Re: 问关于A20开关的问题!

Windows内核调试

问关于A20开关的问题!

井底之蛙 2009-05-15, 11:49 上午
请问现在的32位PC机(P4等的),A20开关在CPU执行第一条指令时(BIOS里的第一条指令)是禁止的(=0)还是开启的(=1)?
还有,请问A20开关是只控制第21根地址线,还是同时控制了第21根至第32根的所有地址线?

有人说A20默认是开启的, 因为Intel手册上说CPU第一条指令在0xFFFFFFF0, BIOS初始化结束时把它关闭的 !

第二个问题在网上也有不同的回答, 纳闷……

Re: 问关于A20开关的问题!

王宇 2009-05-15, 14:12 下午

我来抛砖引玉。

Intel 8088 芯片具有 20 位地址总线, 2^20 寻址能力达到 1MB。也就是说, 8088 最大的寻址能力是 FFFF:FFFF, 计算一下:FFFF0 + FFFF = 10FFEF 这实际已经越界了… 所以, 8088 芯片有一个特性叫 Memory Wraparound, 大概意思就是“模 1MB”, 例如访问 0x10FFEF 实际上访问的是 0x00FFEF。这种技术融合为寻找的一部分。

之后, IBM PC-AT 架构开始采用 Intel 80286 芯片, 翻翻资料就会发现:现在的32位 GDT 数据结构都有兼容 80286 的影子 —— 那可恶的位计算 / 拼接啊… 80286 GDT 的 BASE 是 24 位, 2^24 寻址能力达到 16MB。好的, 问题来了, 如何向下兼容? —— 原先按照20位地址线并且使用 Memory Wraparound 功能的程序会寻址出错。IBM 给出的解决方案 (注意是 IBM) 是 A20 地址线, 就像一个小开关, 当运行使用 Memory Wraparound 特性的程序时, 需要将 A20 Disable;当运行 80286 程序时, 就将 A20 Enable (高电平), 此时就可以使用全部的 24根地址线访问内存了。因为那时 Intel 8042 键盘控制器芯片 (键盘端的芯片叫8048、PC 端的芯片叫8042, 键盘端8048检测到矩阵状态变化时产生扫描码2,

传输到PC端后8042又会转码成扫描码1，这是键盘原理）还有多余的针脚，就用了一个针当这个“与门开关”。

在系统启动的时候，A20 地址线是低电平，所以，32位操作系统必须打开它。我所知道的打开方式大于3种：
(1) 操作 i8042
The output port of the keyboard controller has a number of functions.
Bit 0 is used to reset the CPU (go to real mode) – a reset happens when bit 0 is 0.
Bit 1 is used to control A20 – it is enabled when bit 1 is 1, disabled when bit 1 is 0.

(2) 操作 System Control Port A，这种最常见。
MCA, EISA and other systems can also control A20 via port 0x92.
Bits 0,1,3,6,7 seem to have the same meaning everywhere this port is implemented.
Bit 0 (w): writing 1 to this bit causes a fast reset (used to switch back to real mode; for MCA this took 13.4 ms).
Bit 1 (rw): 0: disable A20, 1: enable A20.
Bit 3 (rw?): 0/1: power-on password bytes (stored in CMOS bytes 0x38-0x3f or 0x36-0x3f) accessible/inaccessible. This bit can be written to only when it is 0.
Bits 6-7 (rw): 00: hard disk activity LED off, 01,10,11: hard disk activity LED on.
Bits 2,4,5 are unused or have varying meanings. (On MCA bit 4 (r): 1: watchdog timeout occurred.)

