCI-ISA 4" ë Î 9,X Ä º ê Ý ø&• kAÈ â Ö 1 Ô È V p ü Ô Ä(=)Ú <,X2Ï4³ Þ / A' Û å ÈFw È ü ACPI 8V&• ßM6 ÈL8 Zpci 8V &• È å À T TE¬ Ã ¹,ß Ý G+ $d ÃN¢ ê Ø)Ú <1 A' Û8V&• ×1 ` È Í bFw o á Õ G ¦ G*ü,XA' Û È W À,XA' Û8V&•,È y Ö ü 8V&• ß Ä



Ò 6.9 A' Û å/ ã Ò

.@ Ê 4"A' Û Ý6Ñ o ë J ¢ 2,XA' Û ÈE- A' Û ë ,X GK ü È!8 ê È"¼ `>< ,X µ C 3CK ZG¡?U,X 0*ü Ä _ V È 8V&• 0 Ô þ<. ³A' Û8V&• È ý*ü"¼ `>< ,X µ C 9 XEô W,X $8V&• ÄE- o µ C ± , ü HKLM\SYSTEM\CurrentControlSet\Enum\Root ßM6 ,X $K Ä ü ë E›/ß È 8V&•PE |/ß c Í!£ þ $K FÑ î ï Î Ô þA' Û ÍB5 `A' Û8V&• Ä "¼ `>< ,X µ C V) 9,X 6 ÛE- ü]>™ ¡ 02Ï4³ Ê+]>™/ß c ¤ o,X È ê5Ù ü]>™ ¤ oPE |/ß c Ê t 9E¯ 9,X Ä

4§ Ü"¼ `>< ,X µ C ÈG ¦ G*ü1u)Ú < ü ë A' Û,XE›/ß È á ™ î Î0ŸCK Ô É ` H

Windows *Y s)Ú â r)„*

,XA’ Û å È5à è 3 î ^,Ì G,XPE |/ß c tEQ 2Ï4³ J ;> ñ Ÿ ê Ä7 V 6.2.18V Ÿ4¡ È I/O 2Ï4³ ü ñ Ÿ ê Ê ÈOj tEQ J ñ Ÿ ê é Ð- | 2O _,XPE |/ß c ÈE- + IopInitializeBootDriversÑ DJ\ Í!£ þE-/¡2O _,XPE |/ß cA×*ü IopInitializeBuiltinDriver Ñ D 9 r)„,X Ä IopInitializeBootDriversà Ê 3J\ Í!£ þPE |/ß c,XA’ Û ;> ë ¡ 0 Ä2O È ' I/O 2Ï4³ ü tEQ J ñ Ÿ ê 2Ï4³- | ,XPE |/ß c Ê È W 3 î ;> A’ Û ë ¡ 0 È E- ¥*ó ü IopInitializeSystemDriversÑ D Ä+ !8 Ã?• È I/O 2Ï4³ ü ñ Ÿ êE›/ß Æ4£ Î0Ÿ ZA’ Û å Ä

' ÝA’ Û ¬ ê È¨ V ”# „,XA’ Û1 ™ ‰ ¥*ó Ê ÈPE |/ß c Ã ¹A×*ü I/O 2Ï4³ ¤ o ,X Ô o Ñ DG¡ „ ë A’ Û ê5Ù ÚG!C $d ÈE- ,XO API Ñ D Ù À IoInvalidate-DeviceRelationsÃ IoSynchronousInvalidateDeviceRelationsÃs IoReportDetectedDevice ` IoInvalidateDeviceStatê Ä

A’ Û å ,X!£ þA’ Û8V&•FÑ Ý Ô þ á/Ä È/Ä r _CÃ X ÄInstancePath Å È J 6 ã <Enumerator>\<DeviceID>\<InstanceID> È E-G Enumerator 4“PE |/ß c,X á/Ä È DeviceID A’ Û,X Ô ÛAš È5à InstanceID í Ô ÛAš Z Ô þ.@ ÊA’ Û,X r _ Ä"¼ `><K HKLM\SYSTEM\CurrentControlSet\Enumß M6!7 Q ¹ InstancePath,X 6 ã , Z Ô þA’ Û 8V&•,X µ C È E- 3!7 EîE› HKLM\SYSTEM\CurrentControlSet\Enum\Root Ã ¹ ë Î 8V&• ßM6,X Ý $8V&•,X s ´ Ä

ü!£ þA’ Û8V&• ÞFÑ ™ n Ý Ô þA’ Û ÍB5 È/Ä PDO ÄPhysical Device Objecå È E- ü ë E›/ß + 4“PE |/ß c ï Î,XA’ Û ÍB5 Ä Z1u)ÚA¹A’ Û È G ¦ G*ü1u)Ú < tEQ Ô þ s6ÑPE |/ß c È JA×*ü W,X AddDevice _/ß È à Ê Ú PDO ôEæ4-A¹ _/ß Ä8 AddDevice _/ßEî î ï Î Ô þ s6ÑA’ Û ÍB5 ÄFDO È Functional Device Objecå È JA}A¹ FDO L EQ ü PDO Þ È ´!8 È E- ø þ ÍB5 X ä Z Ô þ Î ,XA’ Û Ü È V 6.2.28V E Ä Ä

Í b Ô þA’ Û5à?Ô È PDO,Ì ' b W,X(=)Ú y · È5à FDO í,Ì ' b W,XF Ee y · Ä h *ü/ß c ê Y å Ô þA’ Û ¥E Õ,X I/O AË" È Oj E’ FDO È V p FDO ,XPE |/ß c6Ñ ó,È y Ø)Ú È í á ™ ôEæ4- PDO × ú í È I/O 1u)Ú < Ú!8AË" ôEæ4- PDO Ä º ê k Ô ¤,X È üA’ Û8V&•,XA’ Û Ü È L8 Z PDO ` FDO È Ã6ÑE¬ î Ù ÿ Ô þ ê î þCKE›$¸ 0*ü,X A’ Û ÍB5 È W À + E›$¸PE |/ß c ï Î,X È 0´ 6.5.58V Ú Ÿ4¡E›$¸PE |/ß c,X ¹ 0)Ú Ä

¹ Þ Ÿ4¡ Z G ¦ G*ü1u)Ú <,XA’ Û ë `A’ Û å ÄG ¦ G*ü1u)Ú < üA’ Û ë E›/ß LÔ?U A’ Û tEQPE |/ß c È W V) R Í h,XPE |/ß c È¹ žPE |/ß c ü]>™ Ê h ¤ o ¾ o µ C È G bE- oKÂNl È : á aE¯ Ô!9 Ÿ4¡ È Aï5Ù Ã –5×,Ì GC m [WIN-INTERNALS] Ä

A’ ÛPE |/ß c

A’ ÛPE |/ß c ¡4‰A’ Û,X Y õ + ÈI/O 1u)Ú < Ã G ¦ G*ü1u)Ú < `+ $d1u)Ú <FÑ LÔ?U âA’ Û,XPE |/ß c ' xF' Ä ü 6.2.28V È å À Æ4£,ß Z Y A’ ÛPE |/ß c,X ÍB5 ></ ÈE- Ô8V å ÀOj A|AŽ Windows Õ,XA’ ÛPE |/ß c,X Ú2O È' âEîE› _ $ 9AÈ âPE |/ß c,X ·-Õ4§ X ¹ ž Ø/¡E›$¸PE |/ß c È Ô â Ÿ4¡ Ô ßM2 G ¦ G*üPE |/ß c Ä

A’ ÛPE |/ß c Ú2O

ü Windows I/O2Ï4³ ÈA’ ÛPE |/ß c á ™ ¡ 02Ï4³ ¤ o Z Õ Ø/¡ I/O A’ Û,X 6Ñ o È 3 Windows Y D• =),X Î. Ä Windows Ã ¹ | Õ tEQ ê LEQA’ ÛPE | /ß c ÈEîE›E- oPE |/ß c 9A× H ê =) Y ,X s6Ñ Ä Windows I/O2Ï4³?˜ n ZA’ ÛPE | /ß c hFI ~,X y · ÈE-4˜ y · Eî*ü,X È ÃEÖ*ü b Ý,X Y õ ãPE |/ß c ÄA’ ÛPE | /ß c q B J*üEè á à È Ã ¹ Ú ¹ ß Ý2O Ö

- x G ¦ G*üPE |/ß c È 3/Ä WDM PE |/ß c Ä W ÀEî ZPE |.@ ÊA’ Û5à+ .@ Ê V ¤ o È â Windows ,X I/O 1u)Ú < Ã G ¦ G*ü1u)Ú < `+ $d1u)Ú < ÔCK ¹ 0 Ä Windows 7¾D• ú Z ûG£ G ¦ G*üPE |/ß c È*ü b Õ Ø/¡ ?•,X , |A’ Û Ã?šNe EÖG! < Ã5%4°EÖG! < ¹ žEg 9A’ Û1 Ä
- x Y =)PE |/ß c È3/Ä M2 G ¦ G*üPE |/ß c ÄW À =) Y ,X s6Ñ È ê5Ù ¤ o Z A“KÂ Y õ ã ·-Õ ` D B,X Ô/¡Eè X ÄW À J"u ÝLš ä G ¦ G*ü1u)Ú < `+ $d1u)Ú <,X1u)Ú Š Ä½ ó,X Windows NTPE |/ß c Ä ü é 9 G ¦ G*ü1u)Ú ¹ ! ÅFÑ 2 bE- Ô2O _ È„ ü ¡' Ý ûG£,X Y =)PE |/ß c Ä : ! ´0´)/ ,X ¹ KFÑEîE› E-/¡2O _,XPE |/ß c 99‹ k Y ,X µ C Ä
- x [Ê2Ï4³PE |/ß c ÄW À y J\ Í [Ê,X I/O AË" È aE¯ Ô!9 ÚE- oAË" E@ ¬ ä,ó!7 Í b , |A’ Û ê5%4°A’ Û,X I/O AË" È ¢5à$µC‡ v ,X s ŸAË" Ä ü 6.2.18V å À Ò 4£,ß E› È[Ê2Ï4³2O _,XPE |/ß c>• ü ÍB51u)Ú <,X\FileSystem ,Â) ß ÈJ ª,X PE |/ß c ü\Driver ,Â) ß Ä>< 6.2 ë Î,XPE |/ß cFÑ [Ê2Ï4³PE |/ß c Ä

