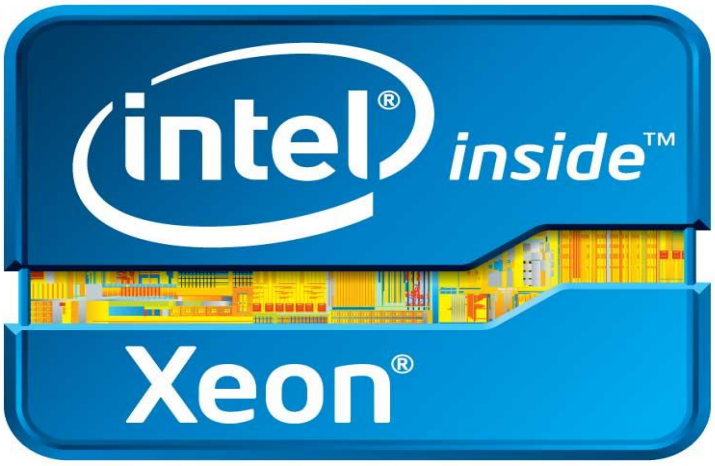
BÁO CÁO TIỂU LUẬN

KỸ THUẬT VI XỬ LÝ

GIẢNG VIÊN : HOÀNG XUÂN DẬU

Đề Tài:

TÌM HIỂU KIẾN TRÚC DÒNG VI XỬ LÝ INTEL XENON 6000



Thành Viên :
Lê anh Tuấn
Nguyễn Đình Thịnh
Nguyễn Xuân Tiến
Vũ Thành Tuân
Vũ Văn Thuẫn

I.GIỚI THIỆU

Các thương hiệu Xeon đã được duy trì qua nhiều thế hệ của vi xử lý x86 và x86-64 , tên của vi xử lý này ở mô hình cũ thường được thêm vào phần sau tên của các vi sử lý thông thường (vi xử lý dành cho máy tính để bàn) , Nhưng các mô hình gần đây dùng Xeon theo tên riêng của mình . CPU thường có bộ nhớ Cache cao hơn nhiều so với các vi xử lý khác và có khả năng multiprocessing capabilities (đa xử lý) .

Intel Xeon Processor 6000 được thiết kế cho các khối công việc bộ nhớ hạn chế . Intel Xeon Processor 6000 với máy chủ đa lõi 64-bit là sự lựa chọn hợp lý nhất .

Đặc Điểm :

- Với 8 core và 16 threads cho mỗi Socket và công nghệ Intel ® Hyper-Threading Technology . Intel Xeon đã tăng hiệu xuất xử lý với việc sản xuất trên công nghệ 45nm và hỗ trợ khoảng không cho các ứng dụng đòi hỏi xử lý đa luồng .
- Với vi kiến trúc Nahalem cho phép thúc đẩy hiệu xuất của bộ nhớ cache trên nhiều ứng dụng , mô trường người sử dụng . Cho phép triển khai dữ liệu với mật độ cao .

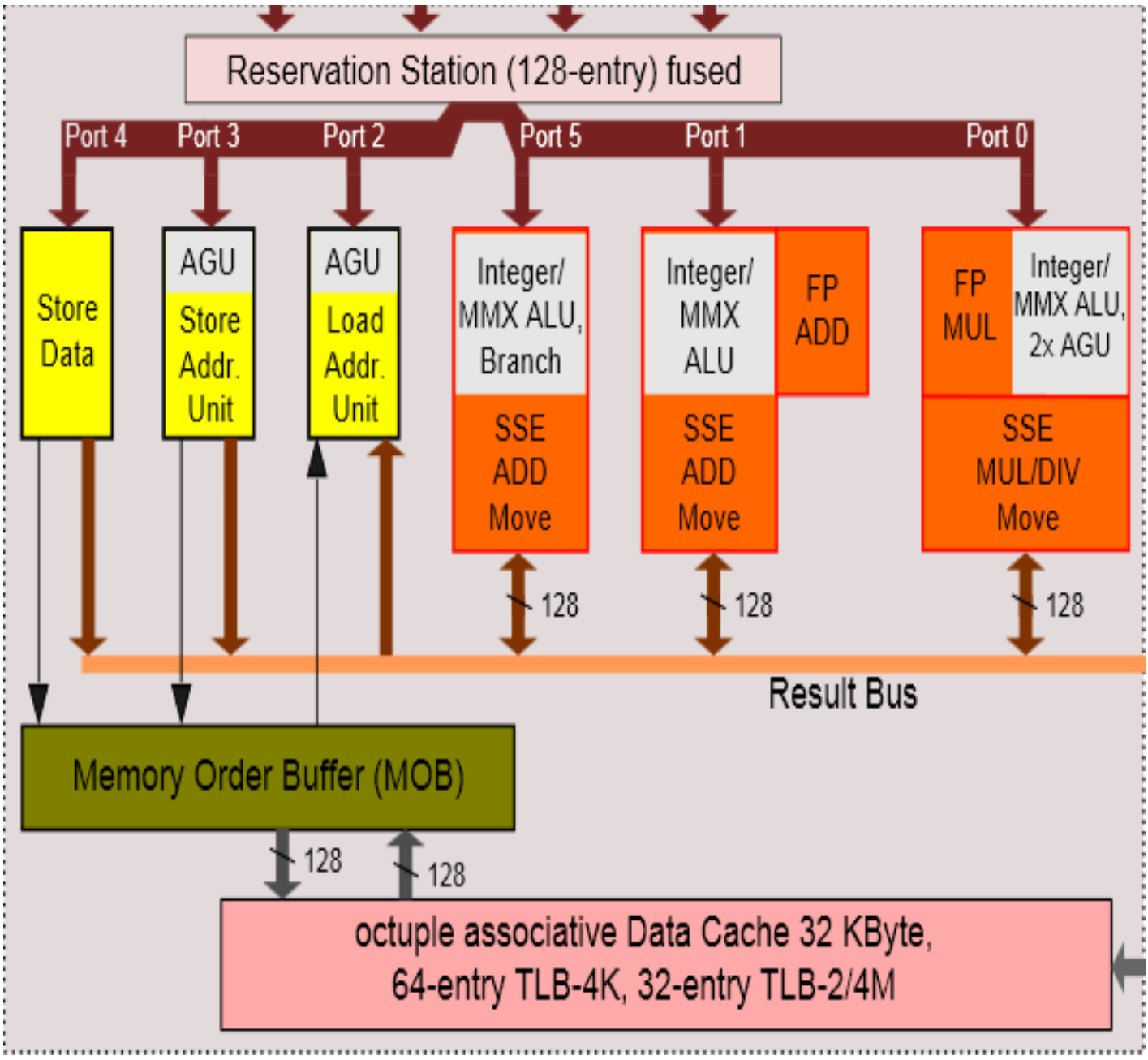
- Bộ nhớ cache L3 18 MB làm tăng hiệu quả truyền dữ liệu cache – to – core , tối đa hóa bộ nhớ chính để xử lý băng thông .
- Intel QuickPath Interconnect (Intel QPI) cung cấp tốc độ cao (lên đễn 25,6 GB/s), point – to – point kết nối giữ vi xử lý , cũng như giữa các bộ sử lý và trung tâm I/O hub .

II.KIẾN TRÚC VI SỬ LÝ

1-Sơ Đồ Khối

CPU Xeon 6000 dựa theo kiến trúc nehalem.

Sơ đồ khối của các khối thực thi:

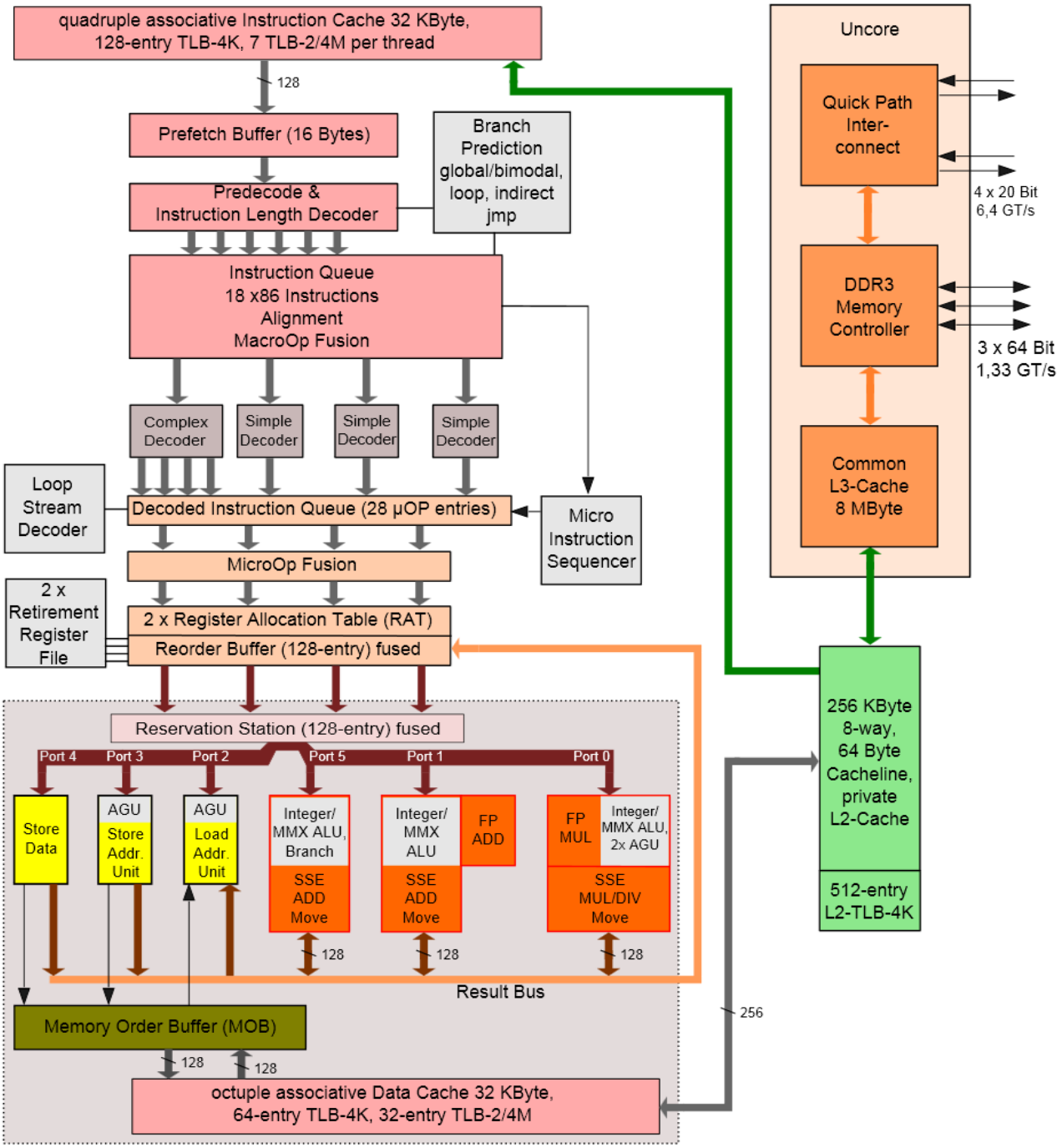


- FPU : Floating - Point Unit. Khối này chịu trách nhiệm cho việc thực thi cácbiểu thức toán học floating-point và cũng cả các chỉ lệnh MMX và SSE. Trong CPU này, các FPU không “hoàn thiện” vì một số kiểu chỉ lệnh (FPmov, FPadd và Fpmul) chỉ được thực thi trên các FPU nào đó :

- Fpadd : Chỉ có FPU này mới có thể xử lý các chỉ lệnh cộng floating-point như ADDPS.
- FPmul: Chỉ có FPU này mới có thể xử lý các chỉ lệnh nhân floating-point như MULPS
- FPmov:Các chỉ lệnh cho việc nạp hoặc **copy** một thanh ghi FPU, như MOVAPS (đượcdùng để truyền tải **dữ liệu** đến thanh ghi SSE 128-bit XMM). Kiểu chỉlệnh này có thể được thực thi trên các FPU, nhưng chỉ trên các FPU thứhai và **thứ ba** nếu các chỉ lệnh Fpadd hay Fpmul không có trongReservation Station.