(3) BIOS INT 0x15 AX : 240?
这个在 CMU 计算机系台柱 Ralf Brown 泰斗的 Interrupt List 里有详细的介绍 —— “INT 15 2400 - SYSTEM - later PS/2s - DISABLE A20 GATE”

(4) AMI BIOS（不通用）
Bit 7 = 1: Weitek math coprocessor present
Bit 6 = 1: Floppy drive seek at boot disabled
Bit 5 = 1: System boot sequence A:,C: (otherwise C:,A:)
Bit 4 = 1: System boot CPU speed high
Bit 3 = 1: External cache enabled
Bit 2 = 1: Internal cache enabled
Bit 1 = 1: Fast gate A20 operation enabled
Bit 0 = 1: Turbo switch function enabled

题外话，关于 A20 的设计有一种非常罕见的情况会导致系统崩溃，这是由 Kai Germaschewski 发现的。他的 reports 我就不在这个帖子里发了。

查了下 Award BIOS 6.00 的源代码，最后好像是 A20_OFF 了...

```
;□============================================================□
;
; A20_OFF:
;
; Turn off gate A20.
;
;ENTRY: NONE
;EXIT: Z JZ (Z=1) if success, JNZ (Z=0) if failed
;
;DESTROYS: AX
;
;□============================================================□
```

至于 BIOS 执行之前的状态，强烈建议 Raymond 老师上硬件调试器...
我有一个折中的实验方案，就是用 Bochs，在 BIOS 执行之前修改 BIOS 代码（应该可改写）：

```
00000000000i[     ] set SIGINT handler to bx_debug_ctrlc_handler
Next at t=0
(0) context not implemented because BX_HAVE_HASH_MAP=0
[0xfffffff0] f000:fff0 (unk. ctxt): jmp far f000:e05b   ; ea5be000f0   /* 跳转到 BIOS */
```

就是把 f000:505b 里面的值改成 in al, 92h 指令，再看看 al 的值。

最后，附上 windows 开启 A20 地址线的代码：

```
;VOID
;EnableA20(
;    VOID
;    )
;
;Routine Description:
;
;    Enables the A20 line for any machine.  If the MachineType global variable
;    is set to MCA, then it will call the EnableMcaA20 routine.  If not, it
;    will execute the ISA code for enabling the A20 line.
;
;Arguments:
;
```

```
;    None
;
;Return Value:
;
;    None.
;
;    The A20 line is enabled.
;
;--
        public  _EnableA20

_EnableA20      proc    near

extrn   _MachineType:dword

        test    dword ptr _MachineType,MACHINE_TYPE_MCA
        jz      EA0

;
; This is an MCA machine, so we use the special MCA routine
;
        call    _EnableMcaA20
        ret

EA0:
        mov     ah,0dfh                 ; (AH) = Code for enable
        call    empty_8042              ; ensure 8042 input buffer empty
        jnz     EA2                     ; 8042 error return


;           Enable or disable the A20 line

        mov     al,0d1h                 ; 8042 cmd to write output port
        out     STATUS_PORT,al          ; send cmd to 8042
        call    empty_8042              ; wait for 8042 to accept cmd
        jnz     EA2                     ; 8042 error return
        mov     al,ah                   ; 8042 port data
        out     PORT_A,al               ; output port data to 8042
        call    empty_8042

;       We must wait for the a20 line to settle down, which (on an AT)
;       may not happen until up to 20 usec after the 8042 has accepted
```

```
;       the command.  We make use of the fact that the 8042 will not
;       accept another command until it is finished with the last one.
;       The 0FFh command does a NULL 'Pulse Output Port'.  Total execution
;       time is on the order of 30 usec, easily satisfying the IBM 8042
;       settling requirement.  (Thanks, CW!)

        mov     al,0FFh                 ;* Pulse Output Port (pulse no lines)
        out     STATUS_PORT,al          ;* send cmd to 8042
        call    empty_8042              ;* wait for 8042 to accept cmd

EA2:
        ret

_EnableA20    endp
```

Re: 问关于A20开关的问题!