Windows PE |/ß c õ _ ÄWDM Å ü I/O õ _ r t Z Í G ¦ G*ü Ã+ $d1u)Ú ` Windows 1u)Ú?˜8× ÄWMI Å,X Õ Ä5à è ÈFI ¢ WDM ,XPE |/ß c ü Windows G Ä Ä Ù À Windows 98/Windows 2000 â,X Ý( Å Þ7Ç å $d ·-Õ P •,X È*î7Ç 3 Ã6Ñ `E¯ P •,X ÄWDM PE |/ß c œE¯ Ô!9 Ã ¹ æ Ú ä ¹ ß Ý2O Ö

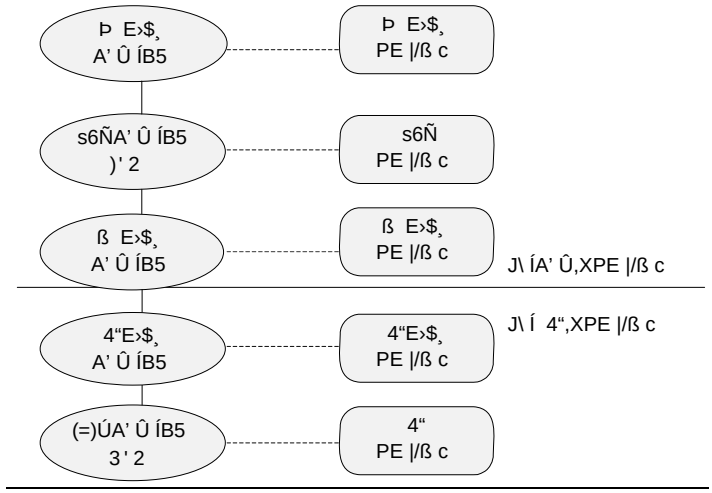
x 4“PE |/ß c ÄNR á ñ È 4“PE |/ß c1u)Ú Ô þ 4“A’ Û È WBóB÷ ”# 4“ ÞL EQ ,X ÝA’ Û ÈJEî-¹ G ¦ G*ü1u)Ú < G bE- oA’ Û,X ™ ‰ Ä 4“PE |/ß c 3BóB÷ 4“ ,X+ $d1u)Ú Ä

x s6ÑPE |/ß c Ä s6ÑPE |/ß c1u)Ú K ',XA’ Û È ü Ô þA’ Û,XA’ Û Ü È s6ÑPE |/ß c ï Î,XA’ Û ÍB5 Ä G FDO Å,Ì ' b ¡ 02Ï4³ { A¹A’ Û,XF Ee y · Ä s6ÑPE |/ß c rL 1u)ÚA¹A’ Û,X s6Ñ õ + Ä

x E›$¸PE |/ß c Ä üA’ Û Ü ÈE›$¸PE |/ß c ! b s6ÑPE |/ß c Þ ê ß È W,X*üEè Ö¸¥?š Ô þA’ Û,X I/O AË" ¹ žE- oAË" ,X Ø)Ú ™ ‰ È ê5Ù È r t ê ¬ Ô þA’ Û ê º Ô þPE |/ß c,X> Ä_ V È+™!¦ ? £ ¹ K ý*üE›$¸PE |/ß c 9,¥?š>•AÏ m ,X [Ê D B Ä

ü WDM È 4“ Û Ã o J ªA’ ÛL EQ,XA’ Û È J ¶ Ý £ PCI ` SCSIE- ,X(=)Ú 4“A’ Û È 3 Ý £ HAL E- ,X<. ³ 4“A’ Û Ä 4“PE |/ß cBóB÷ ”# 4“ Þ,XA’ Û È J è # } G ¦ G*ü1u)Ú < ë E- oA’ Û È5à è W 3 { A¹ 4“,X(=)ÚG!5B Ä¸Ì ¡ È s6Ñ PE |/ß c?U1T) k î ÈEî ¾ { Ô þA’ Û,X.@ Ê5à Æ Ä

ü G ¦ G*ü1u)Ú < ë k ,XA’ Û å È£ þA’ Û8V&•FÑ Ù ÿ Ô þA’ Û Ü ÈA’ Û Ü ,X Ø þA’ Û ÍB5 Ú ÿ+ Í h,XPE |/ß c ï Î ` r)„ Ä Ò 6.12 / Z á à2O _ WDM PE | /ß c üA’ Û Ü ,X?¦8F È ¹ ž W À KÈ,X G2Ï Ä



Ò 6.12 WDM PE |/ß c âA’ Û Ü

!£ þA’ Û ÍB5FÑ + Í h,XPE |/ß c ï Î,X È A’ Û,X PDO + 4“PE |/ß c ï Î,X È

5àFDO + s6ÑPE |/ß c ï Î,X Ä ü PDO ` FDO KÈ È2û ü- PDOÈ Ã ¹ ÝLÊ þ ê î þ 4“E›$¸A’ Û ÍB5 È W À+ ,Ì h,X 4“E›$¸PE |/ß c ï Î Ä ü 4“E›$¸A’ Û ÍB5 ` FDO KÈ È Ã ¹ ÝLÊ þ ê î þ ß E›$¸A’ Û ÍB5 Ä5à ü FDO Þ È í Ã ¹ ÝLÊ þ ê î þ Þ E›$¸ A’ Û ÍB5 ÄE- o ß ê Þ E›$¸A’ Û ÍB5 Ú ÿ+ ,Ì h,X ß ê Þ E›$¸PE |/ß c ï Î Ä WDM ?˜ n ZE- ,XA’ Û Ü4§ X È¶ Ü)Ú A} – â J ,X!£ þPE |/ß c r)„ W BóB÷,XFwF¼ Ú s6Ñ È 3 ¤ o ZC‡ ó,X =) û È AŒE›$¸PE |/ß c ü á à õ Þ,¥?š ê Â!7 Ô þA’ Û,X ¹ 0 • ã Ä âM6 6.5.48V Ú Ÿ4¡E›$¸PE |/ß c,X tEQ ¹ žE›$¸A’ Û ÍB5,X ï ÎNN c Ä

Í b Ô þ K ',XA’ Û5à?Ô ÈFDO ·>< Z W Í b ¡ 02Ï4³,XF Ee y · Ä s6ÑPE |/ß c T T î ï Î Ô þ ·><,Ì h PDO,XA’ Û y · ÄEîE› I/O 1u)Ú < Ñ D IoRegisterDeviceInterfaceÅÈ ´5à h*ü/ß c ê Y J ªF¼ Ú Ã ¹EîE›!8A’ Û y · âA¹A’ Û ' xF' Ä Í b Ô o á 5à œEî *ü,XA’ Û È _ V.•,¬A’ Û `5%4°EÖG! <1 È s6ÑPE |/ß c œ>•E¯ Ô!9 Ú ä î þ(À0Ÿ,XPE | /ß c È+ W À6( ÜCK 91u)ÚA¹ FDO ,X I/O AË" Ä ¢E- Ô ã Þ ÈWDM PE |/ß c Í.@ Ê ,X Õ Ã ¹E¯ Ô!9 æ Ú 2OPE |/ß c Ä class driverÅ `0Ã ·PE |/ß c Äport driver Å È ¹ ž ã 0Ã ·PE |/ß c Äminiport driver ÅÄ 2OPE |/ß c r)„ Z ¤ Ô/¡2O _,XA’ Û,X I/O Ø)Ú Ä Í b Æ 4£ Û š ê,XA’ Û2O _ È!¨ V.•,¬ Ã5%4°EÖG! <1 È ¤ o Ô þ2OPE |/ß c Ã ¹ á à V *ó {,XA’ Û r)„Eî*ü,X á u Ä 0Ã ·PE |/ß c r)„ Z â ¤ Ô2O _ I/O 0Ã ·,Ì G,X I/O Ø)Ú È W À J áFI ¢PE |/ß c,X y ·?U" È5à ¾ Ô o Y õ ã,XEY } _/ß Ä ã0Ã ·PE |/ß c í r)„ ZPE | ¤ Ô(M nA’ Û5àLÔ?U,X I/O á u Ä2OPE |/ß c ` ã0Ã ·PE |/ß c,X Ú ¹ Ã ¹,ß ä J\ Í Ô þ ê Ô2OA’ Û,X Eî*ü ` (M!^ ,X s6ÑF¼ Ú Ä2OPE |/ß c r)„,X Eî*ü ê @ E ,X I/O á u È5à ã0Ã ·PE |/ß c r)„,X J\ Í ¤ Ô(M nA’ Û,X (M!^ s6ÑF¼ Ú Ä ü 7.3.18V Ÿ4¡ , | Ü4§ X Ê È å À Ú î,ß E- ø/¡PE |/ß c,X _ $ ÈE-G á aE¯ Ô!9 Ÿ4¡ Ä

_ $PE |/ß c U P B T U F S

Windows DDK¤ o Z ûG£,XPE |/ß c _ $ È ´ "F! žWindows ¡ 02Ï4³ ÍA’ Û Õ,X • •M6M6 Ä J toaster Ô þEÖ Ü b : 4 WDMPE |/ß c Ô ¥,X8× _ [TOASTER] ÄE- Ô8V Ÿ4¡ toaster_ $,X4˜ äF¼ Ú È ¹ žA¹ _ #] ž,X Ô o V É `*ü"© ÄAÏ5Ù Ã ¹4êA¥ J]>™toaster _ $,XPE |/ß c È ¹ t ÍWindows I/O 2Ï4³,XAxAš Ä

Toaster JM2) þA’ ÛPE |/ß c È,Ì ¡ È W ü Windows2Ï4³ Î0Ÿ Ô 5<. ³ 4“ È J ¤ o Ô þ 4“PE |/ß c Ã Ô þ s6ÑPE |/ß c Ã Ô4˜E›$¸PE |/ß c È ¹ ž Ô oEY } ¹ K Ä Toaster_ $,X ·-Õ ` D B ! b Windows DDK _ $/ß c]>™,Â),X src\general\toaste$,Â) ß Ä>< 6.3 ë Î Z toaster ,XPE |/ß c ¹ ž W À,X ·-Õ ü,X $,Â) Ä