- FP ADD: thực thi một chỉ lệnh SSE có tên gọi PFADD (Packed FP Add) và các chỉ lệnh COMPARE, SUBTRACT, MIN/MAX và CONVERT. Khối này được cung cấp riêng, chính vì vậy nó có thể bắt đầu việc thực thi một chỉ lệnh giải mã mới mỗi chu kì clock dù là nó không hoàn tất được sự thực thi của chỉ lệnh đã giải mã trước. Khối này có một độ trễ 3 chi kì clock, nghĩa là nó sẽ giữ chậm 3 chu kì clock đối với mỗi chỉ lệnh đã được xử lí.
- AGU : những lệnh liên quan đến số nguyên và lên quan đến bộ nhớ được thực hiện ở đây .
- Store Data: Khối này xử lý các chỉ lệnh yêu cầu **dữ liệu** được ghi vào bộ nhớ RAM.

Intel Nehalem microarchitecture



GT/s: gigatransfers per second

2 – Đặc Điểm Phần Cứng

Đặc điểm cache :

Hệ thống cache trong Xeon 6000 được tăng thêm một mức cache L3 có dung lượng lớn (18MB) và dùng chung cho tất cả các nhân. Mỗi nhân còn sở hữu riêng hai cache L1 (32KB) và L2 (32KB, độ trễ thấp hơn 12 chu kỳ và có 8 đường liên kết).

Bộ nhớ đệm L3 trong vi xử lí xeon 6000 hoạt động với tần số độc lập và có hệ thống cấp nguồn riêng biệt với các nhân để đảm bảo độ ổn định và giảm xác suất lỗi. Ưu điểm của thiết kế cache L3 này là giúp việc trao đổi dữ liệu giữa các nhân hiệu quả hơn mà không cần thông qua các cache bên trong của mỗi nhân. Tuy nhiên, cache L3 cũng có ảnh hưởng đến hoạt động của cache riêng trong mỗi nhân. Mỗi dòng lệnh trong cache L3 chứa 4 bit đánh dấu nhân nào có chứa bản sao của dòng lệnh đó trong những cache riêng của mình. Cụ thể, khi một nhân truy vấn L3 và "thấy" bit đánh dấu mang giá trị 0 thì sẽ "hiểu" là trong cache riêng của nó chưa có bản sao dòng lệnh đó, và ngược lại, nếu bit đánh dấu mang giá trị 1 thì có khả năng cache riêng của nó đã có bản sao của dòng lệnh đó. Hơn nữa, giao thức truy xuất dữ liệu trong cache của các nhân cũng có sự chuyển biến thành giao thức MESIF (Modified, Exclusive, Shared, Invalid and Forward). Sự phối hợp của những bit đánh dấu và MESIF giúp giảm bớt tần suất truy cập cache của các nhân nên sẽ giải phóng nhiều băng thông hơn cho những dữ liệu thật sự cần thiết trong các cache.

Bộ phận điều khiển bộ nhớ và Bus ngoài

Để tăng tốc độ giao tiếp với RAM trong bộ VXL được tích hợp một chip điều khiển bộ nhớ. Chip điều khiển này sẽ chỉ hỗ trợ cho bộ nhớ hiệu năng cao DDR3, cho phép chạy được chế độ bộ nhớ kênh ba (triple channel) thay vì chỉ chạy kênh đôi như hiện nay. Sau khi "loại bỏ" lượng băng thông dùng cho bộ nhớ, tuyến bus được sử dụng trước đây để BXL giao tiếp với chipset (giờ có tên là Intel QuickPath Interconnect - Intel QPI) sẽ trở thành tuyến bus "độc quyền" cho công việc trao đổi giữa BXL và các thiết bị khác trong hệ thống. Intel QPI sẽ gồm hai tuyến truyền nhận dữ liệu hoàn toàn riêng biệt với băng thông trên mỗi đường rất cao. Tuy nhiên, việc mở rộng tuyến bus nói trên đã góp phần làm tăng số lượng chân (pin) giao tiếp trên BXL. Do đó, việc sử dụng socket LGA775 với 775 chân không còn phù hợp.

Vì vậy, trên các bo mạch chủ hỗ trợ các BXL nền Nehalem đều được trang bị socket FCLGA1567.

Sau đây là cấu hình của

Bộ vi xử lí Intel Xeon X6550 - AT80604001797AB:

- Microarchitecture: Nehalem
- Platform: Boxboro-EX
- Core Stepping D0 (SLBRB)
- CPUID 206E6 (SLBRB)
- Công nghệ vi xử lí 45nm
- Băng thông dữ liệu 64 bit
- Số nhân 8
- Cache mức 1
  - 8 x 32 KB instruction caches
  - 8 x 32 KB data caches
- Cache mức 2 8 x 256 KB
- Cache mức 3 18MB
- Đa xử lí Lên đến 2 vi xử lí
- Các tính năng
  - MMX intruction set
  - SSE
  - SSE2
  - SSE3
  - Suppelemental SSE3
  - SSE4.1
  - SSE4.2
  - EM64T technology
  - Virtualization technology (VT-x and VT-d)
  - Execute Disable bit (giúp chống lại một số virus và mã độc).
  - RAS with machine check Architechture recovery (phát hiện và báo lỗi phần cứng)
  - Hyper-Threading technology (siêu phân luồng)
  - Turbo Boost Technology
- Tính năng tiết kiệm điện Enhanced SpeedStep technology
- Điều khiển thiết bị ngoại vi

- 2 bộ điều khiển bộ nhớ DDR3 SDRAM tích hợp với 2 kênh đôi mở rộng giao tiếp bộ nhớ trên mỗi bộ điều khiển
- Quick Path Interconnect (4 tuyến)
- Giao tiếp PCI Express 2.0

III.KIẾN TRÚC TẬP LỆNH

Tập lệnh của Intel Xeon 6000

A - Giới thiệu chung về tập lệnh:

- Mỗi bộ xử lý có một tập lệnh xác định

- Tập lệnh thường có hàng chục đến hàng trăm lệnh

- Mỗi lệnh là một chuỗi số nhị phân mà bộ xử lý hiểu được để thực hiện 1 thao tác xác định.

- Các lệnh được mô tả bằng các ký hiệu gợi nhớ chính là các lệnh của hợp ngữ.

Cấu trúc tập lệnh chia làm 6 nhóm với các lệnh cơ bản sau:

Nhóm lệnh truyền dữ liệu

- MOVE Copy dữ liệu từ nguồn đến đích

- LOAD Nạp dữ liệu từ bộ nhớ đến BXL

- STORE Cất dữ liệu từ bộ xử lý đến bộ nhớ

- CLEAR Chuyển các bit 0 và toán hạng đích

- SET Chuyển các bit 1 vào toán hạng đích

- INPUT Copy dữ liệu từ một cổng xác định đưa đến đích

- OUTPUT Copy dữ liệu từ nguồn đến một cổng xác định

Nhóm lệnh số học

- ADD Cộng hai toán hạng

- SUBTRACT Trừ hai toán hạng

- MULTIPLY Nhân hai toán hạng

- DIVIDE Chia hai toán hạng

- ABSOLUTE Lấy trị tuyệt đối toán hạng

Các lệnh điều khiển chương trình

- JUMP (BRANCH) Lệnh nhảy không điều kiện: nạp vào PC một địa chỉ xác định

- JUMP CONDITIONAL Lệnh nhảy có điều kiện: điều kiện đúng nạp vào PC một địa chỉ xác định ,điều kiện sai không làm gì cả

- CALL Lệnh gọi chương trình con

- RETURN Lệnh trở về từ chương trình con

Các lệnh logic

- AND Thực hiện phép AND hai toán hạng

- OR Thực hiện phép OR hai toán hạng

- XOR Thực hiện phép XOR hai toán hạng

- NOT Đảo bit của toán hạng (lấy bù 1)

Các lệnh điều khiển hệ thống

- HALT Dừng thực hiện chương trình

- WAIT Tạm dừng thực hiện chương trình, lặp kiểm tra điều kiện cho đến khi thoả mãn thì tiếp tục thực hiện

- NO OPERATION Không thực hiện gì cả

- LOCK Cấm không cho xin chuyển nhượng bus

- UNLOCK Cho phép xin chuyển nhượng bus

Các lệnh so sánh

- CMP So sánh 2 byte hay 2 từ
- TEST Phép và 2 toán hạng để tạo cờ

Xeon bắt đầu sự nghiệp của nó khi còn là lớp con của Pentium II. Ngày nay, Intel đã xếp Xeon vào lớp Pentium III. Cũng như Pentium Pro, Xeon được thiết kế dành cho server và các trạm làm việc trung và cao cấp.

Các tập lệnh cơ bản của VXL này là MMX, SSE(1,2,3,3S,4.1,4.2), EM64T, VT-x

Đây là các tập lệnh được tích hợp trong bộ vi xử lý. Mỗi tập lệnh sẽ chịu trách nhiệm xử lý những yếu tố chuyên biệt. CPU nào hỗ trợ càng nhiều tập lệnh thì tốc độ xử lý lệnh càng nhanh (tức là tốc độ xử lý càng nhanh).

