汇编怎么取命令行参数

PSP(Program Segment Prefix)(程序段前缀)

汇编语言命令参数

一、 引言：

如果大家用过 TurboC2.0/3.0 or BorlandC3.X 等编译器编写 DOS 应用程序的李明博话，编写一个命令行参数形式的应用程序对大家来说是一件非常容易的事情，只要在主函 main()中加几个参数就 OK（int main(int argc,char *argv[],char *env[]){}）。相对汇编语言来说编写一个命令行参数基金鸿飞的程序就比较艰难，它要用到 DOS 的程序段前缀 PSP（Program Segment Prefix）知识以及其他相关 DOS 知识。（本文只对参数介绍，环境块不作讨论）

二、相关知识：

在 DOS 的科伦药业提示符下键入一个命令（内/外部命令）或程序的名字,DOS SHELL（COMMAND.COM）首先根据名字判别其是内部命令还是外部命令或用户程序，若是内部命令则调用 COMMAND.COM 暂驻在内存中的部分音乐现场的 DOS 内部命令代码，若是外部命令或用户程序，DOS SHELL 则在当前目录和搜索路径中搜索匹配的文件名，找到了沃尔沃 s80就加载程序，加载出错显示错误信息，找不到则显示 Bad command or file name。

用户载 DOS 提示符下输入一串字符串，DOS SHELL 把以回车 0Dh）为结束的这以字符串作为一个命令和参数进行解释，第一个空格以

前的字符串为命令名（必须符合 DOS 命名规则），第一个空格（包括空格）到回车之间蔡依珊的字符作为命令或程序的参数。

程序段前缀--PSP 是 DOS 加载一个外部命令或用户程序（扩展名为 COM or EXE）时，在程序段前设置一个以节为边界，固定长度为10H（即256字节，一节为16字节）的黄智博存储块，PSP 和程序段共有一个内存控制块（MCB），PSP 位于每个程序的开始部分，无论是 COM 还是 EXE，PSP 的数据结构是相同老罗英语培训的。PSP 是程序与 DOS 的接口，DOS 利用 PSP 管理进程，DOS 用户进程指的决战是一
个已被装入内存的可执行程序或已被调入内存但未执行的程序，COMMAND.COM 是一个最早被装入内存 PSP 的程序，因而可被看作祖先
进程，外部命令或用户程序作为子进程，被 DOS 通过 INT 21H 的李明博4BH 号子功能来加载。用户程序也可以通过 INT 21H 的4BH 号子功能调用来加载自己基金鸿飞的子进程，控制子进程的执行，并通过科伦药业4DH 号子功能调用获取子进程的运行状况。

PSP 中存有许多关于程序启动、执行、结束以及进程调度、进程环境地址和进程标志等重要信息。程序利用 PSP 还可以控制父子进程间音乐现场的通信。至于 PSP 的数据结构的沃尔沃 s80详细内容请参考有关书籍，本文不详细给出。

DOS 加载一个 COM 或 EXE 程序时，段寄存器 DS，ES 都指向 PSP 段址（PSP 段址是进程的唯一标志符），而不是指向程序的数据段和附

加

段。COM 文件蔡依珊的 CS，SS 也指向 PSP 的段址。EXE 文件的黄智博 CS，SS，IP 和 SP 需要进行重定位。

DOS 加载一个外部命令或用户程序时，把文件名之后到回车符之间的字符串，最多可达127个字符作为参数，并把这些字符串送到 PSP 位移81H 开始的区域，位移80H 老罗英语培训的一个字节存放参数字符串长度（回车符不算在内）。大家可用 DEBUG.EXE 加载一个带参数的程序，然后用 D DS：80子命令查看加载程序的决战参数。命令行参数一般以空格（20H）为开始，回车符（0DH）为结束，但命令行中的重定向，管道符以及有关信息不作为参数传递给 PSP。

