NULL 描述符

选自：Dr.Dobb’s Microprocessor Resource：THE NULLDESCRIPTOR

翻译：coly li

全局描述符表（GDT: Globale Descriptor Table）的第一项称为 null 描述符。NULL 描述符在 GDT 中是唯一的，它的 T1=0，INDEX=0。大多数公开的文档都声明这个描述符表项应当为 0。Intel 在这个话题上一直很态度暧昧，从没有说他不能做何用途。并且 Intel 还声明这个描述符表项永远不会被处理器引用。

既然处理器从来不会引用 NULL 描述符，那么这就意味着存储在这个位置的数据可以用来做任何事情。我的爱好是用 NULL 描述符指向 LDT 本身。将 NULL 描述符这么使用是非常明智的。LGDT 指令需要一个 6 字节的指针指向 GDT，而 NULL 描述符有 8 个字节并且不会被 CPU 访问——因此 NULL 是一个作为指向 LDGT 的指针的一个非常明智的选择。（这是比较可信的方法，我已经使用了近 10 年了）

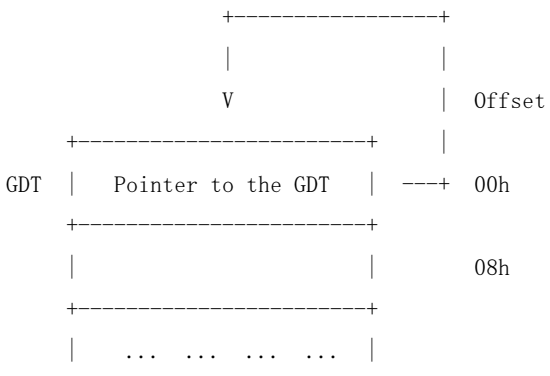
对 GDT 编址的一般协议如下：

```
GDT_PTR   DW   GDT_LENGTH-1
          DD   PHYSICAL_GDT_ADDRESS
```

然后在代码段：

```
LGDT      GDT_PTR
```

使用 NULL 描述符作为指向 GDT 的一个指针，简化数据段，概念图如下：



然后在代码段：

```
LGDT      GDT
```

由于 NULL 描述符取代了 GDT_PTR，GDT_PTR 变量不再需要了。

在这里使用 NULL 描述符来提供一种对 GDT 寻址的很干净的方法。

这种技术可以在我的任何使用模式模式的汇编语言源代码中看到。例如 INT09.ASM。

可在下列地方看到我的示例源代码：

ftp://ftp.x86.org/pub/x86/source/int09/int09.asm

ftp://ftp.x86.org/pub/x86/source/386load/macros.386

在下列地址可以获取所用的源代码：

http://www.x86.org/ftp/dloads/int09.zip