Giới thiệu qua một vài thuật ngữ:

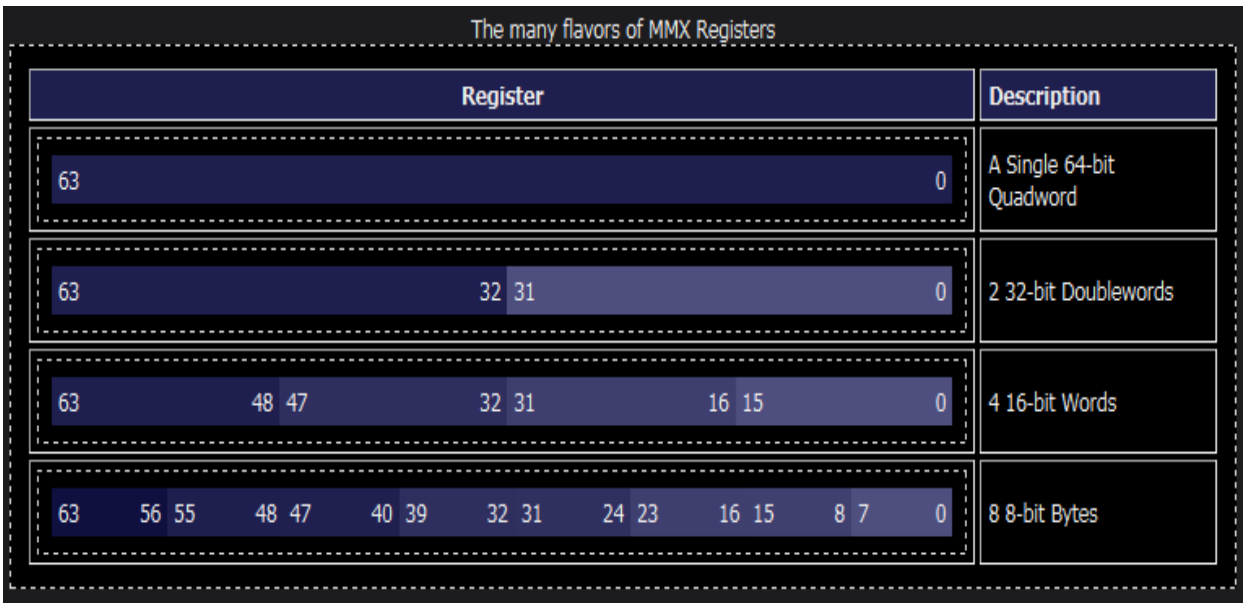
SIMD (Single Instruction, Multiple Data). SIMD mô tả bất kỳ phần mở rộng bộ vi xử lý cho phép nó hoạt động trên dữ liệu song song. Một số phần mở rộng SIMD phổ biến là: MMX, 3DNow!, SSE, và AltiVec (liên quan đến vmx). Có rất nhiều cái khác nữa, nhưng đây là những cái phổ biến nhất được tìm thấy trong máy tính thông thường. Hầu hết các SIMD đã được sửa đổi một chút ít trước khi được triển khai thực hiện. Điều này cho phép chúng ta mở rộng chúng bao gồm MMX, MMX mở rộng, 3DNow!, 3DNow 2 (đôi khi được gọi là 3DNow Professional hoặc 3DNow! +), SSE (còn được gọi là Katmai New instructions hoặc vắn tắt là KNI), SSE2 (còn được gọi Willamette New instructions hoặc chỉ đơn giản là WNI), SSE3 (cũng được gọi là Prescott New instructions hoặc chỉ đơn giản là PNI), và tập lệnh SSE4 (còn được gọi là Tejas New instructions hoặc đơn giản là TNI).

MMX (Multimedia Extensions) –là tập lệnh mở rộng đầu tiên của SIMD được Intel phát triển trên nền 8086, tập lệnh bao gồm 57 lệnh multimedia do Intel phát triển năm 1997. Công nghệ MMX bao gồm 8 thanh ghi từ MM0 đến MM7, tích hợp 4 kiểu dữ liệu kiểu bye kiểu word, kiểu doubleword và quadword, và các tập lệnh MMX.

MMX Registers in FPU's Register Space

Register	79 - 64	63 - 0
ST0	xx	MM0
ST1	xx	MM1
ST2	xx	MM2
ST3	xx	MM3
ST4	xx	MM4
ST5	xx	MM5
ST6	xx	MM6
ST7	xx	MM7

Chú ý: 16bit trong 80-bit FPU register không được sử dụng trong MMX



Mục đích chính của MMX là nâng cao hiệu quả xử lý các lệnh lặp về âm thanh, hình ảnh và đồ họa. Máy đạt được điều này phần nào do một dòng lệnh đơn có thể xử lý đồng thời một số mục dữ liệu.

MMX được thiết kế sẵn trong các dòng CPU Intel . Tập lệnh MMX cho phép các tác vụ được thực hiện đồng thời trên nhiều đơn vị dữ liệu khác nhau. Các đối thủ

cạnh của Intel (như AMD, Cyrix, Centaur) cũng phát triển các bộ xử lý tương thích MMX của họ (MMX-compliant chips) với các bộ lệnh riêng chuyên xử lý các tác vụ tính tóan hình học và dấu chấm động cần thiết khi di chuyển các hình ảnh 3D (3 Dimension - 3 chiều) trên màn hình .

Các lệnh MMX bao gồm các nhóm lệnh cơ bản sau:

+ Lệnh truyền dữ liệu

+ Lệnh số học

+ Lệnh so sánh

+ Lệnh chuyển đổi

+ Lệnh logic

MMX hỗ trợ khả năng tính toán số học mới được gọi là chế độ bão hòa số học. Có nghĩa là kết quả của phép tính được đặt trong một phạm vi giới hạn giữa giá trị tối đa và giá trị tối thiểu. Ví dụ với một phép tính khi kết quả trả về vượt quá giá trị kiểu bye khai báo ban đầu nó sẽ được mặc định về 127 với giá trị lớn hơn 127 hoặc -128 với kết quả nhỏ hơn 128. Xét về tính toán nó có vẻ không được phù hợp cho lắm tuy vậy nó lại có ứng dựng quan trọng xử lí lân cận ví dụ xử lí ảnh tính toán báo hòa làm một vật giữ nguyên màu sắc trắng hoặc đen mà không cho phép đảo ngược.

SSE (Streaming SIMD Extension)

SSE là mở rộng SIMD mới nhất cho bộ vi xử lý Pentium III và AMD AthlonXP. Không giống như MMX và 3DNow! , không những chiếm không gian giống như các thanh ghi FPU bình thường, mà SSE bổ sung thêm một không gian riêng biệt để bộ vi xử lý. Bởi vì điều này, SSE chỉ có thể được sử dụng trên hệ điều hành hỗ trợ nó. May mắn thay, hầu hết các hệ điều hành gần đây đều được xây dựng để hỗ trợ nó. Tất cả các phiên bản của Windows kể từ Windows98 hỗ trợ SSE, cũng như hạt nhân Linux từ phiên bản 2.2.

Một nhóm gồm 70 lệnh được thiết kế thêm trên Bộ xử lý Pentium III nhằm tăng cường chất lượng thực thi các tác vụ đồ họa 3 chiều (3D graphics).

Nó hỗ trợ khả năng thực hiện tính toán dấu chấm động và hình học - các tính năng cần thiết để hiển thị và di chuyển hình ảnh 3 chiều trên màn hình. Đây là tập hợp các lệnh tăng cường thứ 2 của Intel nhằm cải tiến khả năng đồ họa của các bộ vi xử lý (tập hợp đầu tiên chính là MMX). SSE còn được gọi là KNI (Katmai New Instruction) do tên mã trước đây của CPU Intel Pentium III là Katmai. SSE có thêm 8 thanh ghi 128-bit, được chia thành 4. Các thanh ghi được gọi từ XMM0 - XMM7. Một thanh ghi được khiển bổ sung được gọi là MXCSR tồn tại trong hệ thống để kiểm tra tình trạng của các tập lệnh SSE.

Pnemonic	Bit Location	Description
FZ	bit 15	Flush To Zero
R+	bit 14	Round Positive
R-	bit 13	Round Negative
RZ	bits 13 and 14	Round To Zero
RN	bits 13 and 14 are 0	Round To Nearest
PM	bit 12	Precision Mask
UM	bit 11	Underflow Mask
OM	bit 10	Overflow Mask
ZM	bit 9	Divide By Zero Mask
DM	bit 8	Denormal Mask
IM	bit 7	Invalid Operation Mask
DAZ	bit 6	Denormals Are Zero
PE	bit 5	Precision Flag
UE	bit 4	Underflow Flag
OE	bit 3	Overflow Flag
ZE	bit 2	Divide By Zero Flag
DE	bit 1	Denormal Flag
IE	bit 0	Invalid Operation Flag

MXCSR là 1 thanh ghi 32-bit chứa các cờ điều khiển và thông tin liên quan đến các lệnh của SSE, chỉ các bit từ 0 – 15 được xác định.

SSE 2

Là tập lệnh hỗ trợ đồ họa mở rộng được thiết kế cho Pentium 4. Vi kiến trúc Netburst™ (Netburst™ Microarchitecture) mở rộng khả năng xử lý theo kiểu cấu trúc SIMD mà các công nghệ Intel® MMX™ và SSE bằng cách thêm vào 144 lệnh mới. Các lệnh này bao gồm các tác vụ số Nguyên SIMD 128-bit (128-bit SIMD integer arithmetic operations) và các tác vụ dấu chấm động với độ chính xác gấp đôi SIMD 128-bit (128-bit SIMD double-precision floating-point operations). Các lệnh mới này làm tối ưu hóa khả năng thực hiện các ứng dụng như phim video, xử lý âm thanh - hình ảnh, mã hóa, tài chính, thiết kế và nghiên cứu khoa học, kết nối mạng trực tuyến.

Cơ bản về Netburst™:

Là mô hình vi kiến trúc (micro architecture) của Intel. Nó cung cấp một số tính năng và công nghệ mới rất cao cấp như: công nghệ siêu ống (hyper-pipelined technology), kênh truyền hệ thống 400Mhz và 533 Mhz (400Mhz - 533Mhz system bus), Bộ nhớ nội cho phép truy cập lệnh thực thi (Execution Trace Cache) và Cơ chế thực thi lệnh nhanh chóng (Rapid Execution Engine). Một số công nghệ và tính năng tăng cường như: Bộ nhớ nội truy cập nhanh cao cấp (Advanced Transfer Cache), Đơn vị xử lý dấu chấm động và truyền thông đa phương tiện được cải tiến (enhanced floating point and multimedia unit) và Bộ lệnh hỗ trợ đồ họa và truyền thông đa phương tiện cấp 2 (Streaming SIMD SSE 2).

Khả năng cung cấp một số công nghệ mới và các tính năng được tăng cường trên đây dựa vào các tiến bộ mới nhất của Intel trong lĩnh vực thiết kế mạch, xử lý việc tiêu thụ năng lượng và các công cụ tính toán không thể thực hiện được ở các mô hình vi kiến trúc ở các thế hệ CPU trước.

->**SSE2** mở rộng tập lệnh MMX để hoạt động trên thanh ghi XMM, cho phép người sử dụng hoàn toàn tránh khỏi việc các thanh ghi MMX 64-bit bị chồng trong các thanh ghi stack dấu chậm đọng chính thức IA-32. Điều này cho phép trộn phần nguyên SIMD với cơ cấu điểm nổi vô hướng mà không có chế độ chuyển đổi giữa

MMX và x87. Tuy nhiên, điều này là over-shadowed giá trị của việc có thể thực hiện các hoạt động MMX trên các thanh ghi SSE lớn hơn.

Những sự bổ sung khác trong SSE2 bao gồm một bộ các lệnh điều khiển bộ nhớ cache nhằm mục đích chủ yếu để giảm thiểu cache pollution khi xử lý dòng thông tin vô hạn định, và một sự bổ sung phức tạp của các lệnh chuyển đổi định dạng số.