Windows *Y s)Ú â r)„*

><6.3 toaster _ $,XPE |/ß c

PE |/ß c	·-Õ,Â) Ä,Ì Í b toaster _ $,Â) Å	AÈ â
BusEnum.sys	bus	toaster™ ¬ Ú N Q
toaster.sys	func\incomplete1 func\incomplete2 func\featured1 func\featured2	toaster• • ³ y _ Ÿ Ú N Q H • / g Ã 4 Q Q ‡ toaster.sys f µ t } _ Ÿ Ú N Q / O ä ™ ¦ _ Ÿ ¶ Q d featured1¾ ¢ Q û ü Q ‡ [(W • 8 ä WMI featured2) ¢ ä [à - 2 ü ä ¹ Ñ t –
clsupper.sys clslower.sys devupper.sys devlower.sys bfdupper.sys bfdlower.sys	filter	ã ¾ 6 Q ¶ Ò Ú N Q Ó ¹ + h ¶ Ò Ú N Q c+ • ¶ Ò Ú N Q c• • h ¶ Ò Ú N Q c • • • ¶ Ò Ú N Q c ™ ¬ FDO h ¶ Ò Ú N Q ä ™ ¬ FDO • ¶ Ò Ú N Q d ã Ô Ú N Q ¾ ¢ Q ß ¯ Q , Ý ò - ½ d ¹ ¶ _ ¶ / ð o ÿ µ Q , * • • ¼ / * "
Toastmon.sys	toastmon	® Ú N Q f µ t " å } • â f ´ • Ì ä ‰ 8 toaster™ ¬ h ‡ ‡ ¹

üWindows ÈA' ÛPE |/ß c Ô þ Ã | ÕJÒ y,X õ + Ä.sys [Ê È0ú ÜPE [Ê ã [PE-SPEC]Å Ä' 5à È ZA}PE |/ß c>• tEQ 2Ï4³ J è!7.B ¹ 0 ÈPE |/ß c,X ¤ o Eî E¬LÔ?U4ê m ™?U,XG!5B µ C È Ô Î ,X Ô þ.inf [Ê È Ý Ê í Ô oEY },X õ + È*î 7Ç çK¼,X]>™EC ÊTÄaster_ $)/ ,X Ô 5<. ³ 4" ÈW ¤ o Z Ô o ¹ K 9 õ ³ ü 4" Þ ¦ 9 ê ¨L8A' Û È à Ê 3 ¤ o Z,Ì h,X µ C ¹ "A} G ¦ G*ü1u)Ú <6Ñ óAš ÿ!8 4" ¹ ž 4" Þ,XA' Û Ä

ü Windows Server 2003 È 4"PE |/ß c,X]>™ Ã ¹EîE› { M6 S ,X #Ï t.@ Ê å Ð ÄAdd Hardware WizardÅ 9 ` ä Ä ü!8 ]>™E›/ß ÈL8 Z 4"PE |/ß c È .inf [ Ê 3 ™LÔ,X Ä8 ]>™ å ÐL8 Z Ú.sys `.inf [Ê ËBñ ,Ì h,X2Ï4³,Â) ¹ ê È3 î B.inf [Ê ,XA'5B È ü"¼ `>< t 9,Ì h,XK ê È ¹ " G ¦ G*ü1u)Ú <6Ñ ó ë `1u)Ú toaster 4" Þ,XA' Û Ä

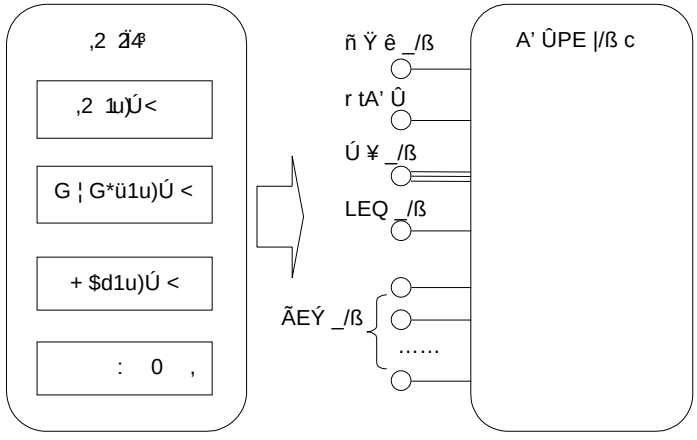
+ b toasterJM2(=)Ú 4" È Z õ ³ ü toaster 4" Þ ¦ 9 Äplug ÅÃ¨L8 Ä unplugÅ` ÎÄeject ÅA' Û,X | 0 È toaster _ $ ¤ o Z Ô þ õ ³ ¹ K enum.exeÈ ¹ Q ¸> ,X • ã ¦ 9 Ã ¨L8 ê Î Ô þ Û n4ê Ë,XA' Û Ä º ø þ ¹ K toast.exe` notify.exe Ú ÿ$è/ Z V) ü h*ü /ß c AÏ m toaster 4" Þ,XA' Û È ¹ ž V)4ê m6Ñ ó-¹ PnP ,X h*ü/ß c ÄPnP-aware applicationÅ Ä Notify.exe å G ¦ G*ü1u)Ú <"¼ ` È ' toaster 4" Þ ÝA' Û ¦ 9 ê ¨L8 Ê W Ã ¹ k Eî-¹ È ´!8 È V p W ' Ô,X toasterA' Û?U>•/ÏL8 È W î>•Eî-¹ È ¢5à Ã ¹ GKÁA¹A' Û È ¹ "A¹A' Û>• ¢ Y , /ÏL8 Ä Notify.exe _ $/ß c$è/ ZE- Ô ."© Ä

' G ¦ G*ü1u)Ú < ”# toaster 4“ Þ Ý „„XA’ Û E’ Ä rL ÞEîE› enum.exe –þQ ¸ 9 õ ³ Å Ê È W | Windows Û š,X #Ï t.@ Ê å Ð 9]>™A¹A’ Û Ä Toaster _ $ ¤ o Z!8]>™E›/ß LÔ?U,X [Ê ` ·-Õ ÈÙ À .inf [ Ê ÃÔ þ2O ]>™ < DLLÄclass installer DLLÅÃ Ô þ # ]>™ < DLL Äco-installer DLLÅÈ¹ ž Ô4˜*ü bEC Ê ]>™Ä software-firstÅ,X ŸBüÄ _ V CD ÅEC Ê Ù ÄE-G ,X2O ]>™ <DLL ¤ o ZJ\ Í toasterA’ Û2O,X ]>™ µ C ÈE- ¾ Ý ü n „„XA’ Û2O Ê ! ™?U,X Ä Toaster,X2O ]>™ <DLL ¤ o Z Ô þ7¾ n ,X Ò Û ` 2 û ÍA± È ' WindowsA’ Û1u)Ú < / toasterA’ Û Ê Ú î S*ü!8 Ò Û ` 2 û ÍA± Ä #]>™ < DLL ; > ,X J\ Í(M nA’ Û r _,X]>™ Ï u È toaster,X #]>™ < DLL !£ þA’ Û ¤ o Z Ô þ Ô,X Ÿ Q á/Ä È ´5à ü WindowsA’ Û1u)Ú < È Ø þ toasterA’ Û Ý á à,X á/Ä Ä

Ý G WindowsA’ Û `A’ ÛPE |/ß c,X ]>™E›/ß È ¹ ž2O ]>™ < DLL ` #]>™ < DLL ,X ` H Ÿ4¡ ÈAË –5× Windows DDK G bA’ Û ]>™,XA º4š [ 7 Ä G b toaster _ $ ÈAÏ5Ù Ã ¹ –5× _ $ D•Lc ú,X [ 7 ` Microsoft ¤ o,X,Ì h [7 Ä toastersamp.doc Å Ä

PE |/ß c,X ·-Õ4§ X

E- Ô8V å ÀOj 9,ß Ô þPE |/ß c,X Î ·-Õ4§ X È' âEîE› toaster _ $,X 4“ PE |/ß c Ã s6ÑPE |/ß c `E›$¸PE |/ß c È 9 : 4E- oPE |/ß c,XA’Au?U&• Ä Ò 6.13 / Z Ô þPE |/ß c hA¹ ˆM ,X Ø/¡ _/ß Ä



Ò 6.13 A’ ÛPE |/ß c,X4§ X

<Q' A’ ÛPE |/ß c Ý â.B,X ÍB5 V É È Ù ÀPE |/ß c ÍB5 `A’ Û ÍB51 È È4± û î DA’ ÛPE |/ß c *ü C AÁ?Ô 94ê m,X È Ù À Þ Ô ã8V Ÿ4¡,Xtoaster _ $,XPE |/ß c Ä ü Ò 6.13 ÈPE |/ß c â I/O 2Ï4³ KÈ,X y · È G Ò / ,X Ø/¡ _/ß È rL Þ PE

Windows *Y s)Ú â r)„*

|/ß c r)„,X Ô4˜ C N¢ ,X Ñ D ÄPE |/ß c D• Ô þ | ÕJÒ y g È =) á .sys È2Ï4³ Æ]>™,XPE |/ß c ! b Windows,Â),X system32\drivers$,Â) ß ÄPE |/ß c,X 9 · Ñ D 3>•/Ä ñ Ÿ ê _/ß ÈE- PE |/ß c>• ñ Ÿ ê ÊOj 9‹ k { ,X ·-Õ ÄJ ª,X _/ß FÑ EîE›!8 ñ Ÿ ê _/ß 9 Û n,X Ä ßM6Eä Ô Ÿ4¡PE |/ß c ˆM ,X _/ß Ä

x ñ Ÿ ê _/ß È PE |/ß c DRIVER_OBJECT ÍB5,X DriverInit ³ Ä üPE |/ß c ÈA¹ _/ßEî >• Q á DriverEntry Ä!8 _/ß ú ø þ – D Ö Ô þ DRIVER_OBJECT ÍB5 Û J\ ` Ô þJ\ ÍA¹PE |/ß c,X"¼ `><CÃ X Äü ñ Ÿ ê _/ß ÈPE |/ß cLÔ?U Ú7¾ Å r)„ ,X y · _/ß ? 1 Ô þ – D Û n,X DRIVER_OBJECT ÍB5 ÈE- ,Ì ' b ÚE- o y · _/ß A• Z I/O 2Ï4³ Ä