井底之蛙 2009-05-17, 15:11 下午
我也强烈建议Raymond 老师上硬件调试器！

```
;;nasm -o my my.asm
org 0h
A1:
in al,92h
mov cx,[0]
mov ax,0FFFFh
mov ds,ax
mov bx,[10h]
times (512-16)-($-$$) db 0
jmp A1
times 13 db 0
```

我用两种方法测试了一下，在Bochs中A20是开启的！

Re: 问关于A20开关的问题!

王宇 2009-05-17, 16:10 下午

1. 楼主的代码没有 0xAA55 的话，Bochs 是不能运行的（认为没有可启动的扇区）。

2. 楼主的问题是 "CPU 执行第一条指令时(BIOS里的第一条指令)" A20 的状态，用启动扇区做实验肯定不行...

3. Bochs 的 BIOS 的确是打开了 A20：

info cpu
rax: 0x00000000:0000aa02 rcx: 0x00000000:00000000
rdx: 0x00000000:00000000 rbx: 0x00000000:00000000
rsp: 0x00000000:0000ffd6 rbp: 0x00000000:00000000

这点在 OS-Dev 上有讨论：

http://forum.osdev.org/viewtopic.php?f=1&t=16642&start=0

Normally A20 IS enabled in bochs. Because bochs runs a lot faster if it doesn't have to check the A20 enabled bit on every single simulated memory access.

所以，这个问题我觉得和 BIOS 的实现标准相关，Bochs 的那个 BIOS 应该不准确。

4. 硬件调试器啊硬件调试器... T_T 眼泪哗哗的...

Re: 问关于A20开关的问题!

格蠹老雷 2009-05-17, 18:16 下午
哈哈哈，卖ITP的看到这个帖子该有多高兴呀:-)
这两天忙着写专栏的文章，ITP也不在手上，明天会试验一下。

Re: 问关于A20开关的问题!

井底之蛙 2009-05-17, 18:39 下午
我不加载ISA模块，而是替换了整个BIOS，
romimage: file=../my
#romimage: file=../BIOS-bochs-latest
哈哈！
// Settable A20 line. For efficiency, you can disable

```
// having a settable A20 line, eliminating conditional
// code for every physical memory access. You'll have
// to tell your software not to mess with the A20 line,
// and accept it as always being on if you change this.
// 1 = use settable A20 line. (normal)
// 0 = A20 is like the rest of the address lines

#define BX_SUPPORT_A20 1
```

Bochs在编译的时侯确实可以指定A20开关,
但是我关闭A20重新编译Bochs后, 经测试发现还是打开的※※※※
我认为BX_SUPPORT_A20只是决定BIOS初始化完成后对A20的开/关
我无法想象CPU在运行第一条指令时, A20是关闭的!

Re: 问关于A20开关的问题!

格蠹老雷 2009-05-18, 22:21 下午

今天比较忙, 使用ITP匆忙看了一下。

(一)CPU复位后, 0x92端口的值是0

```
[[P0] RESET break at 0xf000:000000000000fff0 ]
[ RESET break at 0xf000:0000000000000000 ]

[P1]>port(0x92)
00
```

这与ICH(南桥)手册上所描述的默认值是一致的。

(二)在BIOS阶段, (至少是对于试验中的这个BIOS)确实曾经将0x92端口写为2

(三)在进入操作系统(Windows)后, 向0x92写0或者写2都能写成功(可以读回所写的值), 系统仍然正常运行, 没有察觉到影响。

(四) 仔细读了下IA-32手册卷三A(Vol3A)的有关内容, 起切换作用的关键是A20M管脚, 它是低电平有效的, 当这个管脚为低时, CPU会屏蔽A20地址线, 也就是始终认为A20这个地址线的值是0:

A20M# pin — On an IA-32 processor, the A20M# pin is typically provided for compatibility with the Intel 286 processor. Asserting this pin

causes bit 20 of the physical address to be masked (forced to zero) for all external bus memory accesses. Processors supporting Hyper-Threading Technology provide one A20M# pin, which affects the operation of both logical processors within the physical processor.

