HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

BÀI GIẢNG MÔN

KỸ THUẬT VI XỬ LÝ

CHƯƠNG 7 – CÁC VI XỬ LÝ VÀ CÔNG NGHỆ TIÊN TIẾN

Giảng viên: Vũ Hoài Nam

Điện thoại/E-mail: namvh@ptit.edu.vn

Bộ môn: Khoa học máy tính - Khoa CNTT1

Lecture note link

- http://www.travelvisatousa.com/cntt.ptit/vxl/

NỘI DUNG

1. Các vi xử lý tiên tiến
   - Các vi xử lý họ Intel Pentium
   - Các vi xử lý họ Intel Atom
   - Các vi xử lý họ Intel Core và Core 2
   - Các vi xử lý họ Intel Xeon
   - Các vi xử lý họ Intel Core i3, i5, i7
   - Các vi xử lý họ AMD A-Series
2. Các công nghệ tiên tiến
   - Công nghệ Intel Centrino
   - Các tập lệnh tiên tiến MMX, SSE, AES và AVX
   - Công nghệ thực thi không theo trật tự (Out Of Order Execution)
   - Công nghệ cache thông minh (Advanced Smart Cache)
   - Công nghệ tiết kiệm điện (SpeedStep)
   - Công nghệ siêu phân luồng (Hyper Threading)
   - Công nghệ ảo hóa (Virtualization)

7.1.1 Các VXL họ Intel Pentium

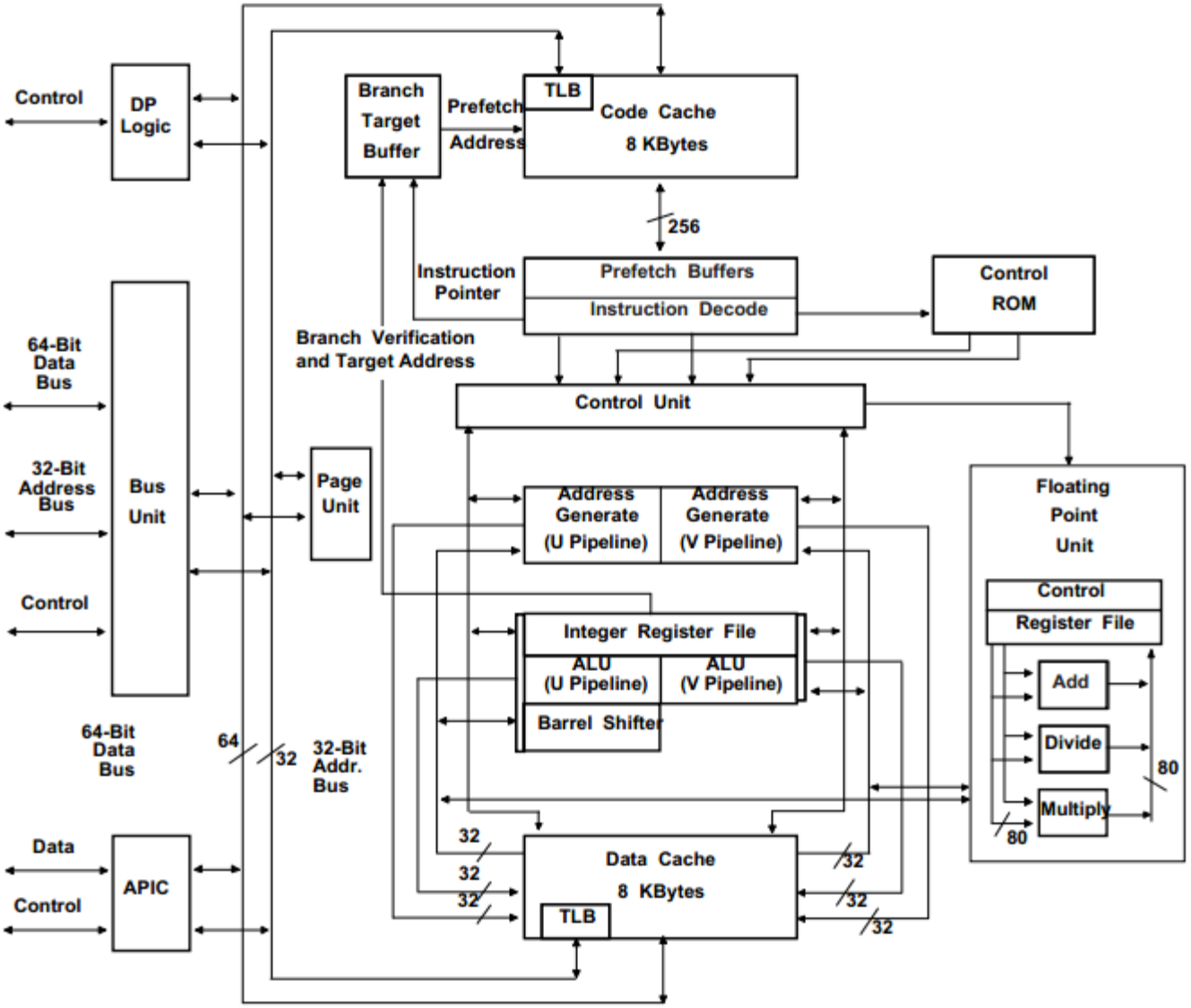
- Intel Pentium I (1993)
- Intel Pentium II (1997)
- Intel Pentium III (1999)
- Intel Pentium IV (2000)
- Intel Pentium M (2002)

7.1.1 Các VXL họ Intel Pentium – Pentium I

- Hỗ trợ 2 ống lệnh (2 lệnh/1CLK):
  - u-pipe: Có thể thực hiện mọi lệnh
  - v-pipe: chỉ t.hiện các lệnh đơn giản;
- Tích hợp 8KB cache L1 cho mã lệnh và 8KB cache L1 cho dữ liệu;
- Tích hợp khả năng dự đoán rẽ nhánh;
- Đường dữ liệu trong 128 và 256 bits;
- Bus dữ liệu ngoài có thể tăng lên 64 bits;
- Hỗ trợ công nghệ MMX (sử dụng SIMD).