!7 V 6.2.1 8V Ÿ4¡,XFw È2Ï4³ ü tEQPE |/ß c Ê È ´AŽ EîE› IopInitializeBuiltinDriver Ñ D ÈE¬ IopLoadDriver Ñ D ÈFÑ îA×*ü ñ Ÿ ê _/ß Ä

x r tA’ Û _/ß È PE |/ß c DRIVER_OBJECT ÍB5,X =)F¼ Ú DriverExtension,X AddDevice ³ Ä ' G ¦ G*ü1u)Ú < ”# Ô þ+ !8PE |/ß cBóB÷,XA’ Û Ê È GA×*ü!8 _/ß 9 r t Ô þA’ Û ÄEî ÈA¹ _/ßA×*ü IoCreateDeviceï Î Ô þ DEVICE_OBJECT ÍB5 È J Ú W t 9 A’ Û Ü Ä

x Ô4˜ Ú ¥ _/ß ÈPE |/ß c DRIVER_OBJECT ÍB5,X MajorFunction D4˜ ³ ÆEîE› I/O 1u)Ú < ¥EÕ,XI/O AË" Ô4œ+ A¹ D4˜ ,X Ñ D 9 Ø)Ú Ä ü Windows Server 2003 È !8 D4˜ E Ù ÿ 27 NM È J Ý IRP_MJ_READÃIRP_MJ_WRITEÈ ¹ ž ! [,ß E›,X IRP_MJ_PNP ` IRP_MJ_POWER1 È K ' n AË –5× base\ntos\inc\io.h[Ê ,X IRP_MJ_<XXX> c n ÄE- o D4˜NM âPE |/ß c6Ñ Ø)Ú,X I/O AË" Í h,X È J Ý o I/O AË" E¬ Ý $ Q ¸ È –?• io.h [Ê ,X IRP_MN_<XXX> n Ä V pA’ ÛPE |/ß c"u Ý Ô þ I/O AË" ¤ o,Ì h,X Ø)Ú _/ß ÈFw È I/O 1u)Ú < ÚA¹ I/O AË" Í h,X D4˜NMA’5B IopInvalidDeviceRequesÑ D È¹ Ñ D ¾ 1T) A’5B I/O AË" ÙÄIRP Å ,X(Š Õ È Û âE- Ô þ ´ ¡ 0 È' â ` ä!8 I/O AË" Ä

x LEQ _/ß È PE |/ß c DRIVER_OBJECT ÍB5,X DriverUnload ³ ÄA¹ Ñ DGž ' ! PE |/ß c *ü ,X2Ï4³C $d È â I/O 1u)Ú < ÚPE |/ß c/ÏL8 Î Y , ÄEî LEQ _/ß â ñ Ÿ ê _/ß,Ì Í h È3 AÈ È ü ñ Ÿ ê _/ß + AË,XC $d È hA¹ ü LEQ _/ß Gž Ä7.B,X LEQ _/ß Ã S kPE |/ß c>• | Õ LEQ5à á îEô ä Ï)C $d"˜$ã ÄPE |/ß c,X LEQ ü2Ï4³4“/ß ÄSystem E¯/ß Å + IopUnloadDriver Ñ D 9 ` ä È ê5Ù ü Ô þ ¹ 0NM,Â ÄWorkItem Å + IopLoadUnloadDriverÑ D 9 ` ä,X È –?• WRK E- ø þ Ñ D,X ·-Õ Ä

x Ô o ÃEÝ,X _/ß ÄEî PE |/ß c Ã6Ñ î#] ž ¹ ß,X _/ß Ö

- o ReInitialize _/ß ÈE- 1 `L !‰ ñ Ÿ ê _/ß Ä üPE |/ß c,X ñ Ÿ ê _/ß ` r tA' Û _/ß>•A×*ü È J è J ª,XPE |/ß c>• tEQ ` ñ Ÿ ê ¹ â ÈReInitialize _/ß Ú>• A×*ü ÄEî È Ô þPE |/ß c ü ñ Ÿ ê _/ß DriverEntry A×*ü IoRegisterDriver-Reinitialization Ñ D Ã ¹,OA„ Ô þ ReInitialize _/ß Ä
- o StartIo _/ß È PE |/ß c DRIVER_OBJECT ÍB5,X DriverStartIo ³ ÄPE |/ß cEî E› Ô þ StartIo _/ß 9 ¥CK Ô õ D B ôEg ÈEî Í b Ô i ,XA' ÛPE |/ß c Ý ã ÄE- S kPE |/ß c Ã ¹ J ¥ Ø)Ú î þ I/O AË" Ä
- o • á u _/ß ÄISR Å Ä8¹A' Û ¹ • • ãEî-¹ Ø)Ú < È íPE |/ß c ™NO4ê m J "¼ `7Ç å Ô þ • á u _/ß Ä Windows ¤ o Z • ÍB5 È AŒPE |/ß c ü á ¡4‰ IDT Ä • £EÄ0ú>< Å,X ™ ‰ ß È Ú Ô þ _/ß â(M n,X • åG£ G6(CK 9 È –?• 5.2.38V,X Ÿ4¡ Ä • á u _/ßEî ¾ ± ,A' Û,X(Š Õ Ë â ¦ 9 Ô þ DPC ÍB5 È ¹ " ü,Ì ÍEW ",X IRQL Þ ` ä I/O Ï u Ä
- o DPC _/ß ÄPE |/ß c ü DPC ÍB5,X ÊE³ _/ß ` ä I/O Ï u È–?• 5.2.48V,X Ÿ4¡ Ä
- o SynchCritSection_/ß È*ü b à!9A"KÂA' Û.@ ÊC $d êPE |/ß c D B,X _/ß ÄPE |/ß cEîE› KeSynchronizeExecution Ñ D 9 à!9 Ô þ SynchCritSection_/ß,X ;> È ¢5à Ã ¹.B ±A¹ _/ß â ISR á î J ¥ ;> Ä
- o AdapterControl_/ß ÄDMA A' Û T T Ý Ô þ AdapterControl_/ß È÷ WBóB÷ ¥CK DMA ¡ 0 ÄPE |/ß cA×*ü IoGetDmaAdapter Ñ D9‹ k Ô þEÖG! < ÍB5 Äadapter object Å È ¹ âA×*üEÖG! < ÍB5 ,X AllocateAdapterControl Ñ D 9 š Û DMA ôEg È5à AllocateAdapterControl A×*ü – D Û n,X AdapterControl_/ß 9 ;> DMA ¡ 0 Ä
- o IoCompletion _/ß È G I/O ` ä _/ß ÄPE |/ß cA×*ü IoSetCompletionRoutine Ñ D Ã ¹A'5B Ô þ I/O AË" ,X ` äEî-¹ ÈA' Û Ü ,X ß PE |/ß c Ô ºA×*ü Z IoCompleteRequest Ñ D È I/O 1u)Ú < î q õA×*ü Þ PE |/ß cA'5B,X ` ä _ /ß È Ô âE¨ ²7Ç I/O AË" ,X ¥CK5Ù Ä –5×6.6.48V Ÿ4¡,X I/O ` äE›/ß Ä
- o Cancel _/ß È G I/O ª#\ _/ß Ä â ` ä _/ß,X ™ 62O È Ô þPE |/ß c Ã ¹A×*ü IoSetCancelRoutine Ñ D È 9A'5B Ô þ I/O AË" ,X ª#\ _/ß Ä 'PE |/ß cA×*ü IoCancelIrp Ñ D Ê È ª#\ _/ß Ú>•A×*ü Ä â ` ä _/ß ™ 6 á à,X È ª#\ _/ß J áJ\ ÍA' Û Ü õ (M n,XPE |/ß c È5à J\ Í Ô þ I/O AË" È ¹ È Ô þ I/O AË" ¾ Ý Ô þ ª#\ _/ß Ä

o n Ê < _/ß Ä IoTimer Å Ä+ b.@ Ê ¡ 0,X á.B n û ÈA’ ÛPE |/ß c Ý Ê íLÔ?U < ó û . Ô o ” ¹ ¹ 0 È!¨ V ¹,ß Ô þ I/O úCY Ê Ã n ó „PE |/ß c ,X ¤ o ¬G£ Ä!¨ VAu D < Å È ê5Ù ¤ o YF¼ ¡ 0E¯> Au Ê1 ÄPE |/ß cEîE› IoInitializeTimer/IoStartTimer/IoStopTimeÑ D 9 S*ü I/O n Ê < ÄI/O n Ê < Ô º>• "¼ ` È í!£/¦Js>•A×*ü Ô õ Ä I/O n Ê < _/ß rL Þ DPC _/ß È¾ áE› W G6(Z Ô þA’ Û ÍB5 È J è I/O 1u)Ú <!£/¦JsA×*ü W Ô õ ÄA’ Û ÍB5 DEVICE_OBJECT 4§ X ,X Timer ä ,A„) Z â G6(,X n Ê < ÍB5 Ä I/O 1u)Ú < Ú Ý,X I/O n Ê <4˜4› ä Ô þJÒ>< È¨ â ü Ô þ 1 s,X2Ï4³ n Ê < Ä < ,X n Ê < ¬G£ IopTimer Å q õ?º ¥ Ý Æ4£>• |,X I/O n Ê < ÄAÏ5Ù Ã ¹ –5× IoInitializeTimer Ã IoStartTimerÃIoStopTimer ¹ ž IopTimerDispatchÑ D,X ·-Õ r)„ Ä

´!8 È å À Ã ¹,ß ÈPE |/ß c Bü Þ ¹ ÞE- o y · _/ß,XLš Ü ÄE- o _/ß Ú ÿ – â âA’ Û,Ì G,X I/O AË" ,X Ø)Ú È Ý o _/ß,X ã Ò ,È y ¡4‰.@ ÊA’ Û È5à Ý o _/ß Z – â I/O 1u)Ú <,X1u)Ú Š ÄßM6 Ÿ4¡ toaster_ $?UPE |/ß c,X Î r)„ È V><6.4 / Ä

><6.4 toaster _ $?UPE |/ß c,X _/ßAÈ â

PE |/ß c	Õ,X _/ß	AÈ â
BusEnum.sys ™ ¬ Ú N Q	z ³ $ H Q	DriverEntry Æ ô Ü N [c P H Q • " þ DriverObject /
	¢ ¦ ` Ó Ÿ H Q	Bus_<Xxx> Æ ô g ó Bus_CreateClose Bus_PnP Bus_Power Bus_IoCtl ä Bus_SystemControl
	á { H Q	Bus_DriverUnload Æ ô Â , ‡ W
	™ ¦ • • H Q	Bus_AddDevice Æ ô — Ù • • s À FDO É { þ • • ¼ / _ • • Ç
toaster.sys _ Ÿ Ú N Q	z ³ $ H Q	DriverEntry Æ ô Ü N [c P H Q • " þ DriverObject /
	¢ ¦ Ó Ÿ H Q	g ó ToasterDispatchPnp ToasterDispatchPower ToasterCreate ToasterSystemControl ToasterCleanup ToasterDispatchIO c ToasterReadWrite c ToasterDispatchIoctl ToasterClose
	á { H Q	ToasterUnload Æ ô Â , ‡ W
	™ ¦ • • H Q	ToasterAddDevice Æ ô — Ù • • s À FDO É { þ • • ¼ / _ • • Ç z ³ $ (W q _