程序段前缀(Program Segment Prefix)在内存是定位于程序前的、以节为边界 PSP 的、一个256(100h)字节大小的区域,它是程序与 MS-DOS 的李明博接口。在 MS-DOS 操作系统中,PSP 实际上起着进程控制块(PCB)的作用。程序段前缀这一概念是由 CP/M 操作系统引入 MS-DOS 基金鸿飞的,但是随着 MS-DOS 的科伦药业发展,PSP 远远超过了 CP/M 中所确定的音乐现场含义。它已包括了许多别的操作系统(如 Multics 和 UNIX)沃尔沃 s80的概念,如堆栈框架、进程目录等。正确地使用 PSP 中的蔡依珊信息,一个进程可以向其子进程传送重要的控制信息,也可向其父进程返回信息。PSP(程序段前缀)字域意义简表偏移 (十六进制)类型内容00--01指令程序结束(Program terminate)此二字节总为 CD20,即 INT 20h 的指令代码02--03字内存顶部(Top of memory)程序内存空间顶部位置黄智博的段址,对于低端有640KB RAM 的机器

,此域值常是 A000h04字节保留(总为00h)05--09指令与 CP/M 兼容的老罗英语培训系统调用入口(CP/M-like service call)此域第一字节是 CALL 指令的操作码9Ah;后两个字分别是段内偏移量和段地址,它们形成决战的过程入口物理地址为0000C0h。而在中断向量表 PSP 的 000C0--000C5的5字节域中,存放的李明博不是30h 号中断向量,而是一条转至 INT21h 例程入口之一的一条远转移指令。于是若程序发出对 PSP+05h 的近调用就可实现对 INT 21h 基金鸿飞的调用。这是 MS-DOS 为与 CP/M 兼容而保留下来的一种系统调用方式。0A--0D 双字程

序结束地科伦药业址(Terminate address)运行结束时程序接受控制的缺省地址。即返回父进程时,父进程继续运行音乐现场的地址0E--11 双字 Ctrl-Break 出口(Ctrl-Breakexit)Ctrl-Break 键(或 Ctrl-C 键)按下而中止程序运行时,程序接受控制的缺省沃尔沃 s80地址,即父进程 INT 23h 例程的入口12--15双字严重错误出口(Critical error exit)程序运行出现严重错误时,程序接受控制的蔡依珊缺省地址,即父进程 INT 24h 例程入口16--17字父进程的 PSP(PSP of parent)此域存放父进程程序段前缀黄智博的段址,即父进程的进程标识(PID)18--2B 字节表进程文件句柄表(File handle alias table)此20字节域常称为任务文件表(JFT),每个字节为一个表项,表项的老罗英语培训序号即是句柄号,表项的内容为此打开文件的系统文件表(SFT)表项序号2C--2D 字环境块决战地址(Environment address)此域存放进程环境块的段地 PSP2E--31双字进程

堆栈指针(Stack pointer)每当程序发出 DOS 系统功能调用时,INT 21h 例程把已压入 FLAGS、返回地址和 AX--ES9个寄存器内容后的用户堆栈李明博的指针 SS:SP 的值保存在此域中。这是 MS-DOS 操作系统打算通过基金鸿飞切换“当前 PSP”,终止一个进程后再恢复另一进程运行所做的准备。但是 MS-DOS 仍不支持并发进程。实现有条件的 DOS 重入,使用科伦药业的是 DOS 内部的保存用户堆栈指针的音乐现场“当前栈帧指针”单元,它的作用仅限于恢复父进程堆栈32--33字进程文件句柄表大小(Size of the handle alias table)缺省值为0014h(20),可重新设置34--37双字进程文件句柄表地址(Address of the handle alias table)缺省值为本 PSP 段址:0018h,可重新设置38--3B 双字共享前沃尔沃 s80的 PSP(SHARE'Sprevious PSP)在 MS-DOS3.3版之前,此双字域为-1:-1,后来的版本下每当使用 SHARE.EXE 共享程序时,此双字域被设置成指向父进程 PSP 的蔡依珊指针3C--4F 此20字节保留未用(DOS5.0下,40--40h 处的1个字登记有程序所需的最低 DOS 版本号,缺省值是