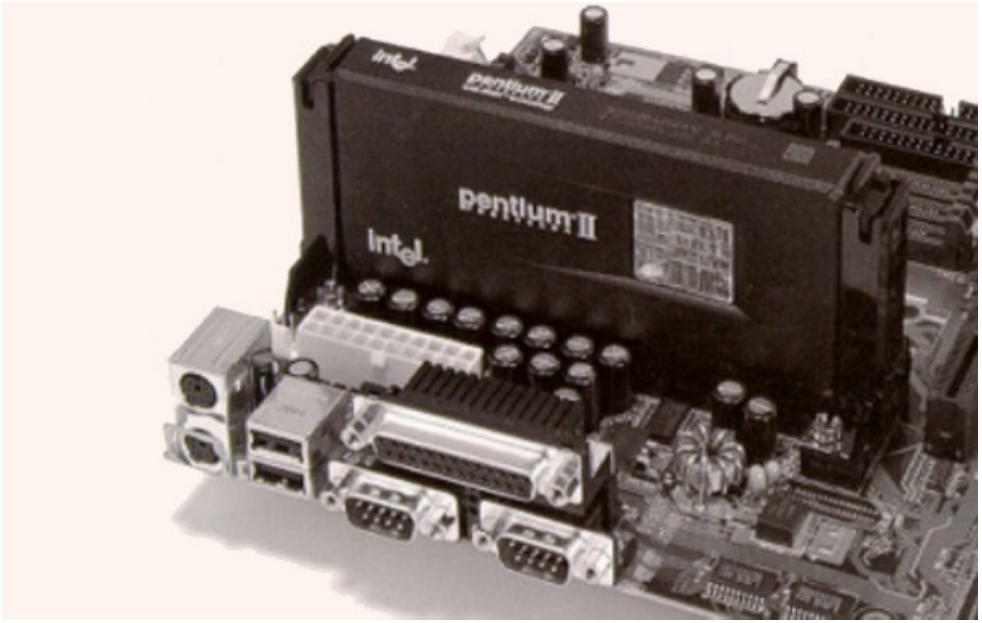
7.1.1 Các VXL họ Intel Pentium – Pentium I

Sơ đồ khối của Intel Pentium I



7.1.1 Các VXL họ Intel Pentium – Pentium II

- Hỗ trợ công nghệ MMX cải tiến;
- Tích hợp 16KB cache L1 cho mã lệnh và 16KB cache L1 cho dữ liệu;
- Tích hợp cache L2 với nhiều lựa chọn: 256, 512 và 1MB;
- Hỗ trợ tính năng quản lý nguồn nâng cao;
- Sử dụng khe cắm kiểu Slot 1.