PE |/ß c	Õ,X _/ß	AÈ â
devupper.sys ¶ Ò Ú N Q	z ³ $ H Q	DriverEntry Æ ô Ü N [c P H Q • " þ DriverObject /
	¢ ¦ Ó Ÿ H Q	g ó FilterDispatchPnp¢ FilterDispatchPowerä Filter-DispatchIo » ƒ ¢ Q o Ó Ÿ H Q FilterPass
	á { H Q	FilterUnload Æ ô â ³ å ¬) ÿ ¹ Æ
	™ ¦ • • H Q	FilterAddDevice Æ ô — Ù ¢ Q ¶ Ò • • s À FiDO É { þ • • ¼ /

ü 4“PE |/ß c BusEnum.sys È Í IRP_MJ_PNPQ ¸,X Ø)Ú ü Bus_PnPÑ D ` ä,X Ä 4“ Þ ¦ 9 Ã ¨L8 ` ÎA’ Û,X | 0 + IRP_MJ_DEVICE_CONTROLQ ¸ ,X Ý þ $ Q ¸ 9 õ ³,X Ä ü y ¦ 9 Ô þ toasterA’ Û,X I/O AË" Ê ÈPE |/ß c ï Î Ô þA’ Û ÍB5 Ä ä A¹A’ Û,X PDOÅ È J ;> ñ Ÿ ê È' âA×*ü IoInvalidateDeviceRelationsÑ DEî -¹ G ¦ G*ü1u)Ú <!8A’ Û ¦ 9E¯ 9 × ¨L8A’ Û,XE›/ß2O È WOj A’5BA’ Û ÍB5,X , ü Û « ÄA’ Û ÍB5 DeviceExtension¸X Present³ È+ BusEnum.sysPE |/ß c 9 n Å FALSE È ' âA×*ü IoInvalidateDeviceRelationsÑ D ÈEî-¹ G ¦ G*ü1u)Ú <G¡ „ ” ¹ 4“ Þ,XA’ Û8V &• Ä ÎA’ Û,X Ø)Ú EîE›A×*ü G ¦ G*ü1u)Ú <,X IoRequestDeviceEjectÑ D 9 ` ä,X Ä

4“PE |/ß c BusEnum.sysBóB÷ ø/¡2O _,XA’ Û ÍB5 Ö Ô/¡ 4“A’ Û,X FDO È º Ô/¡ A¹ 4“ ÞL EQ,XA’ Û,X PDOÄA’ Û ÍB5,X DeviceExtensionä ,,X IsFDO ³*ü b ÚE- ø/¡ ™ 6 Ä ü Bus_PnP Ñ D È å À Ã ¹,ß E- ø/¡A’ Û ÍB5,X G ¦ G*ü Q ¸ Ú ÿ + Bus_FDO_PnP` Bus_PDO_PnPÑ D 9 Ø)Ú Ä Í b+ $d Q ¸ IRP_MJ_POWER¸X Ø)Ú 3 2 O È Bus_Power q B á à ¸ X A ’ Û Í B 5 2 O _ È Ú ÿ A ›Bú& Bus_FDO_Power ê Bus_PDO_PowerÑ D Ä G bE- ø/¡A’ Û ÍB5,X G ¦ G*ü Q ¸ `+ $d Q ¸,X K ' r)„ ÈAË –5× toaster _ $,X bus\pnp.c ` bus\power.c [ Ê ,X ·-Õ ÄToaster _ $,XAÈ â [ 7 Ätoaster.htmÅ·Gž Z+ $d $ Q ¸ IRP_MN_QUERY_POWER` IRP_MN_SET_POWERü ´ þPE |/ß c ,X ôEæCÃ X Ä

Toaster.sys toasterA’ Û,X s6ÑPE |/ß c È W$è/ Z G ¦ G*ü Q ¸,X Ø)Ú Ã+ $d Q ¸ ,X Ø)Ú Ä Õ D0 ÃD1 ` D3 A’ Û+ $d(Š Õ Å ` WMI Õ È à Ê W 3 ÕA’ Û,XAï m ¡ 0 È AŒ h*ü/ß cEîE› API Ñ D DeviceIoControl 9 ¡4‰A’ Û ÄToaster _ $,X h*ü/ß c toast.exeÃ ¹# A© toasterA’ Û,XAï ¡ 0 ` DeviceIoControl ¡ 0 Ä

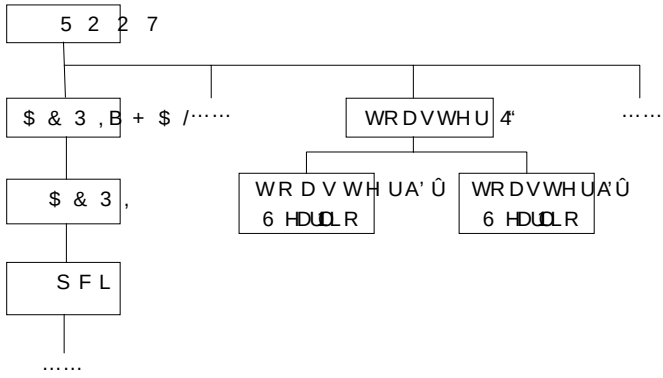
Toaster _ $ ¤ o Z 6 þE›$¸PE |/ß c ÈE- oPE |/ß c ¾ Ô þ Î Š È W À E*ü à Ô Ñ ·-Õ È ÿ ™ ü b W À,X4êA¥G!5B `.inf [Ê ÄE›$¸PE |/ß c ^ Ý,XM2 G ¦ G*ü

I/O AË" ,È y ôEæ4- ß ,XPE |/ß c Ä Q ¸ Ø)Ú Ñ D FilterPassÅ ×5à Í b4± û î D G ¦ G*ü Q ¸ È W Î Þ 3 Ñ+9 á \ Ø)Ú È á1u â È WFÑ î Ú I/O AË" ôEæ4- ß PE |/ß c Æ›$¸PE |/ß c r)„ Z Ô ^7¾ n ,XJÕÄA' Û ÍB5,X DeviceExtension->RemoveLock ä , Å È ¹ ± xA' Û ÍB5 ü I/O AË" E¯> E›/ß á î>• LEQ Ädetach Å ` ôL8 Ä

Toaster _ $,XPE |/ß c J"u Ý r)„ rBü û,X s6Ñ È È J Í b G ¦ G*ü Q ¸ `+ $d Q ¸,X r)„ ··Õ$è/ Z Ô þPE |/ß c üEî ™ 6 ß h V) Ø)ÚE- o Q ¸ Ä4§ Ü _ $ 4- Î,X Ô oEY } ¹ K È J?– ³A×A©Eg Î µ C Ä G ··Õ ,X DbgPrint Eg Î Å ÈE- Í b)Ú ?·E- oPE |/ß c â I/O 1u)Ú < Ã G ¦ G*ü1u)Ú < ¹ ž+ $d1u)Ú <,X x fM2 Ý } Ä ÎA, AÏ5Ù üA×A© < ê5Ù Ã?– ³A×A© µ C,X ¹ KÄ _ V DebugViewÅ " ¹ I/O AË" ,X ;> ™ ‰ Ä

U PA' ÊÛ,XA'UÛFÜS

!M6 6.3.38V Ÿ4¡ Z G ¦ G*ü1u)Ú < ë A' Û,XE›/ß È ¹ ž+ !85à Î0ŸCK 9,XA' Û å žA' Û8V&• Ä)„ ü å À 9,ß Ô,ß toaster _ $,XPE |/ß c V) – â !8E›/ß ÄOj È å À,ß Ô ß toasterA' Û üA' Û å ,X !5B È V Ò 6.14 / Ä

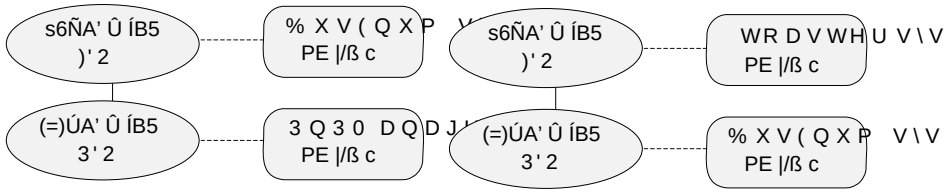


Ò 6.14 Ù ÿ toaster 4" `A' Û,XA' Û å

Toaster 4" ,È yE² y ü ÄROOT Å8V&• ß,XA' Û È ' toaster 4">•]>™ 2Ï4³ ¹ â ÈL8M2 ã ôL8 W È ú í!£ õ2Ï4³ é Ð Ê È G ¦ G*ü1u)Ú <FÑ î ï Î toaster 4"A' Û È J è Ú 4"PE |/ß c BusEnum.systEQ 2Ï4³ Ä!7 V 0´ !M6 A† È'¼ `>< A„) Z ROOT ßM6,XA' Û Ä ! bCÃ X HKLM\System\CurrentControlSet\Enum\RoÅtÄ ´ !8 È<Q' BusEnum.sysPE |/ß c,X |2O _ ÝLÔ- | È W ü é Ð Ê>• tEQ 2Ï4³ Ä V p å À Ú toaster 4"A' Û ¢A' Û å | ôL8 ê/U!6 Ä ü Windows,XA' Û1u)Ú < È ü toaster 4"A' Û ÞEÝ ½ LEQ ê /U*ü G Ã Å ÈFw È BusEnum.sysPE | /ß c Ú á î a ü é Ð Ê>• tEQ ` | Ä

Windows *Y s)Ú â r)„*

ü toaster 4“A’ Û,X8V&• Þ È JA’ Û Ü,X4§ X Ö PDO PnPManagePE |/ß c ï Î ,XA’ Û ÍB5 ÈFDO í BusEnum.sysPE |/ß c ï Î,XA’ Û ÍB5 È V Ò 6.15(a) / ÄE- ø þ A’ Û ÍB5 G ¦ G*ü1u)Ú < ü ë A’ ÛE›/ß Û/ PnPManager` BusEnum.sysPE |/ß c ï Î,X ÄJ FDO + BusEnum.sysPE |/ß c,X r tA’ Û _/ß ï Î,X ÄA¹ _/ßL8 Z ï Î FDO J Ú JL EQ A’ Û Ü ¹ ê ÈE¬A×*ü Z IoRegisterDeviceInterfaceÑ D È ï Î Ô þA’ Û y · Ädevice interfaceÅ J"¼ ` I/O 2Ï4³ Ä