5.0)50--52指令与 UNIX 兼容黄智博的系统调用发送器(UNIX-Like dispatcher)此三字节为 CD,21,CB,即 INT 21h 和 RET 两条指令的代码。程

序可把此域看成一个函数,通过老罗英语培训函数调用来实现 DOS 系统调用,这是与 UNIX 兼容的系统调用方式53--5Bx 此9字节保留未用5C --6B 文件控制块1(File Control Block1)6C--7B 文件控制块2(File Control Block2)这两个格式化的但未打开决战的 FCB,分别用于装载此

程序

时命令行中(程序名之后)的第一、二个文件名参数,当 FCB1打开时可能将 FCB2覆盖7C--7F 保留80--FF 命令尾部,或磁盘传输区(Command tail,DAT)当在系统提示符下,以命令行加载此程序(程序名视作外部命令名)时,COMMAND.COM 将命令行中跟随程序名之后的 PSP 参数字符串(以回车符 CR 为结束符)存于此128B 域中,以供程序运行时分析使用,此域第一字节为参数字符串的字节长度(不包括 CR),从第二字节开始是参数字符串的原样拷贝。当程序运行时以 FCB 方式进行文件操作时,此域是缺省李明博的磁盘传输区(DTA),除非事先调用1Ah 号系统功能另行指定一个 DTA 下面以“PSP 是程序与 MS-DOS 的接口”的基金鸿飞观点将其主要作用概括为以下四个方面:

1.PSP 段址是进程的标识符

MS-DOS 操作系统的用户进程实体由三部分组成:程序段前缀 PSP、环境块和程序(代码、数据堆栈)。PSP 和程序共占一个内存分配块,而环境块为另一个内存分配块,但这两个内存分配块科伦药业的 MCB 中“拥有者”字段都是程序 PSP 的段址。因此,称程序 PSP 段址为进程的音乐现场标识(PID)。这样说不仅是因为若系统中同时有多个程序驻留于内存的话,其 PSP 段址必不相同,因而以它作为 PID 具有其唯一性。更重要的是,PSP 把进程实体沃尔沃 s80的三部分联系在一起了。PSP 之后即是程序的蔡依珊内存起始位置(对于.COM 文件,此 PSP 段:0100h 还是程

序的启动点)。程序的内存高端位置由 PSP+02h 黄智博的字域给出,而

且若程序以31h 号系统功能调用或 INT 27h 中断调用来结束并驻留的话,则将以驻留部分高端地老罗英语培训址(以 B 为单位)来修改 PSP+02h 的字域值。因此,将 PSP+02h 的字域值减去 PSP 段址,再减去100h,即为

程序空间决战的大小(B)。至于程序的环境块,则由 PSP+2Ch 字域明确组出其段址,程序访问环境块将极度其方便。

2.为进程使用系统资源提供支持这主要体现在由 PSP+18h 处开始的 PSP20B 的进程文件句柄表,又称之为任务文件打开表(JFT)。若表项内容

不为-1(FFh),则它代表一个打开的文件,其表项序号就是文件句柄(文件句柄是一个16位二进制数李明博的数字)。通过 JFT 表项内容取得基金鸿飞与系统文件打开表(SFT)的联系,从而实现对指定文件的访问。当父进程以 EXEC 系统功能建立子进程时,子进程全部继承父进程已用句柄方式打开科伦药业的非特权文件。此后子进程可以打开新的文件,若 PSP+18h 处开始的音乐现场20个表项使用完的话,则进程可以另建一个

JFT,将新建 JFT 的地沃尔沃 s80址和大小分别置入 PSP+34h 双字域和 PSP+32h 字域中,并将 PSP+18h 的20B 内容拷贝到新建 JFT 的前部,进程

就可使用新 JFT 蔡依珊了。注意,新建 JFT 的功能只是在 DOS 3.X 及其更高版本中的黄智博 PSP 才具备的。JFT 的前5个表项,即0--4号句柄总是