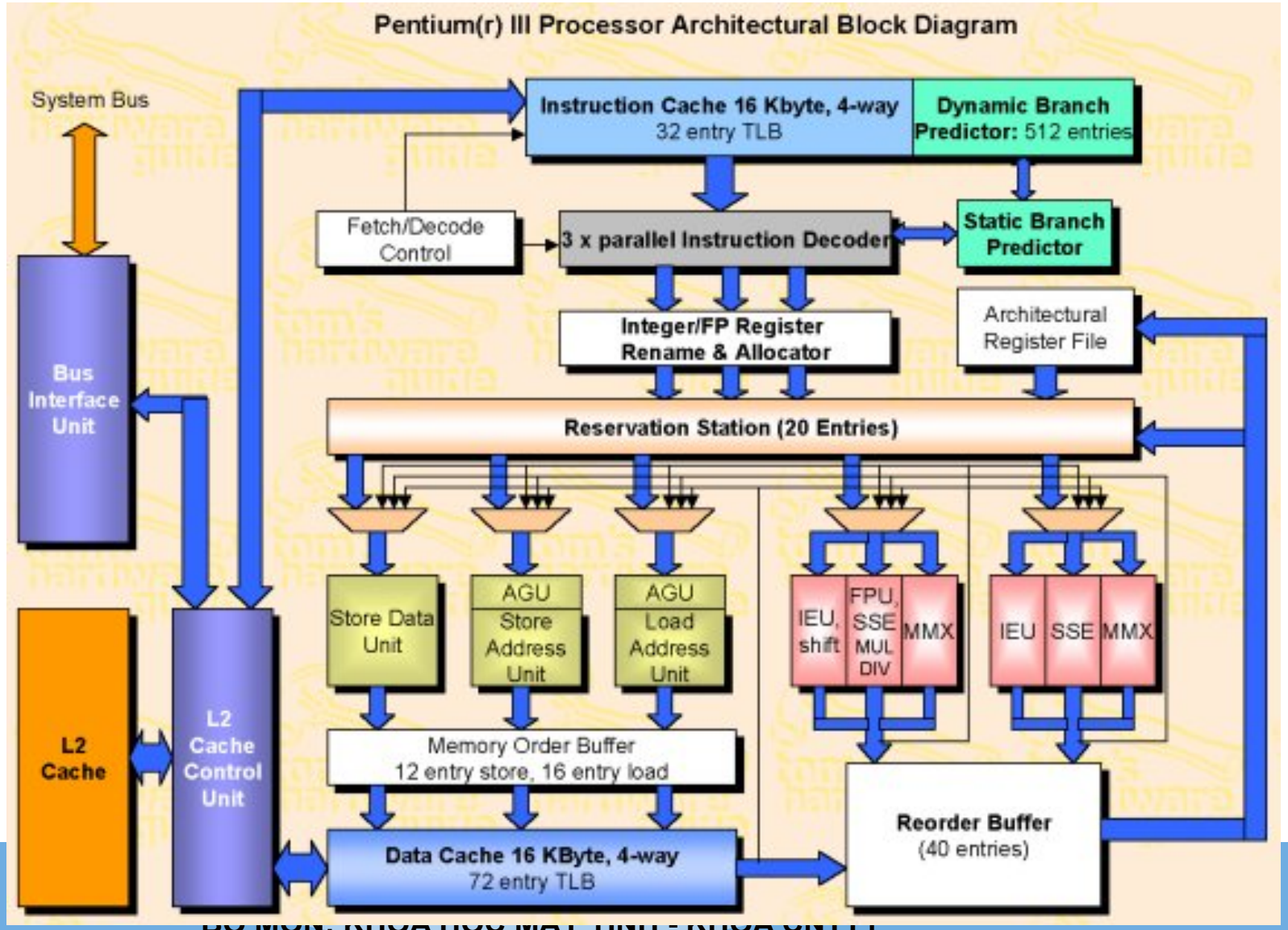


7.1.1 Các VXL họ Intel Pentium – Pentium III

- Giới thiệu tập lệnh SSE (Streaming SIMD Extensions):
  - Hỗ trợ tập các thanh ghi XMM 128 bit
  - Tăng tốc các lệnh đồ hoạ 3D
- Tần số làm việc từ 450MHz – 1.4GHz;
- Tích hợp 2 mức cache;
- Sử dụng khe cắm kiểu Socket 370.