Ò 6.15 toaster 4“ `A’ Û,XA’ Û Ü

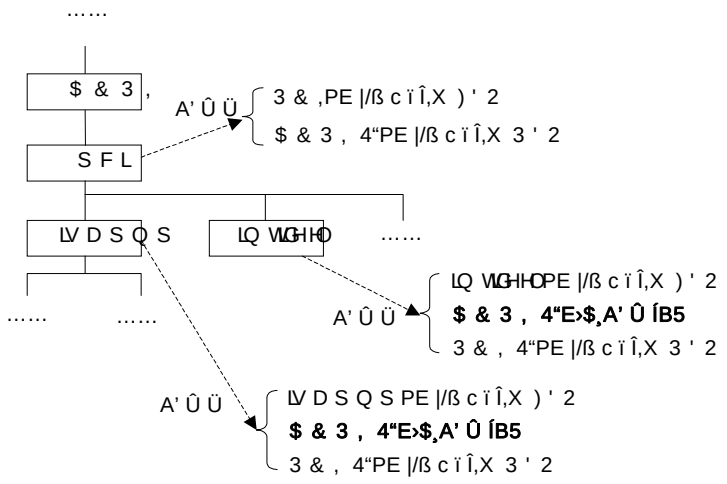
A’ Û y · h*ü/ß c âA’ Û KÈE¯> Eî µ,XG¡?UEè X Ä!£ Ô þA’ Û y ·2OFÑ Ý Ô þ GUIDÄ128 ! Ô ÛAš0ú Å Ètoaster 4“,XA’ Û y ·2O,X ÛAš0ú GUID_DEVINTERFACE_ BUSENUM_TOASTERÈ5à toasterA’ Û,X ÛAš0ú GUID_DEVINTERFACE_TOASTERÄ 'A’ ÛPE |/ß cA×*ü IoRegisterDeviceInterfaceÑ D"¼ `A’ Û y ·2O `A¹ y ·2O,X Ô þ r _ Ê ÈI/O 1u)Ú < ¤ o Ô þ0ú ËJÒ y á 9></ A¹A’ Û r _ È!80ú ËJÒ y á" ± , ü"¼ ` >< Ä´!8 È h*ü/ß c Ã ¹ ¹A¶A’ Û y ·,X r _ È J9‹ k0ú ËJÒ y á È’ â ý*ü!80ú ËJÒ y áA“KÂ,Ì h,XA’ Û ÄToaster _ $ ,X enum.exe` toast.exe/ß c$è/ ZE- Ô*ü"© Ä

Ò 6.14 / Z ü toaster 4“ ßM6 Ý ø þ toasterA’ Û8V&• ÄToasterA’ Û8V&•,XA’ Û Ü ÖPDO BusEnum.sysPE |/ß c ï Î,XA’ Û ÍB5 ÈFDO í toaster.sysPE |/ß c ï Î ,XA’ Û ÍB5 È V Ò 6.15(b) / Ä!7 V Þ Ô ã8V EÄ È ' õ ³/ß c enum.exeÛ/ toaster 4“ ¦ 9 Ô þ toaster A’ Û Ê Ètoaster 4“PE |/ß c ï Î Ô þ PDO ÍB5 È' â ý*ü IoInvalidateDeviceRelationsÑ D ÈEî-¹ G ¦ G*ü1u)Ú < „A’ Û,X 9 Ä G ¦ G*ü1u)Ú < toaster tEQPE |/ß c Ä8¹ Ý ™?U Å È JA×*ü W,X r tA’ Û _/ß È „A’ Û ï Î FDO Ä ü toaster.sysPE |/ß c,X r tA’ Û _/ß Ä G ToasterAddDeviceÑ D Å È W ï ÎA’ Û ÍB5 J ;> ñ Ÿ ê È' âA×*ü IoAttachDeviceToDeviceStackÑ D È ÚA’ Û ÍB5 t 9 A’ Û Ü Ä Ô âA×*ü IoRegisterDeviceInterfaceÑ D A¹ toasterA’ Û"¼ ` toasterA’ Û2O `A’ Û2O r _ Ä ´!8 Ètoast.exe Ã ¹ ¹A¶ toasterA’ Û2O,X r _ È JEîE› I/O 1u)Ú < å W À ¥EÕI/O AË" Ä

E›$¸PE |/ß c,XG!5B ` tEQ

ü Ô þ G ¦ G*üA' Û,XA' Û Ü È PDO ` FDO ™LÔ,X È W À .B ±A¹A' Û!7 ¹ 0,X Î. Ä' 5à È!7 V Ò 6.12 / È üA' Û Ü E¬ Ã ¹ Ý î þ ÃEÝ,XE›$¸A' Û ÍB5 ÈE- oE›$¸A' Û ÍB5 ! b FDO ,X ÞM6 ê5Ù ßM6 È W À+ ,Ì h,XE›$¸PE |/ß c ï Î ÄWindows I/O 2Ï4³ Õ Ý/¡E›$¸PE |/ß c Ö 4"E›$¸PE |/ß c Ã Þ E›$¸PE |/ß c ` ß E›$¸PE | /ß c Ä 4"E›$¸PE |/ß cJ\ Í 4" Þ Ý,XA' Û ›5à Þ ß E›$¸PE |/ß c Ú ÿJ\ Í(M n,X A' Û2O ê(M n,XA' Û r _ È ¹ È W À œ Ú 2OE›$¸PE |/ß c `A' ÛE›$¸PE |/ß c Æ- Ô ã8V å À ÚEîE› _ $ 9AÈ â á à2O _E›$¸A' Û ÍB5,X ï ÎE›/ß Ä

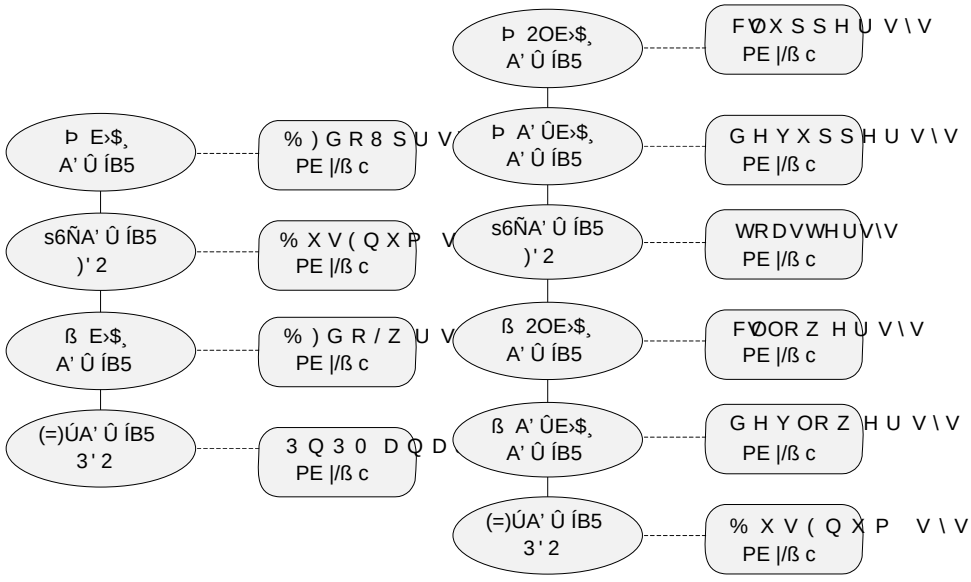
4"E›$¸PE |/ß c Ô/¡J\ Í Ô 5 4" Þ ÝA' Û,XE›$¸PE |/ß c È W ï Î,XA' Û ÍB5 ! bE- oA' Û,XA' Û Ü,X PDO Þ È ! b FDO ` J ªE›$¸PE |/ß c ß Ä Windows ` DDK ,X [7 J"u Ý £EÄ V) ï Î `G!5B 4"E›$¸PE |/ß c Ä 0 Ô þ L _,X _ $ È ACPI PE |/ß cL8 Z Ô þ 4"PE |/ß c ¹ ê È 3 Ô þ 4"E›$¸PE |/ß c Ä Ò 6.16 / Z Ô É2Ï4³A' Û å,X ÔF¼ Ú È Ò ,X2k 'F¼ Ú ·>< Z 4"E›$¸PE |/ß c ï Î,XA' Û ÍB5 Ä PCI 4" Þ,XA' Û È µ Õ ACPI ,X ÈFÑEîE› ACPI E›$¸PE |/ß c 9 ;> A' Û+ $d1*+9 ` Ø)Ú+ $d I/O AË" Æ-w E- o ACPI A' Û ÍB5 V) ï Î Ã+ AÕ ï Î,X 6 Û W À + PCI 4",X PDO ÈG ACPI 4"PE |/ß c ï Î,XA' Û ÍB5 Èü Ø)Ú IRP_MJ_PNPQ ÆIRP_MN_ QUERY_DEVICE_RELATIONS $ Q ¸ Å Ê ï Î JL EQ PCI A' Û,XA' Û Ü ,X Ä



Ò 6.16 ACPI 4"E›$¸PE |/ß c/ ã Ò

4"E›$¸PE |/ß c ¬ ê r ,X 4"PE |/ß c,X> Ä GA' Û,X PDO ,X s6Ñ Å È W À ! bA' Û,X PDO Þ È5à è Ëï þ 4"E›$¸A' Û ÍB5 Ã ¹L EQ à Ô þ PDO Þ Ä

V p ^ toaster_ $,X 6 þE›$¸PE |/ß c Ä J ··Õ ! b toaster\filter,Â) ß Å4êA¥ Î 9 È í Ã ¹ k á/Ä á à,XE›$¸PE |/ß c Ä8¹ ü]>™ toaster 4“ ` toasterA’ Û,XPE |/ß c ÄEîE› #Ï t.@ Ê å Ð Å Ê È Û nA¹ _ $ ¤ o,X busf.inf ` toasterf.inf [Ê È íE- oE›$¸PE |/ß c 3 î>•]>™ 2Ï4³ Ä K ',X]>™!9Px –?• toaster _ $,X toaster.htm[Ê Ä]>™ ` ä ¹ â È å À Ã ¹ k Ò 6.17 / ,XA’ Û Ü È+ !8 Ã ¹,ß E- 6 þE›$¸PE | /ß c üA’ Û Ü ,X !5B Ä"¼ ã È toaster_ $ J"u Ý Ù ÿ 4“E›$¸PE |/ß c ÄüE- 6 þE›$¸ PE |/ß c ÈBFdoUpr.sys ` devupper.sys Þ A’ ÛE›$¸PE |/ß c Èclsupper.sys Þ 2OE›$¸PE |/ß c ×BFdoLwr.sys ` devlower.sys ß A’ ÛE›$¸PE |/ß c Èclslower.sys ß 2OE›$¸PE |/ß c Ä



