

小華的部落格

將自己踏入BIOS領域中所學習到的知識做一些心得整理，像是Legacy BIOS、EFI BIOS、Windows Driver...etc. ※版權與智慧財產權聲明:保留所有法律權利。我在寫文章時如果有引用到其他人的地方我會盡量說明參考出處，如果有遺漏的地方請告訴我，我會馬上註明! 而轉貼我的文章時也請您註明出處!

 搜尋

首頁

About Me

總網頁瀏覽量



1 7 7 6 2 6

1

訂閱小華的部落格

發表文章



留言



訂閱

請輸入您的email address:

星期三, 10月 10, 2007

[我所知道的BIOS]->[Shadowing] 8

[Why shadow BIOS ?]

在此之前所提的BIOS tasks,都是循著 CPU->NB->SB->SIO->ROM的路徑來達成的;意即: CPU是去BIOS ROM裡面抓code來執行! 明顯的一件事是: ROM access time > DRAM access time! 且RAM access width is 32bits, 而 ROM access width 通常為 16 bits. 因此,便有了所謂" BIOS Shadowing"的觀念產生! <- "performance consideration" !!!

[What is shadowing]

意即: 將部分BIOS CODE(in ROM)拷貝至DRAM中! (此後, CPU將從DRAM中抓code來執行...)這樣的動作便稱做 "Shadowing"! 而該處的DRAM即稱為 shadow memory.

Shadowing 在BIOS 中是極為複雜的 kernel code part! 想深入瞭解的人最好有 source code可 trace.

[When to shadow BIOS]

=> 當然是等記憶體穩定了,可以使用後,才做 ^_^

*因此,假如 DRAM sizing 有問題, BIOS shadowing必定有問題 !!!

訂閱電子報

EZMAIL提供

Translate

选择语言 | ▼

網誌存檔

- 2020 (1)
- 2019 (2)
- 2018 (3)
- 2016 (2)
- 2015 (1)
- 2014 (8)
- 2013 (3)
- 2012 (12)
- 2011 (19)
- 2010 (20)
- 2009 (11)
- 2008 (35)
- ▼ 2007 (59)
 - 12/23 - 12/30 (1)
 - 12/16 - 12/23 (4)
 - 12/02 - 12/09 (1)

以下是之前在其他文章中發表關於 shadow 的文章,再次節錄以供參考 !

[System Behavior before & after shadow]

說的更白話一點就是 : 當 Power On後, 跑完 system power-on sequence後, CPU會被 reset (reset 指的是 CPU 的內容會回到 "初始值"); 而 CPU內部的 EIP (32-bit)的初值是 FFFFFFF0h, 所以, CPU的 第一個 code read 就是到 FFFFFFF0h fetch code...

這個 memory cycle 從 CPU發出, 先會經過 North bridge ; 此時, north bridge會說 "這不是我的"...然後,往 south bridge 丟 ; south bridge 會說, "這是我的",收下後丟給 ROM ! 所以, FFFFFFF0h 會被 ROM 接走 !!! (所以 前人才說 "硬體初始值要把0xFFFFFFFF 和 0x000FFFF0 要mapping到同一個地方", 這個地方就是.....ROM !!!)

之後, CPU所發的 cycle 都會照上述的方式一路抵達 ROM...由 CPU循著 fetch, decode, execute, store的順序作事情...

但到某一個階段前, BIOS的 code 會指示 " 要將 BIOS data 從 ROM 搬到 DRAM" ! 而在此階段之後, BIOS會設定 north bridge 暫存器, 告訴 north bridge "之後 CPU所發的 cycle 不可以不收而傳到 south bridge"....

自此之後, CPU 所發的 cycle 全部轉到 DRAM 中,由 CPU循著 fetch, decode, execute, store的順序作事情...

[Summary] 總而言之, BIOS 一開始是CPU讀取 ROM content來執行,之後是CPU 讀取 DRAM content 執行 ^_^

[補充][以提問的方式^_^]

[Q]: shadow memory到底是那一塊 ?

[A]: 以現在的電腦系統而言, shadow memory 是在UMA(upper memory area;傳統記憶體 640K以上至1M之間) "裡面"(part of it) ;在此UMA內可以分為 6 segments(64kB/each), total 384KB.

其中 C0000h~DFFFFh: for VGA BIOS and other devices' Option ROMs
E0000h~FFFFFFh: BIOS ROM code

這兩個 blocks 本質是 memory;之後會被載以ROM content;因此,便稱為 shadow memory(好像: ROM在上面, memory在下面,是ROM的 "shadow"...))

[Q]: shadow memory 的內容 完全 "=" ROM content ?

[A]: of course NOT ! 除了 UMA不大以外,BIOS ROM因為必須support more and more functions/features,size已經越長越大;除此之外,BIOS ROM中也有部分module是經過壓縮的.(UMA不夠放...)