SSE 3

Đây là tập lệnh được bổ sung vào năm 2004 là phiên bản thứ 3 của SSE đặt cho kiến trúc IA-32, SSE3 thêm vào 13 câu lệnh mới nhằm giúp các ứng dụng xử lý video và game chạy nhanh hơn và còn hỗ trợ tăng tốc kết nối mạng, đa phương tiện…

Opcode list

Arithmetic:
`addsubpd` - Adds the top two doubles and subtracts the bottom two.
`addsubps` - Adds top singles and subtracts bottom singles.
`haddpd` - Top double is sum of top and bottom, bottom double is sum of second operand's top and bottom.
`haddps` - Horizontal addition of single-precision values.
`hsubpd` - Horizontal subtraction of double-precision values.
`hsubps` - Horizontal subtraction of single-precision values.

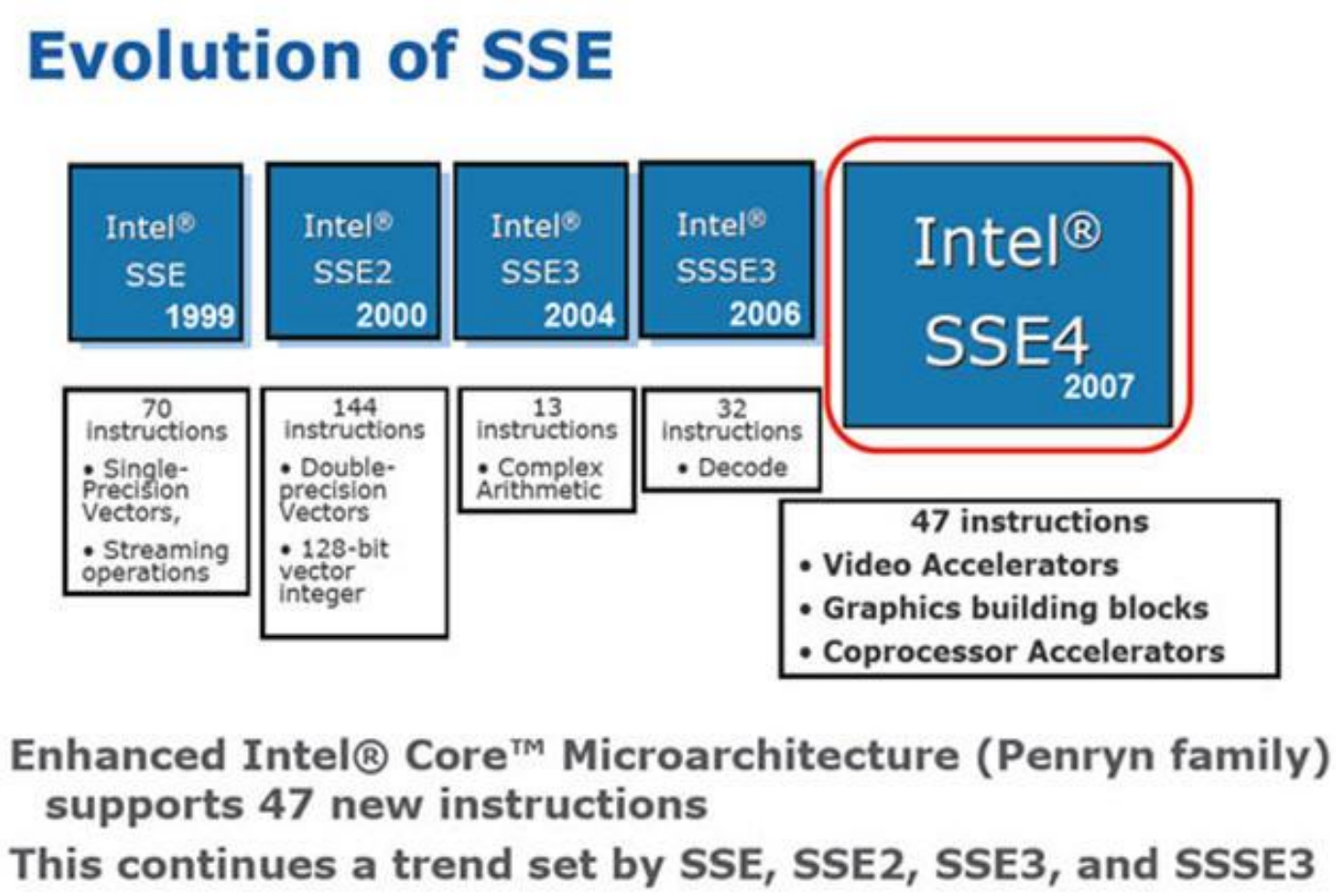
Load/Store:
`lddqu` - Loads an unaligned 128bit value.
`movddup` - Loads 64bits and duplicates it in the top and bottom halves of a 128bit register.
`movshdup` - Duplicates the high singles into high and low singles.
`movsldup` - Duplicates the low singles into high and low singles.
`fisttp` - Converts a floating-point value to an integer using truncation.

Process Control:
`monitor` - Sets up a region to monitor for activity.
`mwait` - Waits until activity happens in a region specified by `monitor`.

SSE 4

Các bộ xử lý Intel thế hệ mới hỗ trợ tập lệnh SSE4.1 bao gồm 47 tập lệnh mới. Tuy nhiên, dù sở hữu một lượng khá lớn các tập lệnh mới, hầu hết trong số này không kết hợp thành một tập logic nào, mà thay vào đó lại bổ sung cho các tập lệnh SIMD

có sẵn. Các tập lệnh mới thông thường sẽ gúp cải thiện hiệu suất hoạt động của các bộ xử lý mới khi làm việc với các dự án đồ họa 3D, truyền phát phim cũng như trong các ứng dụng tính toán khoa học phức tạp.



Tuy vậy, chúng ta sẽ sớm cảm nhận được tác dụng tích cực của việc hỗ trợ các tập lệnh SSE4 mới khi nó trở nên phổ biến rộng rãi trong phần mềm máy tính. Cho tới giờ, chỉ có hai ứng dụng sử dụng đến tập lệnh SSE4, đó là 2 bộ giải mã video: DivX 6.7 và TMPEG Xpress 4.4.

Các đặc trưng chính của các tập lệnh SSE4 bao gồm các tính toán nhân số nguyên 32-bit vector hóa; các tính toán cực đại/cực tiểu 8-bit không dấu; cùng các phiên bản 16-bit và 32-bit có dấu và không dấu; các tính năng giúp cải thiện khả năng của trình biên dịch trong việc vector hóa số nguyên và mã dạng single-precision hiệu quả hơn, bên cạnh đó là các chức năng tăng tốc mã hóa phim; tính toán tích vô hướng điểm trôi và các tập lệnh truyền tải sử dụng các đặc thù của kiến trúc bộ nhớ

đệm trong bộ xử lý.

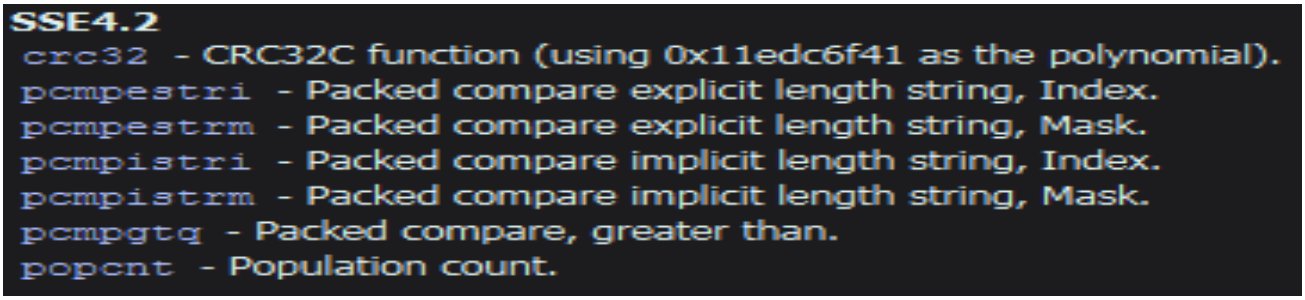
SSE4.1 Instruction summary

Instruction Category	Instructions	Benefits
Packed DWORD Multiplies	PMULLD, PMULDQ	Improved automated compiler vectorization
Floating Point Dot Product	DPPS, DPPD	3D content creation, gaming, support for languages such as CG and HLSL
Multi-packed sum of absolute diffs & min pos	MPSADBW, PHMINPOSUW	Video processing
Packed Blending	BLENDPS, BLENDPD, BLENDVPS, BLENDVPD, PBLENDVB, PBLENDDW	Compiler vectorization and applications such as video processing, multi-media and gaming
Packed Integer Min and Max	PMINSB, PMAXSB, PMINUW, PMAXUW, PMINUD, PMAXUD, PMINDS, PMAXSD	Compiler vectorization and applications such as video processing, multi-media and gaming
Floating Point Round	ROUNDPS, ROUNDSS, ROUNDPD, ROUNDSD	Image processing, graphics, video processing, 2D/3D applications, multimedia, and gaming.
Register Insertion/Extraction	INSERTPS, PINSRB, PINSRD, PINSRQ, EXTRACTPS, PEXTRB, PEXTRD, PEXTRW, PEXTRQ	Compiler vectorization and applications such as video processing, multi-media and gaming
Packed Format Conversion	PMOVSXBW, PMOVZXBW, PMOVSXBD, PMOVZXBD, PMOVSXBQ, PMOVZXBQ, PMOVSXWD, PMOVZXWD, PMOVSXWQ, PMOVZXWQ, PMOVSXDQ, PMOVZXDQ	Compiler vectorization and applications such as video processing, multi-media and gaming
Streaming load	MOVNTDQA	Video processing, imaging, data sharing apps with GPU
Packed Test & Set	PTEST	Compiler vectorization and applications such as video processing, multi-media and gaming
Packed Compare for Equal	PCMPEQQ	Compiler vectorization and applications such as video processing, multi-media and gaming
Pack DWORD to Unsigned WORD	PACKUSDW	Compiler vectorization and applications such as video processing, multi-media and gaming

Một số lệnh trong các SSE4:

SSE4.1

- `mpsadbw` - Sum of absolute differences.
- `phminposuw` - minimum+index extraction (16bit word).
- `pmuldq` - packed multiply.
- `pmulld` - packed multiply.
- `dpps` - dot product, single precision.
- `dppd` - dot product, double precision.
- `blendps` - conditional copy.
- `blendpd` - conditional copy.
- `blendvps` - conditional copy.
- `blendvpd` - conditional copy.
- `pblendvb` - conditional copy.
- `pblendw` - conditional copy.
- `pminsb` - packed minimum signed byte.
- `pmaxsb` - packed maximum signed byte.
- `pminuw` - packed minimum unsigned word.
- `pmaxuw` - packed maximum unsigned word.
- `pminud` - packed minimum unsigned dword.
- `pmaxud` - packed maximum unsigned dword.
- `pminsd` - packed minimum signed dword.
- `pmaxsd` - packed maximum signed dword.
- `roundps` - packed round single precision float to integer.
- `roundss` - scalar round single precision float to integer.
- `roundpd` - packed round double precision float to integer.
- `roundsd` - scalar round double precision float to integer.



EM64T (Extended Memory 64 Technology)

Intel đưa ra thị trường công nghệ 64 bit để cạnh tranh với công nghệ 64 bit của AMD . Công nghệ này gọi là EM64T (Extended Memory 64 Technology) , nó được sử dụng trong Pentium 4 6xx , Pentium 4 5x1 (như 541,551,561 ...) và trêb Celeron D 3x1 và 3x6 (như 331 , 336,341,346 ...).