7.1.1 Các VXL họ Intel Pentium – Pentium III

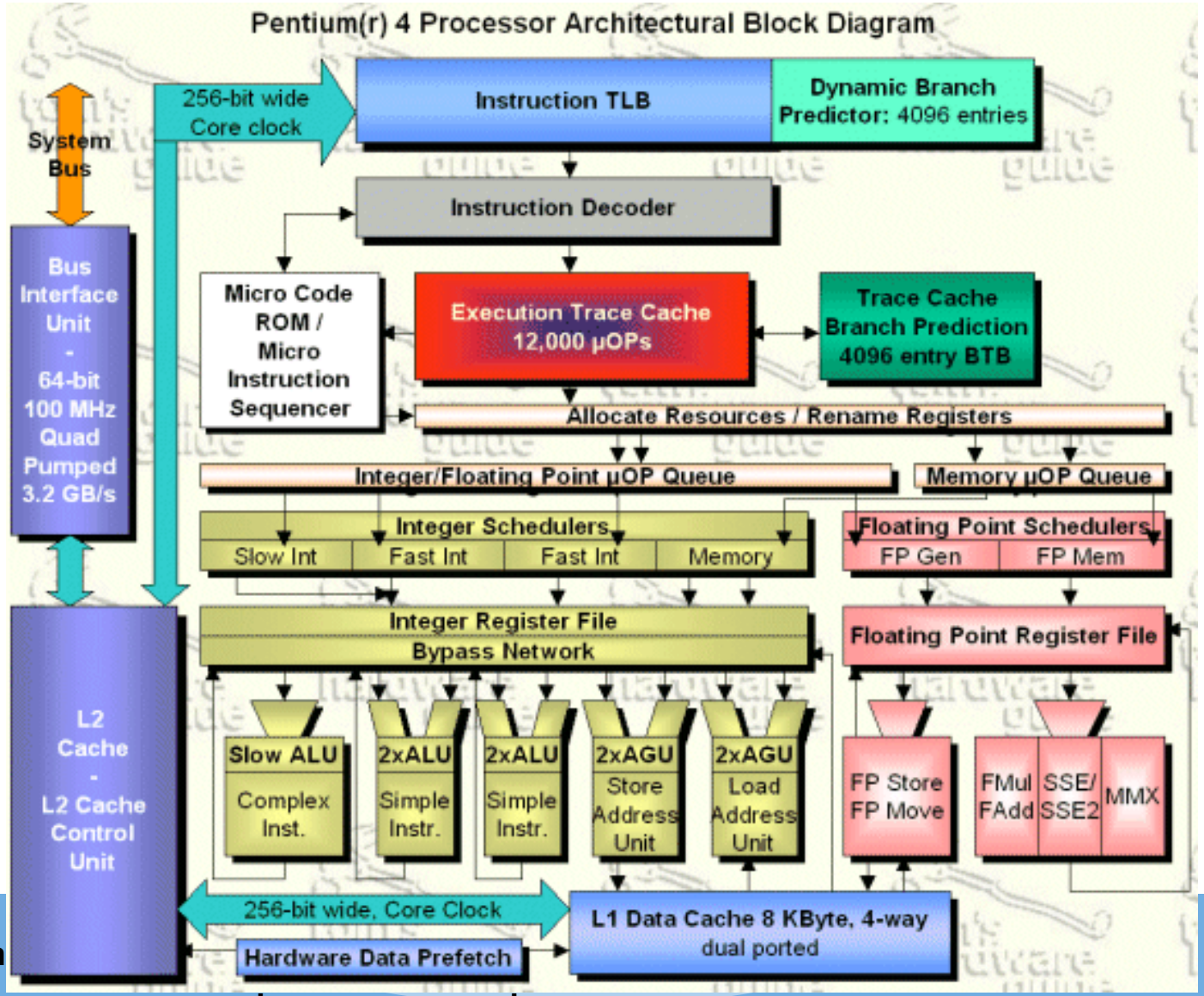
Sơ đồ khối của Intel Pen III



7.1.1 Các VXL họ Intel Pentium – Pentium IV

- Dựa trên vi kiến trúc Intel NetBurst;
- Cache lệnh L1 được chuyển thành Execution Trace Cache;
- Hỗ trợ các tập lệnh tiên tiến MMX, SSE, SSE2, SSE3;
- Một số phiên bản Pentium 4 mới hỗ trợ công nghệ siêu phân luồng (hyper-threading);
- Các phiên bản Pentium 4 662 và 672 hỗ trợ công nghệ ảo hoá (Virtualization Technology).

7.1.1 Các VXL họ Intel Pentium – Pentium IV



7.1.1 Các VXL họ Intel Pentium – Pentium IV

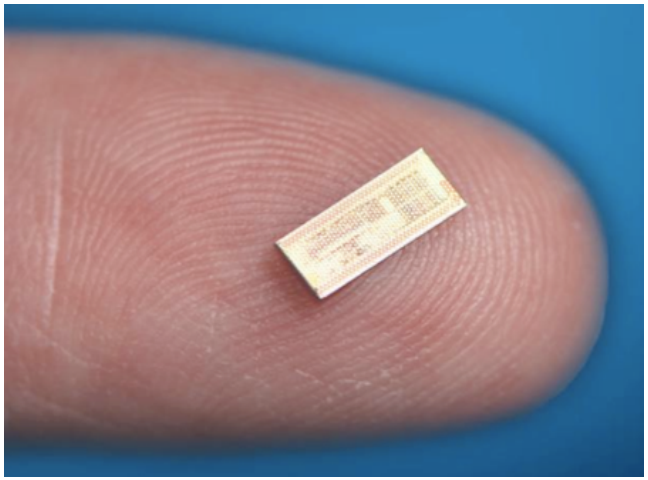
- Execution Trace Cache:
  - Thông thường cache lệnh L1 (L1 I-Cache) được đặt trược bộ giải mã: cung cấp lệnh cho bộ tìm nạp và giải mã;
  - Pentium 4 chuyển cache lệnh L1 thành Execution Trace Cache và đặc sau bộ giải mã;
  - Execution Trace Cache có thể lưu 12.000 vi lệnh đã giải mã;
  - Với các lệnh được thực hiện nhiều lần (các lệnh thuộc vòng lặp):
    - Chúng được giải mã 1 lần thành các vi lệnh và nạp vào Execution Trace Cache;
    - Khi cần thực hiện, các vi lệnh đã giải mã lưu trong Execution Trace Cache được chuyển thẳng đến các khối thực hiện.
- Cache thông thường: mỗi lệnh luôn phải giải mã trước khi thực hiện.

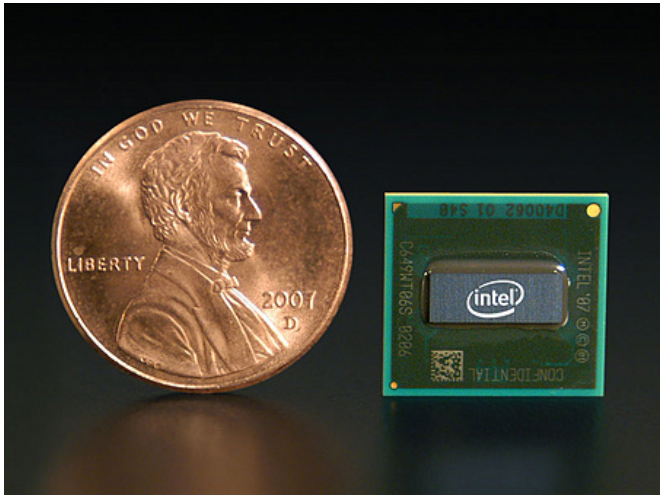
7.1.1 Các VXL họ Intel Pentium – Pentium M

- Là VXL được thiết kế cho các máy tính xách tay: tiêu thụ điện năng thấp, hiệu năng cao;
- Các tính năng tiên tiến của Pentium M:
  - Thực thi động (Dynamic execution)
  - On-chip 32K data L1 cache, 32K instruction L1 cache
  - On-chip L2 cache - đến 1-2MB (rất lớn so với Pen 4: 512K-1MB cùng thời điểm)
  - Advanced Branch Prediction and Data Prefetch Logic
  - Hỗ trợ các tập lệnh MMX, SSE và SSE2
  - Công nghệ quản lý nguồn tiên tiến Intel Enhanced Speedstep.