但是，我觉得上面这段话是有条件的，这个条件就是CPU工作在实模式下。也就是说，只有当CPU处于实模式时，才会应用这个逻辑。

使用ITP的读取管脚信号命令观察A20M管脚的值，始终是1（高点平），不管端口0x92的值是多少。
[P1]>[p0]pins
A20M#=1 ...
这一点令人困惑，不确认是否是工具存在问题。

（五）查阅ICH手册，南桥会输出一个A20M信号，通常的系统（主板）便是将这个信号送给CPU。因此南桥的这个信号输出什么值便很关键。但是在多个版本的ICH手册中，关于这个信号逻辑的描述居然都自相矛盾。可以肯定的是它的值是由下面二者决定的：
1）端口0x92的bit 1
2）ICH的A20Gate输入，这个输入的来源通常便是王宇提到的键盘控制器（历史上曾经是8042）。
一种说法是上面两个值都是0，那么A20M才会Active（low），另一种说法是上面两者设置一个就有效。

虽然还没有完全一清二楚，但是楼主的问题还是比较清楚的：
（1）CPU刚刚复位后（immediate after reset）A20M#是高电平的，Mask逻辑无效，因此A20这个地址位是有效的，或者可以粗略的说A20地址线是开启的。
（2）这个逻辑只影响第21位（A20）这一位地址是一定的。

Re: 问关于A20开关的问题!

格蠹老雷 2009-05-19, 12:45 下午
思考了一下, ICH中的规则应该是:
A20M# = (bit 1 of Port92) .OR. (A20Gate)
这样一来:
1)A20M#是低电平有效的, 也就是当其为0时, 屏蔽逻辑才起作用。
2)不论是设置Port92的Bit 1还是设置A20Gate都可以导致A20M#变高电平, 屏蔽逻辑失效, 也就是A20地址线正常工作。

换句话来说, 要屏蔽A20, 那么要求两个地方都为0;如果要取消屏蔽逻辑, 设置其中任何一个都可以。

Re: 问关于A20开关的问题!

MJ0011 2009-05-21, 16:00 下午
不需要硬件调试器, 用老机器试一下top swap就可以知道了

Re: 问关于A20开关的问题!

井底之蛙 2009-05-21, 17:02 下午
from《Intel® I/O Controller Hub 10 (ICH10) Family》
A20M# (Mask A20)
The A20M# signal is active (low) when both of the following conditions are true:
• The ALT_A20_GATE bit (Bit 1 of PORT92 register) is a 0
• The A20GATE input signal is a 0
The A20GATE input signal is expected to be generated by the external microcontroller (KBC).
Raymond说的没错！！
我在真实的机器和VMWare的XP、2003下做实验, 情况和上面说的一样, 但Bochs就不一样了, 好像是and的关系！

Re: 问关于A20开关的问题!

---

dannydeng 2009-06-19, 13:53 下午
对于Intel 平台, A20状态是由Pot 92 bit1和南桥A20gate信号决定,它们是or的关系.所以要关A20必需同时关92 port和发KBC command. 开机时默认的A20状态, 92 port是0, 但KBC代码在上电reset 过程中会拉A20gate 信号, 所以系统看到默认A20就是开的.

Re: 问关于A20开关的问题!

夜凉 2009-06-26, 17:25 下午
开机时就打开A20和在boot例程里打开有什么不同么？另外A20打开和关闭还有些什么用处没?

Re: 问关于A20开关的问题!

---

quanta 2009-07-13, 23:07 下午
<BLOCKQUOTE><table width="85%"><tr><td class="txt4"><img src="/Themes/default/images/icon-quote.gif"> MJ0011 wrote:</td></tr><tr><td class="quoteTable"><table width="100%"><tr><td width="100%" valign="top" class="txt4">不需要硬件调试器, 用老机器试一下top swap就可以知道了</td></tr></table></td></tr></table></BLOCKQUOTE>

数据怎么抛出来？