

A20 地址线问题全面解析

2013年12月24日

1、先看看 real mode 的寻址方法

8086/8088 的地址线有 20 条：A0 ~ A19，意味着 processor 可以将 20 位地址放上这 20 条地址线上，它的寻址能力是 1M (00000 ~ FFFFF)，它的寻址方法是：**segment:offset**，这是一种被称为 **logic address**（逻辑地址）表示法，它需要转化为 processor 的 linear address（线性地址）表示：

$$\text{segment:offset} \text{ -----} > \text{segment} << 4 + \text{offset}$$

如：**F000:FFFF = F0000 + FFFF = FFFFF**，这是 8086/8088 所能访问的最高地址。这种表示方法是 Intel 为了在 16 位 real mode 下能够访问 20 位地址空间所想设计出来的计算方式。

因此，8086/8088 的寻址范围是可以表示为：从 **0000:0000 ~ 0000:FFFF** 开始到 **F000:0000 ~ F000:FFFF**

2、访问 extended memory

在后续的 80286 上，Intel 实现了 24 位的 Address bus，那么在 real mode 下 80286 能够访问到的最高地址是 10FFEF，这个地址值是由下面的方法而来：

$$\text{FFFF:FFFF} = \text{FFFF0} + \text{FFFF} = 10\text{FFEFh}$$

这已经是 logic address 所能表达的极限范围了。100000h 以上的内存被称为 extend memory，从 100000h ~ 10FFEFh 这片内存区域在 DOS 下被称为 High Memory（高端内存）。高端内存是 80286 在 real mode 所能访问到的区域，而 8086/8088 所不能访问到的。

3、wraparound 现象

当在 8086/8088 下执行 **FFFF:FFFF** 这个内存寻址时，会产生什么结果呢？

				19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
0	0	0	1	0	0	0	0	1	1	1	1	1	1	1	1	1	1	1	0	1	1	1	1

结果很明显：由于 8086/8088 只有 20 条 address bus，地址 10FFEF 的高 4 位会被抛弃，实际上送上 address bus 的只有 **0FFEFh** 值，所以访问 **FFFF:FFFF** 地址结果只能访问到 1M 以内的地址。这就是 wraparound 现象：访问 1M 以上地址都会回绕到 1M 内的模值。

那么，当 80286 下访问 **FFFF:FFFF** 地址时，又会产生什么果呢？由于 80286 具有 24 条 address bus，对于 **FFFF:FFFF** 地址的访问，会正确得到访问。

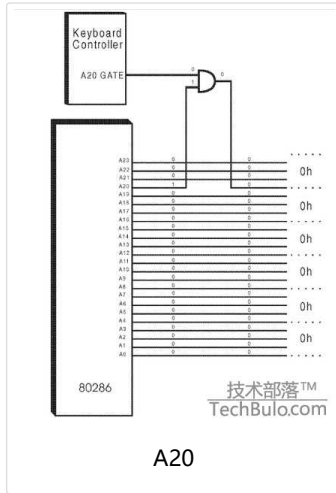
SO，访问 **FFFF:FFFF** 内存，使得 8086/8088 下产生 wraparound 现象，变相访问 **0FFEF** 地址内存。而在 80286 下得到正确的 **10FFEF** 地址，不存在 wraparound 现象。因此：wraparound 现象在 8086/8088 才会产生。这样产生的问题是：**访问高端内存时，80286 在 real mode 下和 8086/8088 的行为不一致！**

4、引入 A20 Gate

为了使用 80286 和 8086/8088 在 real mode 下的行为一致，即：**在 80286 下也产生 wraparound 现象**。IBM 想出了古怪方法：**当 80286 运行在 real mode 时，将 A20 地址线（第 21 条 address bus）置为 0**，这样使得 80286 在 real mode 下第 21 条 address line 无效，从而人为造成了 wraparound 现象。

具体实现方法是：

设立一个 AND Gate (与门电路), AND gate 的 IN 输入端中一端接 A20 line 上, 另一端接在 keyboard control 8042 上, 而 AND gate 的 OUT 输出端接在 A20 line 上。只有两个 IN 端都为 1 时, OUT 端才为 1



A20 line 一直处于 1 状态 (High 电平), 而 8042 内的 A20 gate 一直处于 0 (Low 电平), 因此: 必须使 Keyboard controller 8042 内的 A20 Gate 处于 high 时, A20 line 输出才有效。A20 gate 也被称为 A20 MASK#。

SO, Keyboard Controller 8042 增加了一组命令去控制 A20 Gate 的开/关, 给 8042 发送命令 0xDF 置 A20 gate 有效, 给 8042 送命令 0xDD 置 A20 gate 无效。

现在的 system 中，南桥芯片的 A20 MASK# 缺省都是 MASK 状态，即：A20 gate 缺省都是开的。

5 、打开 A20 gate

在 OS 的 boot 阶段一般都要做打开 A20 gate 操作, 虽然现在 A20 gate 缺省为开的。

打开 A20 gate 的方法最原始的是给 keyboard controller 8042 发送 A20 gate enable 命令字，就是上面所说的 0xDF 命令。

6、打开 A20 gate 的必要性

打开 A20 gate 是为了在 80286/286+ 以后的 processor 上使用 protected mode 来访问完全的 24/24+ 位地址空间, 如: 在 32 位 protected mode 下, 在不打开 A20 gate 的情况下, Bit20 为 0, 导致 Bit20 留下一个空位。

[illegible]

作者: [techbulo](#)

- 该日志由 techbulo 于4年前发表在[基础知识](#)分类下，最后更新于 2013年12月24日。
- 转载请注明: [A20 地址线问题全面解析 | 技术部落](#) + [复制链接](#)