7.1.2 Các VXL họ Intel Atom

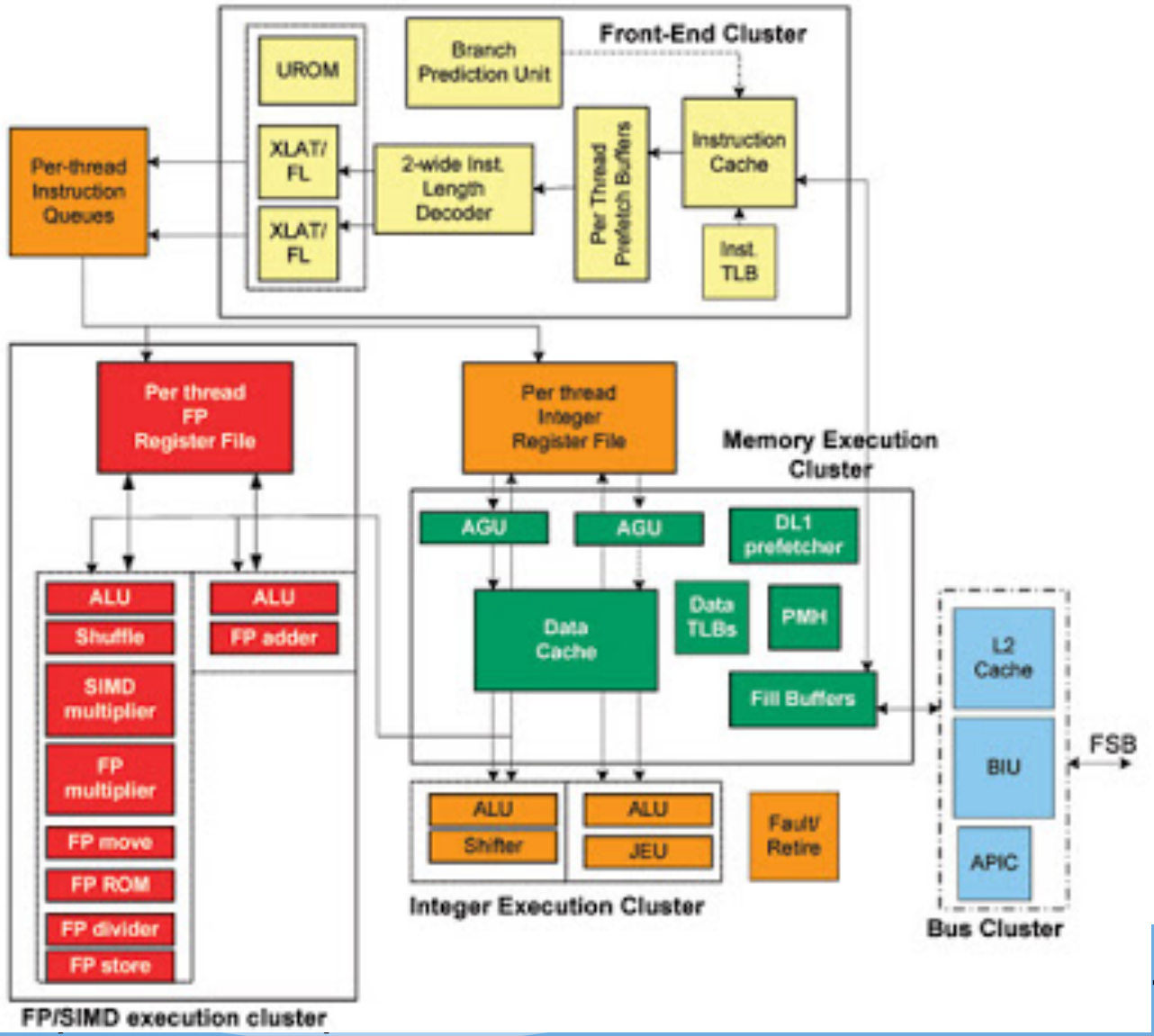
- Dựa trên vi kiến trúc Atom và công nghệ 45nm.
- Vi kiến trúc Atom tối ưu hoá cho các thiết bị có kích thước nhỏ và tiêu thụ ít năng lượng
- Các đặc điểm tiên tiến:
  - Enhanced SpeedStep Technology
  - Deep Power Down Technology with Dynamic Cache Sizing
  - Intel Virutalization Technology
  - Intel 64 architechure.