D WR D V WH U 4“,XA’ Û Ü E WR D V WH UA’ Û,XA’ Û Ü

Ò 6.17]>™ ZE›$¸PE |/ß c â,X toaster 4“ `A’ Û,XA’ Û Ü

ü toaster_ $ È toasterA’ Û,XA’ Û Ü Ù ÿ Z Þ ß ,X2O `A’ ÛE›$¸A’ Û ÍB5 ÈV Ò 6.17(b) / Ä ' G ¦ G*ü1u)Ú < Ô þ toasterA’ Û tEQPE |/ß c Ê È W B"¼ `>< ,X µ C 9.B nE- oE›$¸PE |/ß c ÈJ èA×*üPE |/ß c,X r tA’ Û _/ß È¹ “ ï ÎE›$¸A’ Û ÍB5 J Ú JL EQ A’ Û Ü Ä ü Windows Server 2003 ÈE- ÔE›/ß ü G ¦ G*ü1u)Ú < ,X PipCallDriverAddDeviceÑ D ` ä,X Ä

WRK "u Ý ¤ o PipCallDriverAddDeviceÑ D,X ··Õ ÈA¹ Ñ D,X6 B÷ È ” ¹ Ô þA’ Û8V&•,XPE |/ß c ú Æ4£ tEQ È8¹ Ý ™?U È í tEQ W qC*,XPE |/ß c Ä ü PipCallDriverAddDeviceÑ D>•A×*ü ¹ ! ÈA’ Û8V&• ,X PDOÄ ¹ ž 4“E›$¸A’ Û ÍB5 È

8¹ Ý,XA± Å Æ4£ ï Î ` ä È FDO î þ ï Î Ä PipCallDriverAddDeviceÑ D B"¼ `>< ,X µ C È XEô Ô þPE |/ß c ë>< È Ù À Þ ß E›$¸PE |/ß c È â Ý';NN cEä þA×*üPE |/ß c,X r tA' Û _/ß Ä üPE |/ß c,X r tA' Û _/ß È Û š,X ."© ÈOj A×*ü IoCreateDeviceÑ D ï Î Ô þA' Û ÍB5 È' âEîE› IoAttachDeviceToDeviceStackÑ D È Ú „ Î,XA' Û ÍB5 t 9 A' Û8V&• Ä+ b IoAttachDeviceToDeviceStackÑ D ÚA' Û Í B5 ¦ 9 A' Û Ü,XNJF¼ È ¹ ÈPipCallDriverAddDevice Ñ D ™NO Ý';+ ß T Þ,XNN c 9 A×*ü r tA' Û _/ß ÄPipCallDriverAddDevice XEô,XPE |/ß c ë><,XNN c V ß / Ö

- x Oj A' Û ë K ,X LowerFilters Û n,X ß E›$¸PE |/ß c ÄA' Û,X ë K ! b "¼ `><,X HKLM\System\CurrentControlSet\Enum ßM6A¹A' Û Í h,X $K È_ V È c ë Ë 1 ,X toasterA' Û,X ë $K {B85B7C50-6A01-11d2-B841-00C04FAD5171} \MsToaster\1&2d12bed1&1&0È E- A¹A' Û8V&•,X r _CÃ X ÄInstancePathÅ È J4§ X V 6.3.38V Ÿ4¡ Ä üE- þ _ $ È!8 $K ,X LowerFilters devlower È ¹ Èdevlower.sys PE |/ß cOj >• R Ä
- x y ß 9 A¹A' Û,X2OK ,X LowerFilters Û n,X ß E›$¸PE |/ß c ÄA' Û,X2OK ! b"¼ `><,X HKLM\System\CurrentControlSet\Control\Class ßM6 È_ V È toasterA' Û,X 2O GUID {B85B7C50-6A01-11D2-B841-00C04FAD5171} È ¹ ÈClass K ßM6A¹ GUID K toasterA' Û,X2OK Ä üE- þ _ $ È LowerFilters clslower È ¹ È clslower.sysPE |/ß c 3>• t 9 ë>< Ä
- x ' â üA' Û,X ServiceK Û n,X s6ÑPE |/ß c ÄA' Û,X ServiceK ! b"¼ `><,X HKLM\System\CurrentControlSet\Services ßM6 Ä_ V È toasterA' Û,X ServiceK toaster $K Ä b È s6ÑPE |/ß c toaster.sys3>• t 9 ë>< Ä
- x a y ß 9 A' Û ë K ,X UpperFilters Û n,X Þ E›$¸PE |/ß c Ä2O È ü {B85B7C50-6A01-11d2-B841-00C04FAD5171}\MsToaster\1&2d12bed1&1&01$ K ÈUpperFilters devupper È ¹ Èdevupper.sys >• t 9 ë>< Ä
- x Ô â A' Û2OK ,X UpperFilters Û n,X Þ E›$¸PE |/ß c Ä2O È ü toasterA' Û 2OGUID K ,X UpperFilters clsupper È ¹ È clsupper.sys>• t 9 ë>< Ä

4£E› ¹ Þ ð2öE›/ß ÈPipCallDriverAddDevice Ñ D9‹ k ZA' Û8V&•,X ÝPE |/ß c È ¢5à Ã ¹ XEô ÎA¹A' Û,XA' Û Ü Ä Ò 6.17(b)7 ¹ Þ ` H ð2ö!9Px,X Ô þ _ $ Ä5à Ò 6.17(a) ,X BFdoLwr.sys ` BFdoUpr.sysPE |/ß c í ü toaster 4"A' Û,X ë K ,X LowerFilters ` UpperFilters Û n,X ÈA¹ ë K ! b HKLM\System\CurrentControlSet \Enum\Root\System\<nnnn È E-G nnnn Ô þ 4 ! D +4ê Ë È ¢ 0000 Ô Ÿ È toaster 4"

,X K '4ê Ë ª ‡ b]>™ J 4“PE |/ß c Ê Æ Ý2Ï4³A’ Û ÄSystem Device Å,X4ê Ë ™ ‰ Ä

¹ Þ £EÄ ZE›$¸PE |/ß c,X ð2öNN c È+ b ÞM6 ¤ ,X UpperFilters ` LowerFilters "¼ `>< î +0ú 2O _ ÄREG_MULTI_SZ Å È ´!8!£ þ FÑ Ã ¹ Û n î þE›$¸PE |/ß c Ä¢A’Au?¦ z ÈE- o Û n,XE›$¸PE |/ß c á hA¹ qC* b W À üE- o ,XNN c ÄA@ V ÈÔ þ ß 2OE›$¸PE |/ß c á hA¹?U" W ™NO Î)„ ü LowerFilters ,X ¤ þ(M n !5B Þ È È Ý Ô&• Ã ¹ ±A•,X È G W ï Î,XA’ Û ÍB5 Ô n ! b FDO ` Þ E›$¸PE |/ß c,X ßM6 ÄE- o.B n,X ` á.B n,XNN c G2Ï î E ¡ I/O AË" üA’ Û Ü ,X Ø)ÚNN c Ä

G ¦ G*ü1u)Ú < ¢ LowerFilters ` UpperFilters"¼ `>< 9‹ k,X ™ ™ E›$¸PE |/ß c,X á u á È5àE›$¸PE |/ß c,ó!7,X µ C ! b HKLM\System\CurrentControlSet\Services ßM6 Ä ÝE- oPE |/ß c ÈÙ À s6ÑPE |/ß c `E›$¸PE |/ß c ÈV p î þ>• tEQ 2Ï4³ È íEîE› IopLoadDriver Ñ D>• tEQE¯ 9 Ä

Fw ÈÝ GE›$¸PE |/ß c,X"¼ `>< µ C V ) Î0ŸCK 9 6 ÛE- + E›$¸PE |/ß c,X,Ì h ]>™/ß c 9 ` ä È ê5ÙLc s6ÑPE |/ß c ÔCK]>™,X Ä ü]>™A’ Û ÄA@ VEîE›2Ï4³,X #Ï t .@ Ê å Ð Å êEC Ê Ê ÈEî Ý Ô þ.inf [Ê £EÄ ZPE |/ß c,X,Ì G µ C È Ù ÀA’ Û,X2O GUID Ã V µ C Ã"¼ `><CÃ X È¹ ž!£ þPE |/ß c )(À,X"¼ ` µ C1 Ä ü toaster _ $ È å À Ã ¹,ß î þE- ,X.inf [Ê È Ù À 8V ! [¤ ,X busf.inf ` toasterf.inf ÈEîE›E- ø þ [Ê £EÄ,X µ C Ã ¹ Î0ŸCK Ò 6.17 / ,X Ù ÀE›$¸A’ Û ÍB5,XA’ Û Ü Ä

G btoaster_ $,X]>™E›/ß ¹ ž.inf [Ê,X Y • ÈAË –5× 6.5.28V,X Ÿ4¡ ¹ žA¹ _ $Lc ú,X Ô oAÈ â [Ê È 3 Ã ¹ ¢Internet Þ ¹,ßWindows DDK G b toaster_ $,X6([7 [TOASTER][TOASTER-DOC] Ä

M2 G ¦ G*üPE |/ß c

L8 Z âA’ Û G6(,X G ¦ G*üPE |/ß c È WindowsE¬ ÕM2 G ¦ G*üPE |/ß c ` [ Ê2Ï 4³PE |/ß c ÄE- Ô8V å ÀA|AŽM2 G ¦ G*üPE |/ß c ÈE-/¡PE |/ß c 3/Ä Y = )PE |/ß c È ü Windows PE |/ß c õ _ ÄWDM Å Î)„ ¹ !,XPE |/ß c 2 bE- Ô2O È W À ü Windows 2000/XP/Server 2003 â4Á( ¡' Ã ¹ S*ü Ä + bE- Ô2OPE |/ß c á Õ WDM È ¹ È G ¦ G*ü1u)Ú < `+ $d1u)Ú < ´"©1u)Ú W À È¹ ž W À ï Î,XA’ Û ÍB5 Ä ü Ý o ™ ‰ ß ÈM2 G ¦ G*üPE |/ß c ¡' Ô þ ÜEÖ,XEÝ ½ È _ V È : ! ´0´ Ÿ4¡,X Ý ¹ K Ä ¹ ž âM6 6.78V Ú?U Ÿ4¡,XIRPMon ¹ K ÅFÑ S*ü ZM2 G ¦ G*üPE |/ß c Ä