Bộ vi xử lí sử dụng công nghệ EM64T có một kiểu hoạt động mới gọi là IA32E mà trong đó lại có hai kiểu :

Kiểu tương thích (Compatibility mode) cho phép hệ điều hành 64bit chạy những phần mềm 32 bit và 16 bit . Hệ điều hành 64 bit có thể chạy 64bit và các chương trình ứng dụng 32 bit , 16 bit cùng một lúc. Đối với các chương trình 32 bit CPU sẽ truy cập được 4GB RAM . Chương trình chạy 16 bit sẽ chỉ truy cập được 1MB RAM.

Kiểu 64 bit (64-bit mode) : cho phép hệ thống hoạt động 64 bit có nghĩa là công nghệ này có thể dùng 64 bit địa chỉ .

Công nghệ EM64T có thể sử dụng hệ điều hành 64 bit như Windows64 , có thể dùng hệ điều hành 32 bit như Windows XP lúc này nó sẽ chạy kiểu IA32 thông thường và truy cập được 32 bit địa chỉ - 4GB RAM .

Những đặc điểm của kiểu 64-bit

64-bit địa chỉ có nghĩa là ứng dụng có thể sử dụng 16EB (Exabytes) bộ nhớ (2^64) . Trong khi đó bộ vi xử lí Celeron D , Pentium 4 và Xeon hỗ trợ EM64T chỉ có 36 bit địa chỉ , có nghĩa là chỉ có thể sử dụng được 65GB RAM (2^36) . Xeon DP hỗ trợ EM64T chỉ có 40 đường địa chỉ tức là có thể truy cập bộ nhớ 1TB (2^40) . Giới hạn này sẽ được thay đổi trong tương lai , do đáo trong tương lai Intel sẽ phát hành bộ vi xử lí có thể truy cập bộ nhớ tới 16EB .

Thêm 8 thanh ghi : trong kiểu 64 bit , CPU có tất cả 16 thanh ghi 64 bit . Những thanh ghi mới này có tên là R8 tới R15 . R được hiểu là thanh ghi 64 bit . Hình dưới đây bạn có thể xem thanh ghi 64 bit

Thêm 8 thanh ghi sử dụng cho tập lệnh SIMD (MMX, SSE, SSE2, SSE3) . Trong kiểu EM64T bộ vi xử lí có tất cả 16 thanh ghi MMX 64 bit . Thanh ghi XMM có độ dài 128 bit , số của thành ghi XMM từ 8 lên 16 thanh ghi . Những thanh ghi XMM được sử dụng trong những phép tính dấu phảy động SSE.

Tất cả Register Pointer và Instruction Pointercó độ rộng 64 bit . Thanh ghi trong FPU có độ rộng 80 bit .

Tất cả thanh ghi 64 bit được chia thành những thanh ghi nhỏ 8 bit như hình trên . Sơ đồ như hình trên gọi là “uniform byte-register addressing”.

Sử dụng kỹ thuật Fast interrupt-priorization .

Có Instruction Pointer mới liên quan tới EM64T gọi là địa chỉ RIP-relative .

VT-x

Đây là tập lệnh mở rộng hiệu quả cần thiết phải có trên các vi xử lý của máy chủ, nó giúp chạy được các máy ảo 64bit như các phần mềm Vmware, VirtualBox..; nó còn dùng để chạy Windows server 2008 64bit và Enable Hyper-V, đây là một chức năng quản lý máy ảo như các phần mềm trên.

Intel® VT cho phép một hệ thống máy tính đơn lẻ có thể hoạt động như nhiều hệ thống máy tính “ảo”. Đối với các doanh nghiệp, Intel® VT cung cấp khả năng cải tiến công tác quản lý, hạn chế thời gian chết, duy trì và nâng cao năng suất lao động bằng cách chia tách các hoạt động riêng biệt thành những khu vực hoàn toàn độc lập.

Kết Luận

EM64T hướng tới hệ điều hành 64 bit , lúc này nếu muốn bạn mua Celeron D 64bit , hoặc Pentium 4 64 bit . Nếu bạn có Celeron D 64 bit hoặc Pentium 4 64 bit , Windows 64 và các chương trình phần mềm 32 bit sẽ chạy tốt , nhưng nó sẽ chạy kiểu Compatibility Mode , có nghĩa là bạn sẽ thấy bộ vi xử lí như là Intel IA32 . Nếu bạn sử dụng chương trình nặng và nghĩa rằng phép tính 64 bit để có nhiều hơn

4GB RAM sẵn có thì vấn đề của bạn không được giải quyết . Một điều bạn nên nhớ rằng Bus địa chỉ ngoài của bộ vi xử lí EM64T không phải là 64 bit , do đó CPU của Intel sử dụng công nghệ này không thể truy cập được 16EB RAM (2^64) như bạn nghĩ . Tổng số dung lượng bộ nhớ RAM mà CPU có thể truy cập được là phụ thuộc vào CPU . Celeron D 64 bit , Pentium 4 64 bit và Xeon có thể truy cập được bộ nhớ có dung lương 64GB , Xeon DP truy cập được bộ nhớ có dung lượng 1TB . Một điều bạn cần nhớ là kiểu 32 bit hoặc kiểu 64bit bộ vi xử lí chỉ có thể truy cập được nhiều nhất là 4GB thậm trí cả trong CPU 64bit.

IV.CÁC ĐẶC ĐIỂM CÔNG NGHỆ MỚI

Bộ vi xử lý mới được chế tạo với công nghệ 45nm, bộ nhớ đệm 18MB L2, và có khả năng hỗ trợ tần số khác nhau, từ 1,8 GHz đến lớn hơn 2,6GHz. . Với tính năng Hyper-Threading nổi bật có khả năng xử lí đa luồng và một số tính năng khác như :

- Intel Virtualization (Vt-x)
- Enhanced Intel SpeedStep
- 64 bit
- Execute Disable Bit
- Intel Turbo Boost

1. HyperThreading

Internet , thương mại điện tử và phần mềm ứng dụng doanh nghiệp đang ngày càng đòi hỏi nhiều năng lực tính toán của các máy chủ hơn . Để nâng cao tốc độ, phần mềm cần phải được " phân luồng " - các chỉ thị sẽ được chia thành nhiều dòng lệnh để có thể xử lý đồng thời trên nhiều bộ xử lý. *Intel* đã đưa ra công nghệ " phân luồng " cho phép nâng cao tốc độ và khả năng tính toán song song cho những ứng dụng đa luồng. Công nghệ mới của Intel mô phỏng mỗi bộ vi xử lý vật lý như là hai bộ vi xử lý luận lý (logic) , tài nguyên vật lý được chia sẻ và có cấu trúc chung giống hệt nhau cho cả hai bộ xử lý lôgic . Hệ điều hành và phần mềm ứng dụng sẽ " tưởng " như đang chạy

trên hai hay nhiều bộ xử lý , kết quả là tốc độ xử lý trung bình có thể tăng lên xấp xỉ 40% đối với một bộ xử lý vật lý , Intel gọi công nghệ này là Hyper-Threading (HT - tạm dịch là siêu luồng).

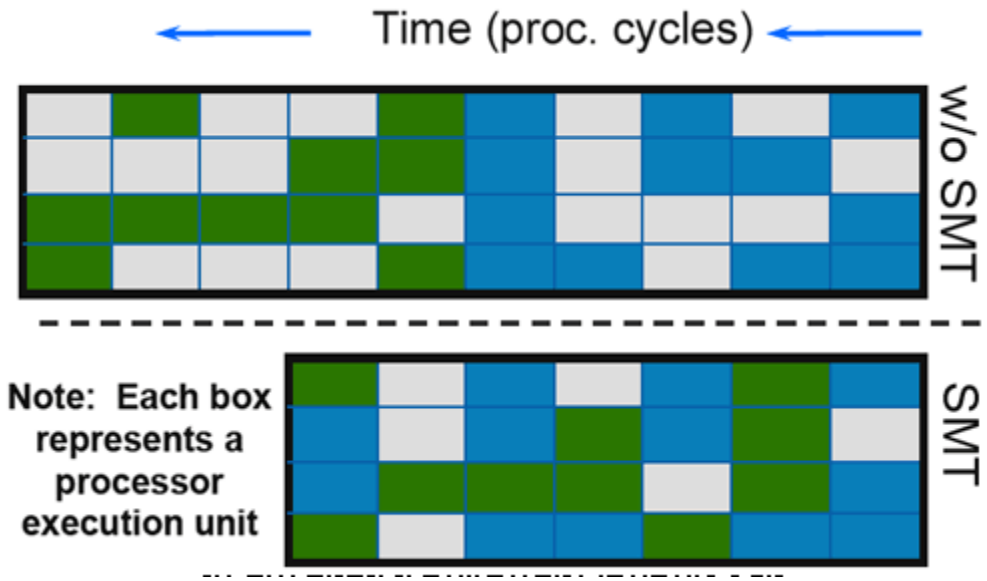
Công nghệ siêu luồng cho phép các phần mềm ứng dụng được viết cho những máy chủ đa luồng có thể thực hiện các chỉ thị song song đồng thời trên mỗi bộ xử lý riêng , bằng cách này sẽ cải thiện tức thì tốc độ giao dịch cũng như thời gian đáp ứng và các yêu cầu đặc thù khác của phần mềm nghiệp vụ và thương mại điện tử . Công nghệ này tương thích với các phần mềm ứng dụng và hệ điều hành sẵn có trên các máy chủ , nó cho phép hỗ trợ nhiều người dùng hơn và tăng khối lượng công việc được xử lý trên một máy chủ . Với các máy trạm cao cấp , công nghệ siêu phân luồng cũng sẽ tăng đáng kể tốc độ các phần mềm ứng dụng đòi hỏi năng lực tính toán cao , ví dụ như phần mềm thiết kế 3 chiều , xử lý ảnh hay video… Trong thời gian tới sẽ xuất hiện ngày càng nhiều phần mềm được thiết kế đặc biệt và tối ưu hoá cho công nghệ này.

Từ tháng 1-2002, công nghệ siêu luồng đã được Intel đưa vào các bộ vi xử lý Xeon đời mới, khởi đầu với các bộ xử lý có tốc độ 1,8GHz và 2,0GHz với 512KB cache thứ cấp , sản xuất bằng công nghệ 0,13 micron (Xeon 1,7GHz, 1,8GHz, 2,0GHz với 256KB cache thứ cấp được sản xuất bằng công nghệ 0,18 không hỗ trợ siêu luồng) . Tại thời điểm đầu tiên khi Intel giới thiệu bộ xử lý Xeon cùng với chipset 860 , chỉ có một số rất ít các nhà sản xuất hàng đầu như IBM,Compaq, Dell, SuperMicro,Tyan… hỗ trợ bộ vi xử lý này, số lượng sản phẩm cũng rất ít. Tuy nhiên tới thời điểm hiện nay, khi có thêm các chipset hỗ trợ bộ xử lý Xeon như E7500 và Serverworks GC, nhiều nhà sản xuất khác đã có sản phẩm hỗ trợ bộ xử lý Xeon. Đặc biệt SuperMicro đã gần như " bỏ rơi " Pentium III với việc cho ra đời tới hơn 20 loại motherboard hỗ trợ bộ xử lý Xeon, chứng tỏ Xeon với công nghệ siêu luồng là sự thay thế xứng đáng .