7.1.2 Các VXL họ Intel Atom

Sơ đồ khối của Intel Atom

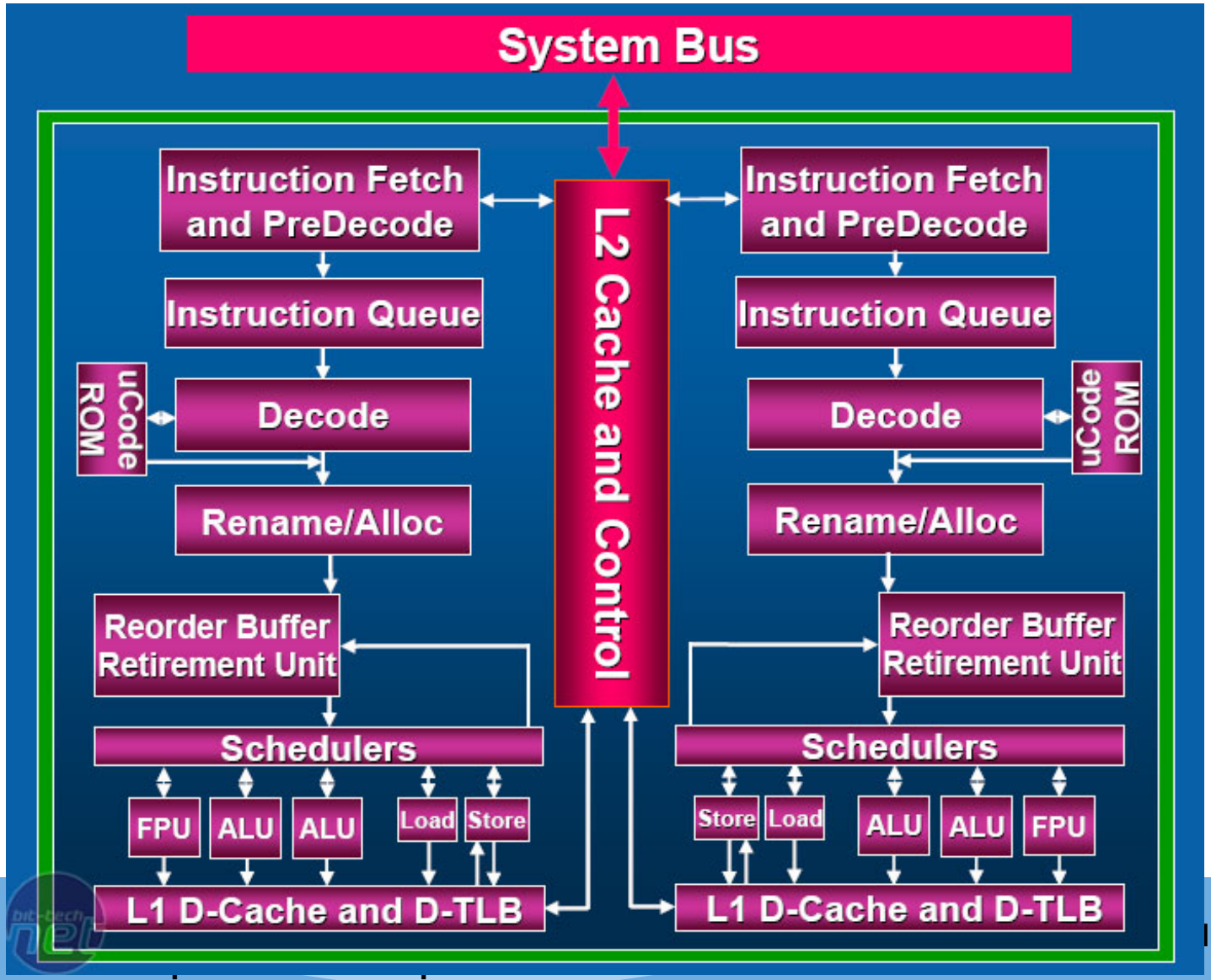


7.1.3 Các VXL họ Intel Core và Core 2

- Vi kiến trúc Core và Core 2 được thiết kế dựa trên Pentium M;
- Core 2 về cơ bản giống Core, nhưng dung lượng cache L2 lớn hơn (2MB so với 1MB của Core).
- Các tính năng tiên tiến:
  - Smart Cache cho phép chia sẻ dữ liệu giữa 2 nhân
  - Cải tiến pha giải mã và thực hiện các lệnh SIMD
  - Các công nghệ giảm tiêu hao điện: Dynamic Power Coordination và Enhanced Intel Deeper Sleep
  - Intel Advanced Thermal Manager sử dụng các sensor số.

