

## Re: Kernel malloc/realloc?

**Source:**

<http://www.tech-archive.net/Archive/Development/microsoft.public.development.device.drivers/2004-02/0786.html>

---

**From:** David J. Craig (*SeniorDriversWriter\_at\_shogunyoshimuni.com.net*)

**Date:** 02/15/04

Date: Sat, 14 Feb 2004 22:36:09 -0500

No, stupid is calling functions belonging to Win32, 'SYSTEM'. Windows NT has a kernel that has several possible environments above it and one of them is Win32. There is or was a POSIX environment. They also had a OS/2 environment at one time because the OS/2 Brief would run under NT4. The use of the GlobalAlloc function is not even recommended since the overhead is high. So how does a function in kernel32.dll even belong in the 'Development Device Drivers' newsgroup? The first question was about allocating and reallocating memory under Windows 2000+.

"Alex" <AIX@a> wrote in message  
news:Oi8rNa28DHA.488@TK2MSFTNGP12.phx.gbl...  
> *Do you even know the difference between a RTL function and a System API  
> function?*  
>  
> *As it's been sed before, pointing to RTL source code to understand how  
> \*\*SYSTEM\*\* APIs work is stupid.*  
>  
> *Sorry, if it's offensive, but this is what it is*  
>  
> *MSDN Library April 2003:*  
> *GlobalAlloc:*  
> *GMEM\_MOVEABLE:*  
> *"Allocates movable memory. Memory blocks are never moved in physical  
memory,  
> but they can be moved within the default heap."*  
>  
> *\*\*"never moved in physical memory"\*\**  
>  
>  
> *"Tim Roberts" <timr@probo.com> wrote in message  
> news:9c9r20dgm2d1drglccnmf30g73lj87r2u4@4ax.com...*  
>> *"Alex" <AIX@a> wrote:*  
>>>  
>>> *"Tim Roberts" <timr@probo.com> wrote:*  
>>>  
>>>> *"Alex" <AIX@a> wrote:*  
>>>>>

> > > > "Tim Roberts" <timr@probo.com> wrote:  
> > > >  
> > > > Isn't the same algorithm behing the user mode reallocation (not  
> > > necessarily  
> > > > realloc, i'm shure this thread has nothing to do with the  
actual  
> > > > realloc  
> > > > >function :P) which we all use in user mode apps?  
> > > >  
> > > > No. Both relloc in the C run-time library and  
> > > > LocalRealloc/GlobalRealloc  
> > > > use the new/copy/free model.  
> > > >  
> > > > Is that a fact? Or a beleif?  
> > > >  
> > > > The source code for Microsoft's C run-time library is included with  
Visual  
> > > > C++. You can look it up. If there's empty space following the  
block, it  
> > > > just expands the block. Otherwise, it's new/copy/free.  
> > > >  
> > > > Think about it for a bit. Your page table magic will ONLY work if  
all  
> > > > heap  
> > > > allocations are done in units of whole pages. As soon as you have  
two  
> > > > objects in the same page, you can't alter the mapping without  
screwing up  
> > > > the other objects in the page. The C run-time malloc and the Win32  
heap  
> > > > alloc work in units of 32 bytes.  
> > > >  
> > > > in order to save page space. So, 80000000 has the DOS interrupt  
> > > > vectors  
> > > > from physical address 0, 800C0000 has the VGA BIOS at physical  
address  
> > > > C0000, and so on.  
> > > >  
> > > > This mapping is documented behaviour? For what OS-es is it used?  
> > > >  
> > > > I've never seen it documented by Microsoft, but it's fact, and  
operating  
> > > > system routines rely on it. I know it's true for the NT-based  
systems  
> > > > (NT/2K/XP). It used to be true on Windows 3.1. I do not remember  
about  
> > > > 95/98.  
> > > > --  
> > > > - Tim Roberts, timr@probo.com  
> > > > Providenza & Boekelheide, Inc  
> > > >  
> > > >

microsoft.public.development.device.drivers: Re: Kernel malloc/realloc?

>