當BIOS shadow時,只會 copy necessary code(Ex. run-time要用的...etc)至 shadow memory ! 另外,已經執行過

► 11/25 - 12/02 (2)

► 11/18 - 11/25 (1)

► 11/11 - 11/18 (3)

► 11/04 - 11/11 (4)

► 10/28 - 11/04 (4)

► 10/21 - 10/28 (2)

► 10/14 - 10/21 (2)

▼ 10/07 - 10/14 (7)

SCI Check List

[我所知道的BIOS]->[PCI
SCAN] 9

[我所知道的BIOS]->
[Shadowing] 8

[我所知道的BIOS]->
[DRAM Sizing](2) 7

從前從前, Big-Endian與
Little-Endian?

[我所知道的BIOS]->
[DRAM Sizing] (1) 7

[我知道的BIOS]->[系統資
源] 6

► 09/23 - 09/30 (6)

► 08/26 - 09/02 (2)

► 07/29 - 08/05 (3)

► 07/08 - 07/15 (1)

► 07/01 - 07/08 (3)

► 06/17 - 06/24 (2)

► 05/27 - 06/03 (3)

後的code也不會被載入. 因此,不是 1-1的copy...

[Q]: what Shadow enabled/disable mean in chipset ?

[A]: 前面提過, CPU要 fetch的code由 shadow memory 提供 or ROM提供,其根本關鍵在於 chipset's behavior ! 意即,NB必須做此決定 ! 所以,這機制一般是由NB來實現的.

NB內有所謂的 shadow registers. 當 shadow register enable時, memory cycle由 shadow memory 來回應;若 shadow disable,則由ROM回應.

意即:

000E0000h~000FFFFFFh由 shadow memory replies if (shadow enabled)

000E0000h~000FFFFFFh由 ROM chip replies if (shadow disabled)

若FFFE000h~FFFFFFFFh呢? 必定由ROM chip來回應(不然一開機怎麼辦?). 與 shadow disable/enable無關 !!!

*若使用 ru.exe 並檢視 memory space,可發現上述的情況.

[Q]: shadow有何好處 ?

[A]: 因為 slower ROM v.s faster RAM,所以放在RAM可以增加 system performance.

*各位可以發現,同樣的code放在 rom & dram中執行速度將大不相同 !

[Q]: shadow memory的 issue ?

[A]: 被 shadowed 的 memory area都會被設成 write-protected ! 因此,這塊area是不能 write 的.所以,若有程式會 "write"這塊,則會有問題 !!!

其實, BIOS shadow這段code大家不太會碰觸到...瞭解基本information即可.

有錯誤請指正 !!!

[附註]

[Q1] "BIOS的所有動作都必須先從ROM COPY至DRAM之後CPU才有辦法去執行"

Ans : 講簡單一點就是對CPU來說, 他只負責提取指令, 解碼指令, 執行指令. 至於是讀取到哪邊的指令他就不管了(IA32 架構). 例如CPU要讀取F0000h的指令來執行, 那F0000h有可能是ROM也有能是DRAM.

[Q2] "那BIOS一開始的0E05BH是ROM的位置? 還是DRAM的位置呢? "

==>0~4G 是指位址線的位址(因為Address bus = 32 bits=2^32), 至於位址線上面是分配給DRAM還是ROM使用還是Others...就要看實際的硬體架構, 例如IA32 架構就有其分配的方式.

- 05/06 - 05/13 (5)
- 04/29 - 05/06 (1)
- 04/22 - 04/29 (2)
- 2006 (1)

逛逛不一樣的地方

演算法 (影像處理, 資料結構, 智慧型視訊分析, 人工智慧)

平凡的幸福

相關資訊

流浪小築

旅遊美食~

小君君的祕密花園

繼續閱讀懶人加強版

幸福雅痞~

懷舊系列~

標籤

一些筆記 (10)

分享 (2)

心情分享 (3)

生活運用 (1)

==>所以某個位址線的位址可以被分配給ROM使用也可以分配給DRAM使用，還可以重疊一起使用，例如 F segment (000F_0000h)就是重疊使用，所謂的重疊就是就像是CPU 對F0000h存取的時候，他是存取到DRAM的資料還是ROM的資料？答案就是看北橋....如果北橋在此時把這個位址是映對到ROM，那麼CPU讀取到的F0000h資料是ROM裡面的，如果北橋是映對到DRAM那麼CPU一樣是讀取F0000h但是會讀取到DRAM內的資料。

==> 所以0E05Bh 是位址線的位址。

==> 另外BIOS一開始的位址是在FFFF_FFF0 不是在0E05Bh...

==> BIOS的程式碼會去改變北橋設定，讓在不同階段的執行期間去存取到DRAM/ROM的資料，我們稱為shadow....例如從F0000h的 ROM讀資料，寫到F0000h 的DRAM中

==> 這邊說的都是IA32，其他架構要看Spec 說明。

張貼者： 小華的部落格



標籤： [BIOS相關](#)

2 則留言：

Unknown 提到...



作者已經移除這則留言。

5月 10, 2018 8:58 上午

badants 提到...



請問一下有辦法讓記憶支援的容量變大嗎？

9月 05, 2018 8:22 上午

張貼留言

[較新的文章](#)

[首頁](#)

[較舊的文章](#)

訂閱： [張貼留言 \(Atom\)](#)