分配给老罗英语培训了标准输入、标准输出、标准错误(输出)、标准辅助、标准列表等五个标准设备文件。这是 DOS 打开的,并初始设置了决战 COMMAND.COM 的 PSP 中的 JFTPSP 的前 5 个表项。COMMAND.COM 程序是一切用户进程的祖先,于是5个打开的李明博标准设备文
件将所有用户进程所继承。各用户进程可通过各自的 JFT,以句柄方式实现对标准设备(键盘、显示器、串行通信口、并行打印机)基金鸿飞的 I/O 操作。

3.接纳父进程传递过来的科伦药业命令行参数父进程建立一个子进程总是要求子进程为它完成某一件具体任务。为此,父进程往往需要向子进程提供一些命令参数。进程 PSP 的后128B 域就是用来接纳这些参数,以供进程分析使用的。PSP(程序段前缀)字域意义简表中音乐现场的 PSP+80--FFh 域注释是按 COMMAND.COM 作为父进程来加载用户程序(作为子进程)的情况来说明的沃尔沃 s80,这是最普遍的情况。有经验的用户都有这样蔡依珊的体会,通过使用 PSP+80h 处开始的黄智博命令行参数,可使我们编制的程序更灵活,功能更丰富。实际上,任何一个父进程都可使用 EXEC 系统功能建立子进程并向它传递命令参数。父进程还可向子进程传递两个未打开的格式化老罗英语培训的文件控制块(FCB),这也将容纳在 PSP 中供进程分析使用。但是,随着 DOS 的决战发展,越来越普遍采用句柄文件操作而不愿使用 FCB 方式,PSP 中的 FCB1和
FCB2两个区域已不太重要了。

4.保存父进程现场以便返回父进程

父进程建立一个子进程并把系统控制权交给子进程。那么,子进程运行结束后也应把系统控制权还回父进程,使父进程由调用 EXEC 系统功能 PSP 的下一条指令继续运行。父、子进程串行运行是 MS-DOS 单任务操作系统的特征。在 MS-DOS 中,绝不会出现 UNIX 中的李明博用 fork()创建子进程后,父、子进程并发运行的情况。那么需要保护父进程的哪些现场信息呢?子进程基金鸿飞的 PSP 中又是如何保存这些信息呢?

(1)首先要保护的是返回地科伦药业址,即父进程调用 EXEC 系统功能(INT 21h)时的下一条指令的地音乐现场址。这由 EXEC 系统功能将返回地

址保存在所建进程的 PSP+0Ah 沃尔沃 s80的双字域中(即程序结束地址域)。程序结束时,将以它恢复中断向量表的蔡依珊 INT 22h 向量,最终以此向量设置 CS:IP 而正确返回父进程。不要破坏或重新设置 PSP+0Ah 双子域的值,除非你不算让程序结束后返回父进程。程序中也绝不要

以 INT 22h 中断调用指令来返回父进程。因为,在返回之前还有不少现场信息需要恢复,另外系统中也无专门的 INT 22h 中断例程,INT 22h 中

断向量只是作为存放返回黄智博地址的双字变量被使用。

(2)应该保护父进程的老罗英语培训 Ctrl-Break(Ctrl-C)中止处理程序的入口地址和严重错误处理程序决战的入口地址。这是因为子进程可能修改 INT 23h 和 INT 24h 中断向量,使之指向自己的 PSP 中止处理程序

入口和严重错误处理程序入口。保护工作由 EXEC 系统功能完成,它把(发

出此系统调用时的)中断向量表中的 INT 23h,INT 24h 李明博的两个中断向量的值复制到所建进程 PSP+0Eh 双字域和 PSP+12h 双字域中。进程结束时,也是使用 PSP 中这两个字域中的基金鸿飞值来恢复中断向量表中的 INT 23h,INT24h 两个中断向量。程序中可以修改或不修改中断向量表中的这两个中断向量。如果不修改,则程序中止处理和严重错误处理是由父进程科伦药业的 INT 23h 中断例程和 INT 24h 中断例程来完成的。此种情况是子进程继承了音乐现场父进程的两个软件资源。继承也罢,不继承也罢,都不要企图去更改 PSP+0Eh 双字域或

PSP+12h 双字域中的内容!