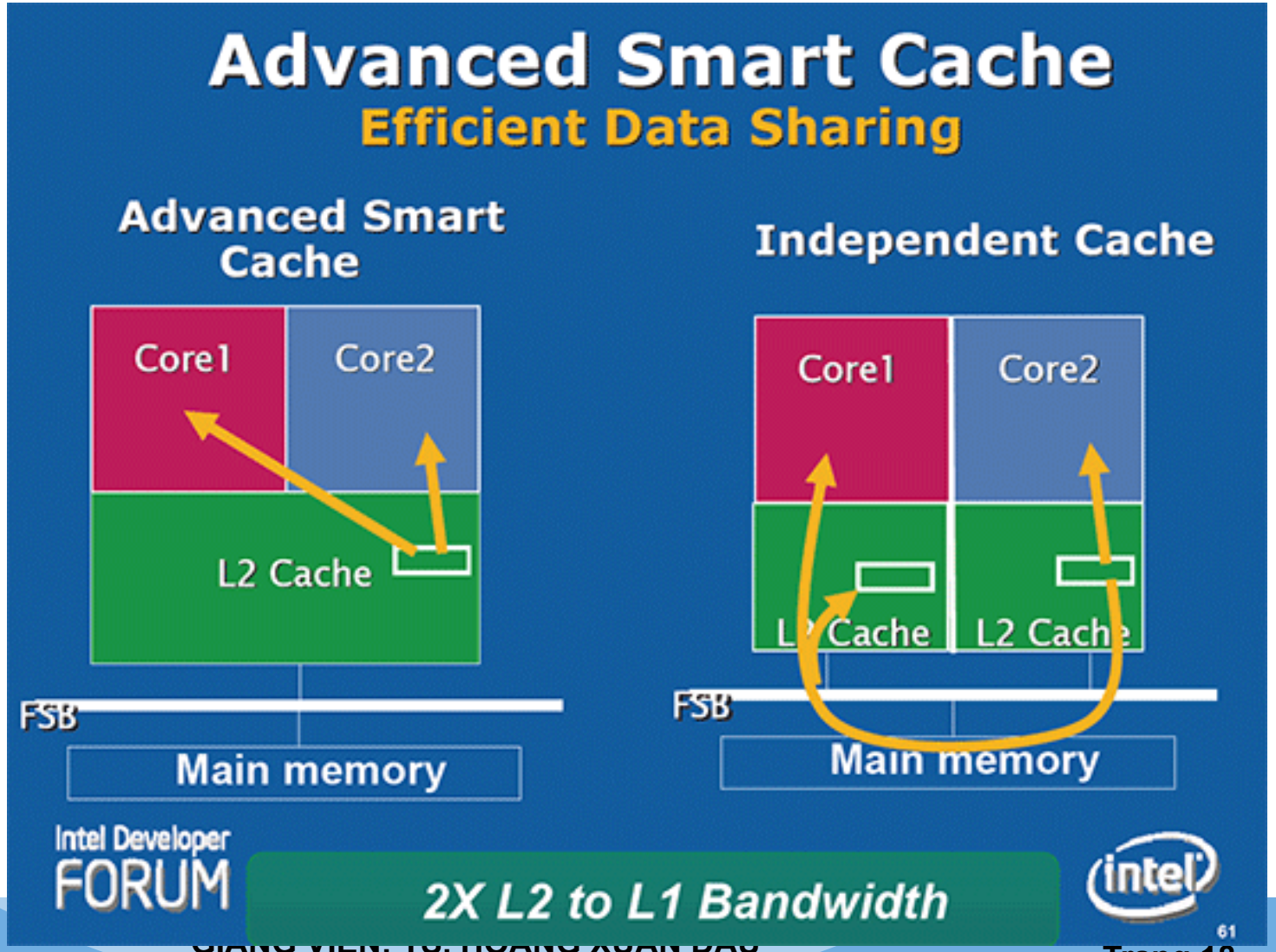
7.1.3 Các VXL họ Intel Core và Core 2

Sơ đồ khối của Intel Core 2



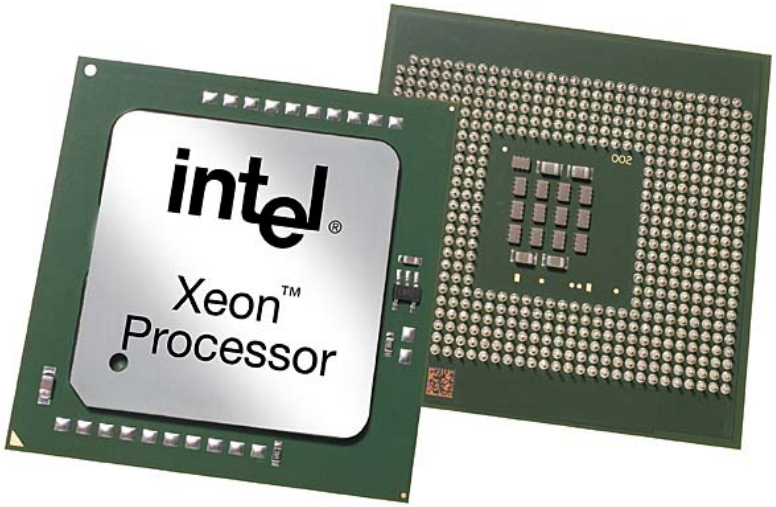
7.1.3 Các VXL họ Intel Core và Core 2

L2 cache của Intel Core 2

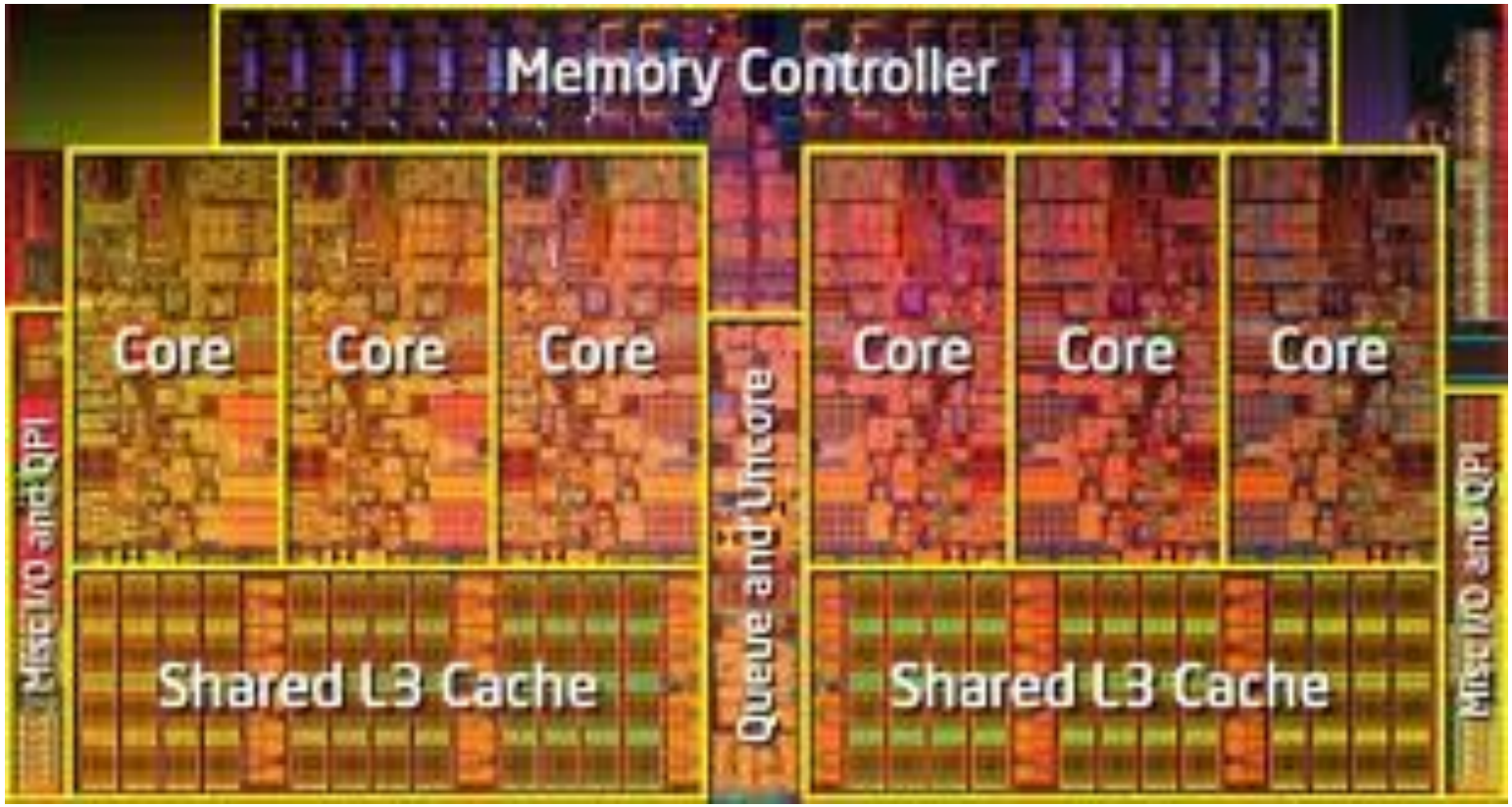


7.1.3 Các VXL họ Intel Xeon

- Được thiết kế riêng cho các máy chủ nhiều CPU có hiệu năng cao
