A20/RESET 的异常

原稿：来自 Dr.Dobb’s：A20/RESET ANOMALIES

翻译：coly li

IBM 通过在键盘控制器的输出上增加了一个 CPU A20 信号来实现在 8088 上的 memory wrap 特性。这两个信号（哪两个信号？是指 memory wrap 和 CPU A20 吗？）都必须在真实的 A20 到达总线之前被激活。当键盘控制器被适当的编程之后，他的输出总是低电平的。这就限制了 CPU A20（这个东东是高电平）并不总是能够出现在地址总线上的。通过 CPU A20 信号就模拟了 8088 所具有的 memory wrap 特性。当键盘控制器被编程为允许在地址总线上传输 CPU A20 信号时，所有当前的地址线都没有别的副作用。当编程为关闭 A20 的时候，没有人会考虑到这会有什么副作用——但是副作用是存在的。

（colyli 对此问题的补充：8088 是 20 位地址总线，具有 20 根地址线，可寻址 1MB 地址空间。8088 有一个特性，叫做 memory wrap，就是当你访问大于 1MB 的空间的时候，实际上访问的是这个地址模 1MB 之后的地址，例如访问 0x10ffff，实际上访问的是 0x00ffff。这种技术在 8088 上被广泛使用，以至于到了 80186 仍然使用。但是在 IBM PC-AT 架构中开始使用具有 24 位地址总线的 20286，这时候，很有可能原先按照 20 根地址线并使用 memory wrap 功能的程序就无法正确执行了。所以就引入了第 21 根地址线——A20 的概念，即当运行使用 memroy wrap 特性的程序时，需要将 A20disable，这样的效果就是对软件来说只有

20 根地址线。当运行 80286 程序时，就将 A20 enable，这样就可以使用全部的 24 根地址线访问 16MB 内存空间）

由于 CPU A20 是唯一的被设置为门（gate）的地址线（也就是说有时会 disable，有时会 enable），所以任何对奇数 MB 区域（1M-2M，3M-4M）的扩展内存的内存访问都会受到限制（当 CPU A20 被 disable 的时候）。当然在任何状态下程序员总是可以访问每一个偶数 MB 的内存范围(0M—1M，2M—3M)的。

有一种非常罕见的情况会导致系统崩溃，即当 CPU A20 被地址总线限制的时候，一个 RESET 发生了。由于 reset 后 CPU 会从内存的顶部（不是 F000:FFF0）开始执行代码（这里应该是 BIOS 代码吧？），而这个时候 CPU A20 是被 disable 的，这个时候就会导致系统崩溃，为什么呢？要考虑 CPU A20。在 286 上，内存的顶端是 FFFFF0h，在 386 或以后 x86 上是 FFFFFFF0h。如果 CPU A20 被关闭了，那么 RESET 信号将会导致 cpu 从内存的 EFFFF0h（286 机器上），或者 FFEFFFF0h（386 或更新的 x86）上开始执行。除非这段内存被通过硬件映射到内存顶端，否则计算机就会崩溃——因为他将会试着执行这些地址上的任何内容。