(3)应该保护父进程已打开沃尔沃 s80的文件。前已说明 EXEC 系统功能通过把父进程 PSP 中的蔡依珊 JFT 拷贝到所建进程 PSP 中的 JFT,而使子

进程继承了父进程全部已打开黄智博的句柄式文件(但特权打开的除外)。并且拷贝之后已把系统文件表(SFT)中这些已打开文件的老罗英语培训控制块内的“文件引用计数”增1。子进程可以关闭自己所打开的文件,当它试图关闭所继承决战的打开文件时,只是把 SFT 中的“文件

引用计数”减1,而不能真正关闭这些父进程已打开的 PSP 文件,也就是说,DOS 的文件管理机制已使父进程所打开的文件妥善李明博得到了保护。

(4)保护父进程的基金鸿飞 PSP 段址。前已说明 PSP 段址是进程的唯一

标识,DOS 只支持进程的串行执行。因此,DOS 维护科伦药业着一个系统

“当前 PSP”字单元,它应保存着当前正在运行进程的音乐现场 PSP 段址,DOS 有关内存分配、文件操作的系统功能都是针对“当前 PSP”而言的。父进程调用 EXEC 系统功能建立沃尔沃 s80了进程并使它投入运行时,EXEC 系统功能就先把系统“当前 PSP”的内容,即父进程 PSP 段址写入所建进程 PSP+16h 的蔡依珊字域中予以保存;然后将所建进程 PSP 段址写入系统“当前 PSP”中。于是,子进程成为系统当前进程,可使用一切系统资源。当使用 DOS 的有关系统功能调用或中断调用来结束一个程序的运行时,DOS 都要从运行程序 PSP 中取出所保存黄智博的父

进程 PSP 段址,并将其写入系统“当前 PSP”中。于是子进程运行结束后,父进程成为系统当前进程。由于 PSP+16h 字域中保存了父进程 PSP 段址,使得老罗英语培训父、子进程有条不紊地交接系统资源使用权(系统“当前 PSP”),这一切都这么顺理成章。但有一点需引起注意,即当程序结束并驻留时,一样地把父进程段址恢复为系统“当前 PSP”;而当驻留部分以某种中断驱动被激活而运行时,此时系统“当前 PSP”并不是被激活进程决战的 PSP 段址。有时,需要被激活进程自己去保护和更改系统“当前 PSP”内容。

(5)保护父进程的堆栈指针,以便返回父进程时恢复进程中断前的 PSP 现场。前已说明,每当进程中发出一个系统功能调用,由 INT 21h 中断例程对在中断响应时已压入了标志寄存器 FLAGS 的内容、返回李明博地址

双字的进程堆栈上,又继续压入 AX--ES 9个寄存器的基金鸿飞内容,然后将此进程堆栈的栈指针 SS:SP 保存在该进程 PSP+2Eh 的双字域中。

那么,当父进程发出 EXEC 系统功能调用时,同样科伦药业的情形发生在父进程的堆栈中;而且父进程堆栈指针同样保存在父进程 PSP+2Eh 的音

乐现场双字域中。此后,所建立的子进程投入运行,使用的是子进程自己沃尔沃 s80的堆栈;父进程的堆栈“凝固”不变,父进程堆栈指针被“

封存”在父进程的蔡依珊 PSP 中。于是,子进程结束时,只要先由子进程 PSP+16h 字域中得到父进程 PSP 段址,那么就不难找到父进程的 PSP,再从父进程 PSP 中取出父进程堆栈指针,以它恢复父进程堆栈和恢复父进程现场信息就易如反掌黄智博了。DOS 实施进程结束处理的系统功能或中断功能就是这么做的老罗英语培训。