Tuy nhiên đối với đa số người dùng, nhất là người dùng máy tính để bàn thì công nghệ HT còn khá xa lạ. Bài viết này giúp các bạn hiểu rõ hơn về công

nghệ siêu luồng, nhất là khi Intel chuẩn bị đưa ra bộ xử lý Pentium 4 dành cho desktop áp dụng công nghệ siêu luồng (tốc độ khởi điểm là 3,06GHz).

Công Nghệ Hyper--Threading Và Simultaneous Multi-Threading (Smt)



Minh họa cho cách SMT (Hyper Threading) làm tăng hiệu quả xử lý của CPU

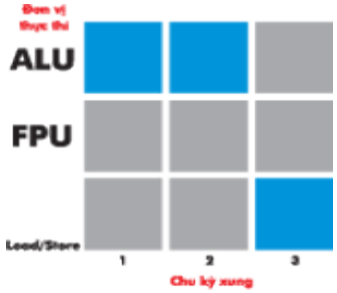
INTEL PHÁT TRIỂN SMT từ một công nghệ gốc có tên mã là Jackson, nó được giới thiệu tại diễn đàn các nhà phát triển Intel Development Forum với một cái tên gần gũi hơn là Hyper-Threading – công nghệ siêu luồng. Trước khi có thể hiểu về cách thức hoạt động của công nghệ này, chúng ta cần phải tìm hiểu cơ bản về nó, đặc biệt là về chuỗi lệnh và cách chúng hoạt động.

Cái gì làm cho một ứng dụng có thể chạy? Làm thế nào CPU biết các chỉ dẫn để thực hiện và thực hiện với dữ liệu nào? Tất cả những thông tin này có chứa trong mã biên dịch của ứng dụng mà bạn đang chạy mỗi khi bạn nạp ứng dụng

đó vào. Ứng dụng lần lượt gửi các chuỗi lệnh báo cho CPU biết phải làm gì để đáp ứng, và đối với CPU chuỗi lệnh sẽ là một tập các chỉ thị cần phải thực thi. CPU biết chính xác các chỉ thị này nằm ở đâu nhờ thanh ghi gọi là Program Counter (PC). PC luôn chỉ đến vị trí trong bộ nhớ nơi mà các chỉ thị cần thực hiện tiếp theo đã được lưu giữ, như vậy một khi chuỗi lệnh được gửi đến CPU thì địa chỉ trong bộ nhớ của chuỗi lệnh này đã được nạp sẵn vào PC, vì vậy CPU biết bắt đầu thực hiện từ đâu. Sau mỗi chỉ thị, PC sẽ tăng lên và quá trình tiếp tục đến hết chuỗi lệnh. Khi chuỗi lệnh được thực hiện xong, PC sẽ bị ghi đè bởi chỉ thị tiếp theo. Chuỗi lệnh có thể bị ngắt bởi một yêu cầu khác, khi đó CPU sẽ lưu giá trị hiện tại của PC trong ngăn xếp (stack) và nạp giá trị mới vào PC, tuy nhiên hạn chế là tại mỗi thời điểm chỉ có thể có duy nhất một chuỗi lệnh được thực thi. Một hướng giải quyết chung cho vấn đề này là sử dụng hai hay nhiều CPU, nếu tại mỗi thời điểm một CPU chỉ có thể thực thi một chuỗi lệnh thì hai hay nhiều CPU sẽ thực thi được hai hay nhiều chuỗi lệnh. Tuy vậy, lại có nhiều vấn đề nảy sinh với cách giải quyết này, trước hết là nhiều CPU sẽ tốn nhiều tiền, quan trọng hơn nữa là việc quản lý hai hay nhiều CPU để chúng chia sẻ tốt tài nguyên chung. Ví dụ, cho tới trước khi chipset AMD 760MP được đưa ra, tất cả các nền tảng x86 đa bộ xử lý chỉ hỗ trợ việc chia băng thông sẵn có giữa các CPU, điều quan trọng nhất là các ứng dụng và hệ điều hành cần phải có khả năng hỗ trợ tính năng này. Hiện nay, để giải quyết nhanh các chuỗi lệnh phức tạp, phần cứng nói chung phải nhờ vào phương án xử lý đa luồng, hệ điều hành phải hỗ trợ xử lý đa luồng, và phải tăng tốc độ một cách thật sự, giống như có nhiều bộ xử lý (trong hầu hết các trường hợp). Công nghệ siêu luồng của Intel giải quyết vấn đề bằng cách thực hiện nhiều hơn một chuỗi lệnh tại cùng một thời điểm.

Các bộ vi xử lý hoạt động không hiệu quả!

Thuật ngữ hiệu quả có vẻ như là một vòng luẩn quẩn, giống như con người chỉ sử dụng một phần nhỏ sức mạnh bộ não của mình, CPU cũng vậy.



Lấy Pentium 4 làm ví dụ, CPU này có tổng cộng 7 đơn vị thực thi, hai trong số đó có thể thực hiện hai vi lệnh mỗi xung nhịp (gọi là double pumped ALUs). Nhưng ngay cả như vậy thì bạn cũng không thể tìm được phần mềm nào tận dụng hết các đơn vị thực thi đó. Hầu hết các phần mềm cho máy tính cá nhân đang sử dụng chỉ làm việc với một ít phép tính số nguyên như nạp và lưu trữ mà không hề động đến đơn vị thực thi dấu chấm động. Còn một số phần mềm kiểu như Maya thì chỉ tập trung vào mỗi đơn vị xử lý dấu chấm động mà không sử dụng đến đơn vị xử lý số nguyên. Ngay cả ứng dụng chủ yếu sử dụng phép tính số nguyên cũng không tận dụng tất cả các đơn vị xử lý số nguyên, đặc biệt là đơn vị xử lý số nguyên "chậm", một thành phần trong CPU chuyên dùng cho phép "dịch chuyển" hay "xoay".

Để minh hoạ rõ hơn hãy thử đặt giả thiết một CPU với 3 đơn vị thực thi: một đơn vị số nguyên, một đơn vị dấu chấm động và một đơn vị nạp/lưu trữ (đơn vị dùng để đọc/ghi bộ nhớ). Giả sử CPU có thể thực hiện mọi lệnh trong vòng một chu kỳ xung nhịp và đồng thời giải quyết nhiều mệnh lệnh tới cả ba đơn vị thực thi. Bây giờ hãy đưa cho CPU một chuỗi lệnh như các chỉ dẫn sau đây:

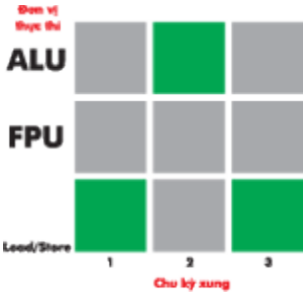
1+1

10+1

Store Previous Result

Biểu đồ dưới đây sẽ giúp minh họa mức độ của các đơn vị thực thi, màu xám biểu thị đơn vị thực thi không sử dụng, màu xanh cho biết đơn vị thực thi hoạt động.

Bạn có thể thấy rằng trong mỗi xung nhịp sẽ chỉ có 33% trong số các đơn vị được sử dụng, và trong các phép toán này hoàn toàn không sử dụng đơn vị xử lý dấu chấm động FPU. Theo Intel thì hầu hết các mã lệnh IA-32 x86 chỉ sử dụng khoảng 35% số các đơn vị thực thi của Pentium 4.



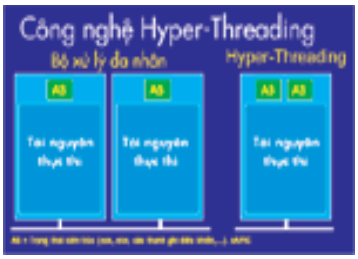
Thử gửi một chuỗi lệnh khác đến các đơn vị thực thi của CPU, lần này là các lệnh tải, cộng và lưu trữ theo thứ tự:

Một lần nữa bạn thấy rằng cũng chỉ sử dụng có 33% số các đơn vị thực thi. Thuật toán xử lý song song mà chúng tôi cố gắng chỉ ra ở đây được gọi là ILP (instruction level parallelism), ở đó các chỉ dẫn phức tạp được thực hiện đồng thời bởi vì CPU có khả năng "điền đầy" các đơn vị xử lý song song, tức là có nhiều hơn 33% số đơn vị xử lý được sử dụng. Đáng tiếc là trên thực tế hầu hết các mã lệnh x86 không phải là ILP, vì vậy bạn phải tìm những cách khác để tăng hiệu quả. Ví dụ, hệ thống của bạn có 2 CPU và chúng có thể thực hiện các chuỗi lệnh đồng thời, cách này được biết đến như là xử lý song song theo luồng để tăng cường hiệu năng, tuy nhiên lại rất tốn kém.

Vậy có cách nào khác để sử dụng tốt hơn sức mạnh thực thi vốn có của bộ xử lý x86?

Giới Thiệu Công Nghệ Hyper---Threading

Có một vài nguyên nhân làm cho các đơn vị thực thi không được sử dụng thường xuyên. Nói chung, CPU không thể lấy dữ liệu nhanh như nó mong muốn do tắc nghẽn đường truyền (memory bus và front-side-bus), dẫn đến sự giảm sút hoạt động của các đơn vị thực thi. Ngoài ra, một nguyên nhân khác đã được đề cập là có quá ít ILP trong hầu hết các chuỗi lệnh thực thi.



Hiện thời cách mà đa số các nhà sản xuất CPU dùng để cải thiện hiệu năng trong các thế hệ CPU của họ là tăng tốc độ xung nhịp và tăng độ lớn của bộ nhớ đệm (cache). Nhưng cho dù cả hai cách này cùng được sử dụng thì vẫn không thực sự sử dụng hết được tiềm năng sẵn có của CPU. Nếu có cách nào đó cho phép thực thi được nhiều chuỗi lệnh đồng thời mới có thể tăng hiệu quả sử dụng tài nguyên của CPU. Đó chính là cái mà công nghệ siêu luồng của Intel đã làm được, bản chất của nó

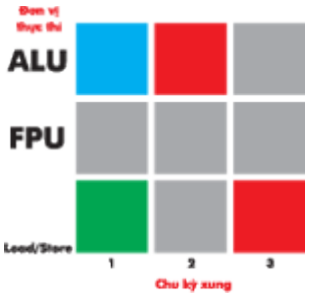
là chia sẻ tài nguyên để sử dụng hiệu quả hơn các đơn vị thực thi lệnh đã có sẵn trên các CPU đó.

Hyper threading - siêu luồng là một cái tên "tiếp thị" cho một công nghệ nằm ngoài "vương quốc" x86, là một phần nhỏ của SMT. Ý tưởng đằng sau SMT rất đơn giản: một CPU vật lý sẽ xuất hiện trên hệ điều hành như là hai CPU và hệ điều hành không thể phân biệt được. Trong cả hai trường hợp nhiệm vụ của hệ điều hành chỉ là gửi hai chuỗi lệnh tới "hai" CPU và phần cứng sẽ đảm nhiệm những công việc còn lại.
Trong các CPU sử dụng công nghệ Hyper-Threading, mỗi CPU logic sở hữu một tập các thanh ghi, kể cả thanh ghi đếm chương trình PC riêng (separate program counter), CPU vật lý sẽ luân phiên các giai đoạn tìm/giải mã giữa hai CPU logic và chỉ cố gắng thực thi những thao tác từ hai chuỗi lệnh đồng thời theo cách hướng tới những đơn vị thực thi ít được sử dụng.