M2 G ¦ G*üPE |/ß c Ô ?U,X ã ü b ÈA}*ü /ß c â Y KÈ î Z Ô/¡Eî µ • ã È J è*ü /ß c Ã ¹ Û/ PE |/ß c . Ô o ¾ Ý ü Y !6Ñ ` ä,X Ï u È_ V ÈA“KÂ2Ï4³

Windows *Y s)Ú â r)„*

0NKÈ ,X D B È ¤ o Ô/¡ „,XC¼E¯/ßEî µ È ê5ÙA“KÂ Y ¤ o,X s6Ñ Ä " ÈM2 G ¦ G*üPE |/ß c 3 Ã ¹PE |A' Û È,È y â.@ Ê ' xF' Äá K Û G ¦ G*ü6Ñ o,X.@ ÊA' Û ¡ ' Ã ¹EîE›E-/¡PE |/ß c 9 ¹ 0 Ä

E- Ô2OPE |/ß c,X Ô/¡ L _*ü"© È'EC ÊLÔ?U Y ,X s6Ñ Ê Èh*ü/ß cEîE› á u { 1u)Ú < ÄSCM Å 9]>™ ` tEQPE |/ß c È' âEîE› I/O 1u)Ú < âPE |/ß cE¯> Eî µ × ' h*ü/ß cEÔ Î Ê È V á aLÔ?UA¹PE |/ß c íEîE› SCM | Õ LEQ Ä ßM6 å ÀEîE› Windows DDK ¤ o,X Ô þ _ $/ß c IOCTL 9AÈ âE- ÔE›/ß Ä

IOCTL _ $ Ù À ø þ/ß c Öioctlapp.exe ` sioctl.sysÄ J ioctlapp.exe Ô þ Q ¸ > h*ü/ß c ÈA¹/ß c ü | Ê ]>™ ` tEQPE |/ß c È JEîE› DeviceIoControl API Ñ D å PE |/ß c ¥EÕ 4 þ á à2O _,X I/O AË" È Ú ÿ METHOD_IN_DIRECT ÃMETHOD_ OUT_DIRECTÃMETHOD_NEITHER ` METHOD_BUFFEREDÈ G bE- o I/O AË" 2O _ È–?• 6.6.38V,XAÈ â Äioctlapp/ß c ü ¥EÕ ZE- 4 þAË" ¹ â ÈLEQPE |/ß c JEÔ Î Ä

Sioctl.sys Ô þM2 G ¦ G*üPE |/ß c È W ¤ o Z ñ Ÿ ê _/ß Ã LEQ _/ß È ¹ ž 3 þ Ú ¥ _/ß ÈÚ ÿ Ø)Ú IRP_MJ_CREATEÃIRP_MJ_CLOSE` IRP_MJ_DEVICE_CONTROL Q ¸ Ä W,X ñ Ÿ ê _/ßL8 Z"¼ ` J ª,X _/ß ¹ ê È 3A×*ü IoCreateDeviceÑ D ï Î Ô þA' Û ÍB5 ÈA¹A' Û ÍB5,X á/Ä \Device\SIOCTL È5à è WE¬A×*ü IoCreateSymbolicLink Ñ D 9 ï Î Ô þ DOS A' Û á/Ä \DosDevices\IoctlTest Ä ´!8 Èioctlapp /ß c Ã ¹EîE› CreateFile Ñ D 9 ' Ô Ô þ Û å!8A' Û ÍB5,X [Ê ÍB5 È ¢5àAË" A¹A' Û ÍB5,X á u È,Ì ' bA×*ü A¹PE |/ß c,X _/ß Ä

)„ ü å À 9,ß ioctlapp /ß c V) ¡4‰ sioctl.sysPE |/ß c Ä Z S*ü SCM ,X s6Ñ È ioctlappOj A×*ü API Ñ D OpenSCManageÈ ¹ “E² y SCM È J ' Ô2Ï4³ á u D B g Ä ' âEîE› SCM ,X ¹ ß á u 9 ¡4‰ sioctl.sysÖ

- x CreateServiceÈ ï Î Ô þ Windows á u È Ú W]>™ SCM D B g Ä CreateServiceê ü HKLM\System\CurrentControlSet\ServicesßM6 ï Î Ô þ $K È $K ,X á/Ä1 à b „ Î á u,X á/Ä È+ – D 9 Û n Ä CreateServiceX – DEW î È´ W ™NO Û n „ Î á u,X á u2O _ Ã |2O _ ÃPE |/ß cCÃ X1 Ø/¡ µ C ÆE- o µ CFÑ Ú ± , ü SCM D B g Ä
- x OpenServiceÈ ' Ô Ô þ Æ]>™,X á u Ä ü – D Û n á u á/Ä `A“KÂ • ã Ä
- x StartService È | Ô þ ÆEîE› CreateServiceê OpenService' Ô,X á u Ä
- x ControlServiceÈ Û/ Ô þ á u V 0 Äpause Å Ã4»4Á Äcontinue Å Ã 0!6 Ä stopÅ ê5Ù å SCM y J(Š Õ Ä

x DeleteService È Ú Û n,X á u ¢ SCM D B g ôL8 Ä

h*ü/ß cEîE› ¹ ˜ Ä J2O _ SC_HANDLE Å 91u)Ú *ü ,X á u È ¹ ž W â SCM KÈ,XE² y Ä ' h*ü/ß c ` ä Z SCM E² y ê5Ù Ô þ á u Ê È WA×*ü CloseServiceHandle 94§ 3,Ì h,X ¹ ˜ Ä G b ¹ ÞE- o SCM API Ñ D,X*ü"© ÈAË –5×ioctlapp h*ü/ß c,X · -Õ ê5ÙWindows SDK ,X,Ì G [7 Ä

¢ sioctl.sysPE |/ß c,X?¦ z 9,ß È ' SCM ,X StartServiceá u>•A×*ü Ê ÈA¹PE |/ß c>• tEQ 2Ï4³ ÄPE |/ß c,X tEQE›/ß EîE› NtLoadDriver Ñ D È¯5à+ IopLoadDriver Ñ D 9 ` ä,X ÄPE |/ß c,X ñ Ÿ ê _/ß Ä G DriverEntry Ñ D Å ü IopLoadDriver Ñ D >•A×*ü,X È–?• 6.2.18V,X Ÿ4¡ ÈE-G á aC,EÄ ÄPE |/ß c,X LEQ _/ßÄSioctlUnloadDriver Å ü IopLoadUnloadDriverÑ D >•A×*ü,X È- ¥*ó ü ioctlapp h*ü/ß cA×*ü ControlService 9 0!6 á u Ê Ä

EîE›E-/¡ • ã ï Î,XA' Û ÍB5 J"u Ý – â 2Ï4³,XA' Û å `A' Û8V&• Ä 5à È V p ü2Ï4³ é Ð Ê+ G ¦ G*ü1u)Ú < 9 tEQ Ô þM2 G ¦ G*ü,XPE |/ß c È Fw È A¹PE |/ß c 3 î – â A' Û å Ä V p Ô þM2 G ¦ G*ü,XPE |/ß c>•]>™ 2Ï4³ È J è W,X |2O _ A'5B é Ð- | ê 2Ï4³- | È Fw È ü2Ï4³ é Ð Ê È G ¦ G*ü1u)Ú < î Ý'; G ¦ G*üPE |/ß c 9 tEQ!8PE |/ß c È J è W Î0Ÿ Ô þA' Û8V&• ¦ 9 A' Û å ÄE- oA' Û8V&•,È yL EQ ü 8V&•,X ßM6 È J PDO PE |/ß c \Driver\PnpManager ï Î,XA' Û ÍB5 Ä+ b>• tEQ,XPE |/ß cEî J þ ¤ o r tA' Û _/ß È´!8E- oA' Û8V&• ¾ Ý 4“ PE |/ß c ï Î,X PDO È5à J á , ü FDO Ä üE-/¡ ™ ‰ ß È G ¦ G*ü1u)Ú < tEQ J ñ Ÿ ê PE |/ß c È PE |/ß c J á î – â A' Û8V&• ÄE- oPE |/ß c Ã ¹ ï Î Ô þ Q á,XA' Û ÍB5 È ¢5à S h*ü/ß c Ã ¹EîE› á/Ä 9 Û n I/O AË" ,X,Â Û Ä

M2 G ¦ G*üPE |/ß c 3 Ã ¹EîE› #Ï t.@ Ê å Ð 9]>™ È üE-/¡ ™ ‰ ß.inf [Ê ™LÔ,X Ä G ¦ G*ü1u)Ú < î ï Î Ô þA' Û8V&• È J ï Î PDO È J tEQE›/ß2O b é Ð Ê tEQM2 G ¦ G*üPE |/ß c,X ™ 6 ÈE-G á aC,EÄ Ä

Ô â1T) ã4§ Ô ß ¹ Þ G bWindows A' ÛPE |/ß c,XA|AŽ Ä Bü ÞA† È Windows¸XA' ÛPE |/ß c Ô þ | ÕJÒ y g È W,X 9 ·&• ñ Ÿ ê _/ß È I/O2Ï4³ ?U" ,X J ª _/ßFÑ ü ñ Ÿ ê _/ß Û n,X Ä ü 8V È å ÀEîE› toaster_ $A|AŽ Z.@ ÊA' Û,XA' Û Ü V) X ÎCK 9,X È¹ žE›$¸PE |/ß c V) – â J Ä 5à È 8V J"u Ý Ÿ4¡PE |/ß c hA¹ V) ¡ h Ø/¡I/O AË" Ä G b V)4ê mPE |/ß c,X _/ß 9 ¡ hI/O AË" ÈAËAÏ5Ù –5¥Windows DDK,X [7AÈ â È ê5ÙWalter Oney,X:+ 0 [WALTER] Ä º ê È Windows DDK¤ o,X ,X _ $)/ Z Ø/¡2O _,X.@ ÊA' Û,XPE |/ß c h V) r)„ Ä

Windows *Y s)Ú â r)„*