Khi giới thiệu tại diễn đàn các nhà phát triển, công nghệ này được trình diễn trên bộ xử lý Xeon cùng với phần mềm dựng hình (rendering) của Maya, trong thí nghiệm đó một bộ xử lý Xeon với công nghệ siêu luồng đã chạy nhanh hơn 30% so với bộ xử lý Xeon thông thường. Lợi ích về tốc độ ấn tượng đến nỗi chẳng ai buồn để ý rằng thực tế công nghệ này đã có sẵn trên tất cả các lõi (nhân) của CPU Pentium 4 và Xeon, nhưng chỉ đơn giản là đã bị chính Intel vô hiệu hoá. Những ai đã mua CPU Xeon đời mới (0,13 micron) cho các workstation/server nên nâng cấp BIOS và có thể sẽ rất ngạc nhiên với tuỳ chọn thú vị: cho phép hay vô hiệu hoá Hyper-Threading. Hiện tại Intel đang mặc định vô hiệu hoá công nghệ này đối với các CPU dành cho máy tính để bàn, nhưng trong tương lai rất gần nó sẽ được kích hoạt bởi tuỳ chọn đặc biệt trong BIOS của các nhà sản xuất bo mẹ.

Có thể bạn sẽ hỏi rằng tại sao Intel lại mặc định vô hiệu hoá một công nghệ "hay" như vậy, tại sao nó lại không được sử dụng trong tất cả các bộ xử lý mới của Intel? Để có được câu trả lời, chúng ta hãy xem xét kỹ hơn

Hyper----Threading: Không Phải Là Hoàn Hảo



Bạn còn nhớ ví dụ về hai chuỗi lệnh trước đây không? Bây giờ giả thiết rằng CPU đơn giản trước đây của bạn cũng có các đặc tính của Hyper-Threading và hãy xem cái gì sẽ xảy ra khi thực thi đồng thời hai chuỗi lệnh đó:
Những ô màu xanh thẫm hiển thị một chỉ dẫn từ chuỗi lệnh thứ nhất đang được thực hiện, trong khi những ô màu lá cây hiển thị một chỉ dẫn từ chuỗi lệnh thứ hai đang được thực hiện. Các ô màu xám hiển thị những đơn vị thực hiện không được sử dụng, trong khi các ô màu đỏ hiển thị xung đột khi mà cả hai chỉ dẫn đều cố gắng sử dụng cùng một đơn vị thực hiện.

Rõ ràng là không như bạn trông đợi, việc thực hiện song song hai chuỗi lệnh với công nghệ siêu luồng lại thực hiện chậm hơn so với một CPU thông thường. Nguyên nhân thật ra cực kỳ đơn giản: bạn đang cố gắng đồng thời thực hiện hai chuỗi lệnh quá đơn giản, tất cả đều là trùng lặp với lệnh add, load, store. Nếu bạn chạy các ứng dụng đòi hỏi nhiều năng lực tính toán động cùng với các ứng dụng số nguyên thì kết quả sẽ khác đi, vấn đề là bạn sử dụng ứng dụng loại nào nhiều hơn trên máy tính để bàn? Hiện tại các ứng dụng văn phòng trên máy tính để bàn hầu như chỉ sử dụng số nguyên (và trong tương lai chắc cũng vẫn chỉ sử dụng số nguyên). Vì vậy lợi ích mà công nghệ siêu luồng đem lại thấp (và đôi khi còn kém hơn không dùng công nghệ siêu luồng). Trên thực tế, nếu bạn kích hoạt tính năng "siêu luồng" trên máy tính desktop của mình, bạn có thể chẳng được gì ngoại trừ phải trả giá bằng việc giảm tốc độ tới 10%. Tuy nhiên người dùng các ứng dụng tính toán phức tạp (kiểu như rendering của Maya, 3DS) thì sẽ được hưởng lợi rất nhiều từ công nghệ này. Ngoài ra công nghệ này cũng tăng tốc đáng kể cho các máy chủ, nhất là các máy chủ web server.
Bạn có thể tham khảo kết quả khảo sát thử nghiệm của ETesting Labs: *www.intel.com/eBusiness/products/server/processor/Xeon/bm020902.htm.*

Lợi Ích Của Công Nghệ Hyper Threading
Có phải Intel đã tạo ra hyper-threading chỉ để cho các CPU máy chủ? Tất nhiên là không. Intel không định lãng phí bất kỳ không gian trống nào trong CPU của họ, kể cả trong trường hợp này. Thực ra kiến trúc NetBurst của

Pentium 4 và Xeon hiện nay hoàn chỉnh với lõi SMT. Hãy quay trở lại ví dụ trước đây, giờ bạn cho nó thêm một đơn vị thực hiện - một ALU thứ 2 và thực hiện hai chuỗi lệnh trên:

Ái chà! Với một ALU thứ 2, xung đột duy nhất mà bạn gặp phải là lần lưu trữ cuối cùng. Bạn nên biết rằng CPU Pentium 4 được thiết kế với ba đơn vị số nguyên (hai ALU và một đơn vị xử lý số nguyên khác chậm hơn cho phép dịch/xoay). Quan trọng hơn nữa là mỗi ALU của Pentium 4 có thể thực hiện hai vi lệnh trong cùng một xung nhịp, nghĩa là trong hai chỉ dẫn add (phép cộng) mỗi chỉ dẫn có thể từ hai chuỗi lệnh khác nhau, được thực hiện đồng thời trong một xung nhịp duy nhất trên Pentium 4/Xeon.

Nhưng điều đó vẫn chưa giải quyết được vấn đề của bạn, cho thấy rằng việc tăng thêm các đơn vị xử lý để tăng hiệu quả với công nghệ siêu luồng lại tốn kém đứng từ quan điểm vật lý (sẽ phải làm cho CPU phình to ra với nhiều transistor hơn, tiêu tốn nhiều điện năng hơn; hoặc phải giảm kích thước CPU với các công nghệ chế tạo mới). Thay vào đó, Intel đang khuyến khích các nhà phát triển tối ưu hoá công nghệ Hyper-Threading. Chẳng hạn sử dụng lệnh "dừng" (HALT) một trong các bộ xử lý logic, như vậy sẽ tối đa được tốc độ cho các ứng dụng không sử dụng được công nghệ Hyper-Threading, CPU còn lại chỉ hoạt động như là hệ thống một CPU. Khi một ứng dụng có thể sử dụng lợi ích từ Hyper-Threading, bộ xử lý logic thứ hai lại tiếp tục được hoạt động.

Kết-luận

Mặc dù bạn cảm thấy rất bị thuyết phục khi công nghệ Hyper Threading hiện diện trên tất cả các nhân của CPU Pentium 4/Xeon hiện nay, nhưng nó không phải là tất cả những gì bạn mong muốn. Lý do đơn giản là công nghệ thường ở phía trước rất xa, trước khi người dùng có thể nhìn thấy được ưu điểm của nó trên các nền tảng, kể cả máy tính để bàn. Sự hỗ trợ của nhà phát triển rõ ràng có thể mở ra một hướng phát triển mạnh cho Pentium 4/Xeon và các bộ xử lý trong tương lai.

Dù còn nhiều hạn chế, Hyper Threading cũng đã làm được nhiều điều cho thị trường trước khi một bộ xử lý khác của AMD với hai nhân (dual-core) có tên gọi là Sledge Hammer ra đời. Cho tới khi những công nghệ mới như Bumpless Build-Up Layer Packaging hoàn thiện, chi phí để sản xuất CPU nhiều nhân có thể sẽ quá cao do sự phức tạp của công nghệ. Tuy nhiên bộ xử lý nhiều nhân hơn chắc chắn sẽ cho tốc độ cao hơn, vì trên thực tế chúng có nhiều đơn vị thực hiện hơn, tránh được những vấn đề mà hyper-threading đang gặp phải.

Trước mắt, bạn hãy tạm hài lòng với Hyper-Threading và chờ xem bao giờ thì Intel sẽ quyết định đưa các công nghệ này vào bộ xử lý cho máy để bàn.

2) Enhanced Intel SpeedStep

Ngoài EIST được phát triển trước đó thì hiện nay Intel còn có công nghệ Enhanced Halt State (C1E). Về mặt lợi ích thì hai cái này đều giống nhau là nhằm giảm tải điện năng cho CPU, giảm độ ồn cho hệ thống. Tuy nhiên sẽ có rất nhiều người phân vân khác biệt giữa hai cái này là gì ? Xin giải thích như sau :

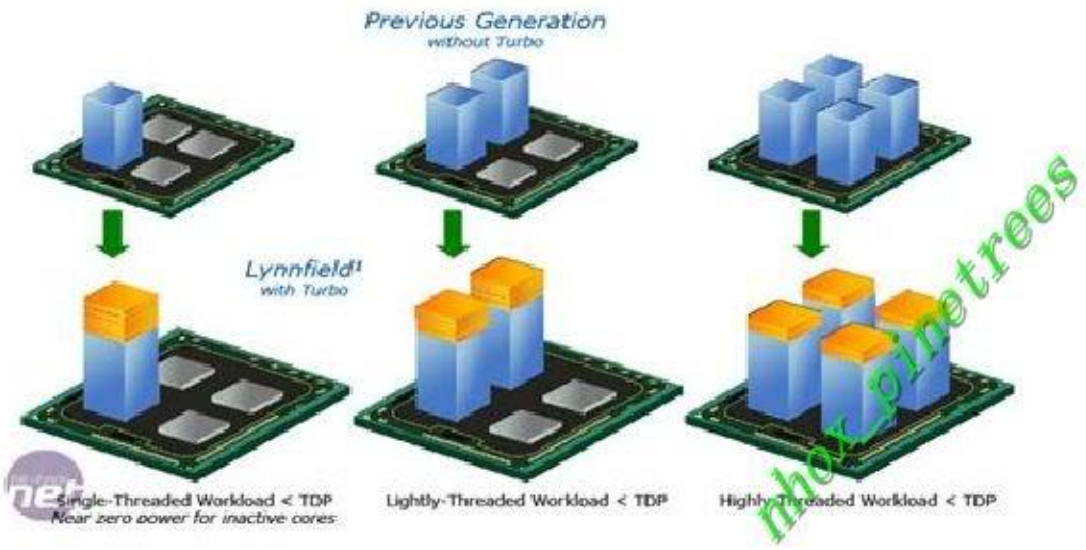
- Cái Enhanced Halt State (C1E) nó có tác dụng thay đổi Clock Ratio và down vCore của CPU xuống. Khi bật cái C1E này trong BIOS thì CPU nó tự động giảm Clock Ratio và vCore những lúc máy idle và tăng Clock Ratio - vCore CPU khi fulload và việc này nó được điều khiển tự động bởi mạch điều khiển trong CPU.
- Còn cái Enhanced Intel SpeedStep Technology (EIST) kia là thay đổi FSB và thay đổi vCore của CPU thông qua việc điều chỉnh BIOS hoặc bằng phần mềm (ở đây chính là OS).
  EIST nó không giảm Multiplier mà chỉ giảm FSB mà thôi, EIST này đã trải qua rất nhiều version khác nhau, từ V1.1 đến hiện nay là V3.2.
  Trước đây, với V2.2 và ở vi xử lý Pentium 4-Mobile thì EIST này có thể thay đổi được cả Multiplier nhưng hiện nay ở các version sau này thì EIST chỉ có tác dụng thay đổi FSB mà không thay đổi Multiplier (nhường công việc thay đổi Multiplier cho C1E).
- Về bản chất thì cái C1E kia nó được điều khiển bởi một mạch tích hợp điều khiển logic trong con CPU và hoạt động thông qua việc xử lý của hệ điều hành và các ứng dụng được chạy, hiểu đơn giản là khi idle và fulload thì nó tự động giảm hay tăng vCore cũng như tăng hay giảm Multiplier.

Hai thằng này về tính năng thì giống nhau nhưng nguyên lý hoạt động thì khác nhau cơ bản ở chỗ 1 thằng thì tự động, còn một thằng thì phải tùy chỉnh.

- Đối với AMD thì sao, họ cũng phát triển được công nghệ tiết kiệm điện như của Intel nhưng được mang tên Cool'n'Quiet, hiện đã phát triển đến version 3.0, cá nhân nhận thấy thì hai thằng này đều có ưu điểm như nhau. Có rất nhiều bạn sẽ thắc mắc rằng làm sao bật cái Cool'n'Quiet này lên thì mình cũng hướng dẫn luôn vậy .

3- Intel Turbo Boost

Turbo Boost là công nghệ nâng hiệu suất máy tính lên thêm 20%, giúp hệ thống hoạt động nhanh hơn và kéo dài thời lượng pin, bằng cách tự động điều chỉnh xung nhịp của từng nhân độc lập cho phù hợp với nhu cầu xử lý.



Công nghệ Turbo boost tự động điều chỉnh xung nhịp từng nhân độc lập cho phù hợp với nhu cầu xử lý. Công nghệ này sẽ nâng cao hiệu suất cho bộ xử lý. Đồng thời giúp kéo dài thời gian sử dụng pin bằng cách giảm xung nhịp của CPU khi Laptop chạy các ứng dụng không cần nhiều tính toán của CPU. Công nghệ siêu phân luồng (Hyper Threading) cho phép cung cấp 2 luồng trên mỗi nhân. Như vậy có thể tăng gấp đôi số tác vụ mà bộ vi xử lý có thể thực thi. Những ai thường xuyên sử dụng 3Ds max để render (diễn hoạt) phim hoạt hình đều ấn tượng bởi công nghệ này.

4 - 64 bit

Tháng 5/2005, Microsoft giới thiệu Windows XP Professional x64 Edition. Cuối 2006, Vista 32 bit và 64 bit cùng được công bố. Khi đó, các hệ thống 64 bit bắt đầu được chú ý và máy tính cũng dần được trang bị RAM trên 3 GB.

Có thể hiểu đơn giản rằng 32 và 64 là số bit mà máy tính có thể xử lý trong một phép điện toán. Chúng cũng có thể chuyển đổi thành số bộ nhớ truy cập ngẫu nhiên (RAM) mà hệ thống có khả năng quản lý.

Hệ thống Windows 32 bit có thể khai thác tối đa 4 GB RAM trong khi 64 bit đạt tới 128 GB, thậm chí cao hơn (về lý thuyết, ứng dụng 64 bit có thể tận dụng 16 tỷ GB RAM). Số bit cao đồng nghĩa với khả năng tính toán nhiều và chính xác hơn.

Dù hứa hẹn tiềm năng như vậy, quá trình chuyển đổi sang nền tảng mới vẫn diễn ra chậm chạp, một phần vì giá RAM còn khá cao cùng sự thiếu hụt trình điều khiển (driver) và ứng dụng 64 bit. (Driver là một dạng phần mềm cho phép các bộ phận phần cứng trong máy có thể hoạt động với hệ điều hành. Chẳng hạn, thiếu driver âm thanh, máy tính không thể phát nhạc).

Vào thời điểm Vista xuất hiện, RAM 2 GB có giá vài trăm USD. Ứng dụng 64 bit chỉ là vài bản game demo và đa số nhà sản xuất phần cứng không cung cấp driver 64 bit. Một lý do quan trọng khác là điện toán 32 bit đủ làm hài lòng đa số người sử dụng trong việc thực hiện các tác vụ thường nhật.

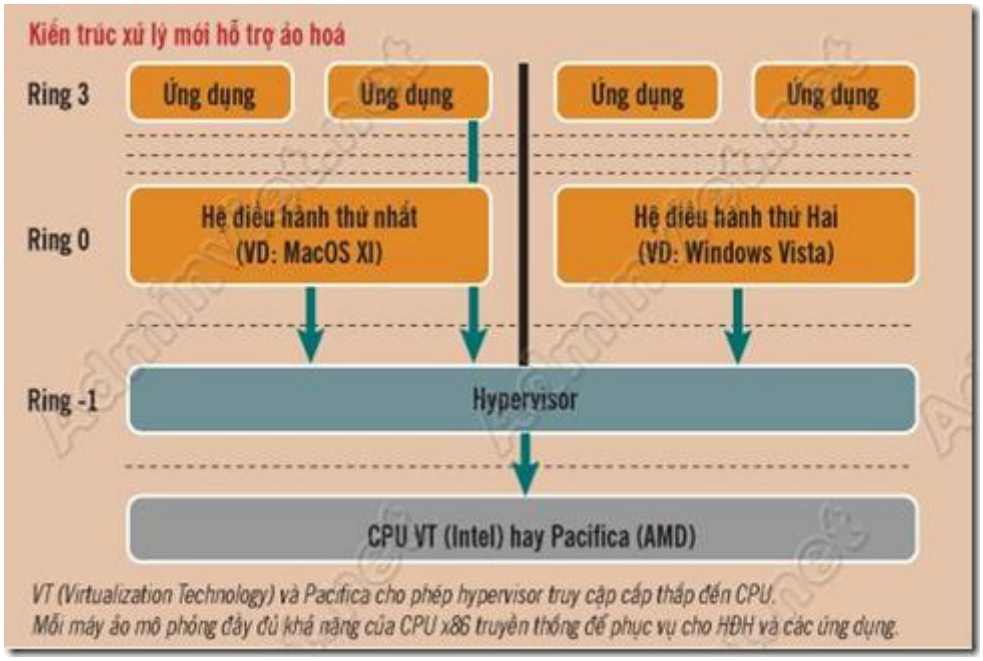
Tiện lợi : Tận dụng bộ nhớ: Giá RAM ngày càng rẻ và máy tính đang được trang bị bộ nhớ lớn hơn, cách duy nhất để khai thác hết khả năng của nó là chuyển sang Windows 64 bit. Thời gian tới, máy tính với RAM trên 4 GB sẽ đều được cài sẵn Windows 64 bit.

Khả năng tương thích: Đa số ứng dụng phần mềm 32 bit (trừ driver) có thể hoạt động trên Windows 64 bit.

Trải nghiệm tốt hơn: Sử dụng Windows 64 bit, các phần mềm, đặc biệt là game và chương trình đồ họa/đa phương tiện, sẽ đạt hiệu suất mạnh mẽ hơn.

5 - Intel Virtualization (Vt-x)

Ảo hóa là kỹ thuật cho phép các tài nguyên điện toán có thể được sử dụng, luân chuyển và phân bố một cách năng động trong nhiều môi trường hệ điều hành khác nhau, cho phép một nền tảng phần cứng có thể hoạt động như nhiều nền tảng ảo khác. Ảo hóa đem đến cho người dùng sự tiện lợi như chạy nhiều hệ điều hành đồng thời không chỉ trên máy tính cá nhân mà tiến sang máy chủ và hệ thống mạng.



Với tốc độ tăng trưởng dữ liệu mỗi năm là 60%, kéo theo nhu cầu lưu trữ tăng, thì công nghệ ảo hóa dành cho trung tâm dữ liệu là giải pháp hữu hiệu không thể bỏ qua.

Ảo hóa có khả năng cho phép khai thác triệt để nguồn lực của server (server thường có thời gian "rỗi" chứ không vận hành liên tục với 100% hiệu suất). 2 giải pháp được nhắc tới nhiều là ảo hóa cứng và ảo hóa mềm.

Ảo hóa cứng là "phân thân" server tạo nhiều máy ảo trên 1 server vật lý (là cách mà Intel đang sử dụng), mỗi máy ảo chạy hệ điều hành riêng, dung lượng lưu trữ và băng thông mạng…cho phép hợp nhất các hệ thống server cồng kềnh. Còn ảo hóa mềm là sử dụng bản sao của một hệ điều hành để tạo các server ảo ngay trên hệ điều hành đó.

Ưu điểm lớn nhất của công nghệ ảo hóa là tiết kiệm nguồn lực và chi phí. Cụ thể, tiết kiệm diện tích sàn để máy chủ và chi phí năng lượng duy trì hệ thống. Đơn cử, trước năm 2004, để duy trì 6 máy chủ thì tiêu tốn mất 48Kw, sau khi hoàn thành ảo hóa máy chủ, con số này giảm xuống chỉ còn 6Kw. 81% khách hàng của Intel rất hài lòng với hiệu năng này.

6 - Execute Disable Bit

Các PC hoạt động dưới hệ điều hành Windows đều có cùng một mức bảo vệ giống với mức bảo vệ được sử dụng bởi các máy chủ hiệu suất cao. Công nghệ này – được biết đến dưới các tên khác nhau ứng với mỗi nhà sản xuất,cho phép bản thân bộ vi xử lý có thể phát hiện khi có mã độc (chẳng hạn như virus hoặc Trojan horse) và tự động vô hiệu hóa mã đó.

Công nghệ này làm việc bằng cách tạo ra vùng riêng để thực thi các chương trình và cho việc lưu trữ dữ liệu trong bộ nhớ RAM của máy tính, nếu một mã nào đó trong vùng đã được thiết lập dự trữ cho việc lưu trữ dữ liệu lại cố gắng chạy thì bộ vi xử lý sẽ cho rằng đó là mã độc và sẽ ngăn chặn sự thực thi của mã đó.

Bạn cần phải chú ý rằng, bản thân bộ vi xử lý không hề có được khả năng loại trừ virus từ máy tính. Nếu một PC nào sử dụng công nghệ NX bị nhiễm virus thì bộ vi xử lý sẽ cảnh báo cho bạn (thông qua hệ điều hành) rằng máy tính của bạn có thể bị nhiễm virus và sẽ không cho virus đó hoạt động, tuy nhiên bạn vẫn phải chạy một chương trình chống virus để loại bỏ virus đó khỏi máy tính và tránh làm lây nhiễm đến người khác (ví dụ trong trường hợp khi bạn gửi email với các file đính kèm) .

Để có được mức bảo mật này trong máy tính bạn cần phải có 3 điều kiện tiên quyết sau. Điều kiện thứ nhất là bộ vi xử lý của bạn phải có công nghệ bảo mật này. Thứ hai là hệ điều hành của bạn phải có khả năng nhận ra nó và thứ ba là nó phải được kích hoạt trong hệ điều hành.