- Các VXL Intel Xeon dựa trên vi kiến trúc Intel P6, NetBurst, Core, Nehalem
- Dòng Intel Xeon MP hỗ trợ công nghệ siêu phân luồng (hyper-threading)
- Dòng Intel Xeon 5100 dựa trên vi kiến trúc Core và Intel 64 tiết kiệm năng lượng và cho hiệu năng cao. Đồng thời nó cũng hỗ trợ công nghệ ảo hoá (Virtualization Technology).



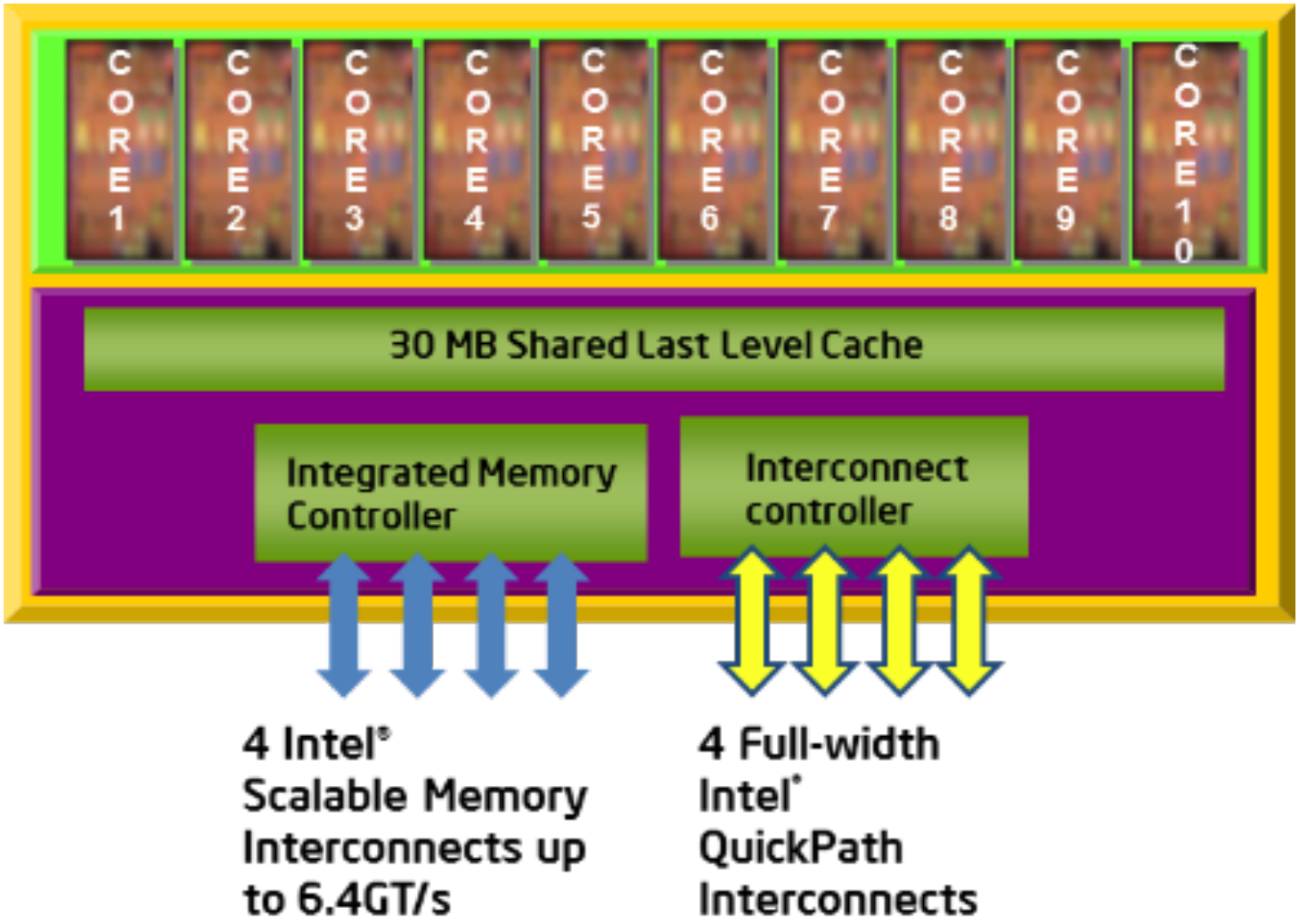
7.1.3 Các VXL họ Intel Xeon



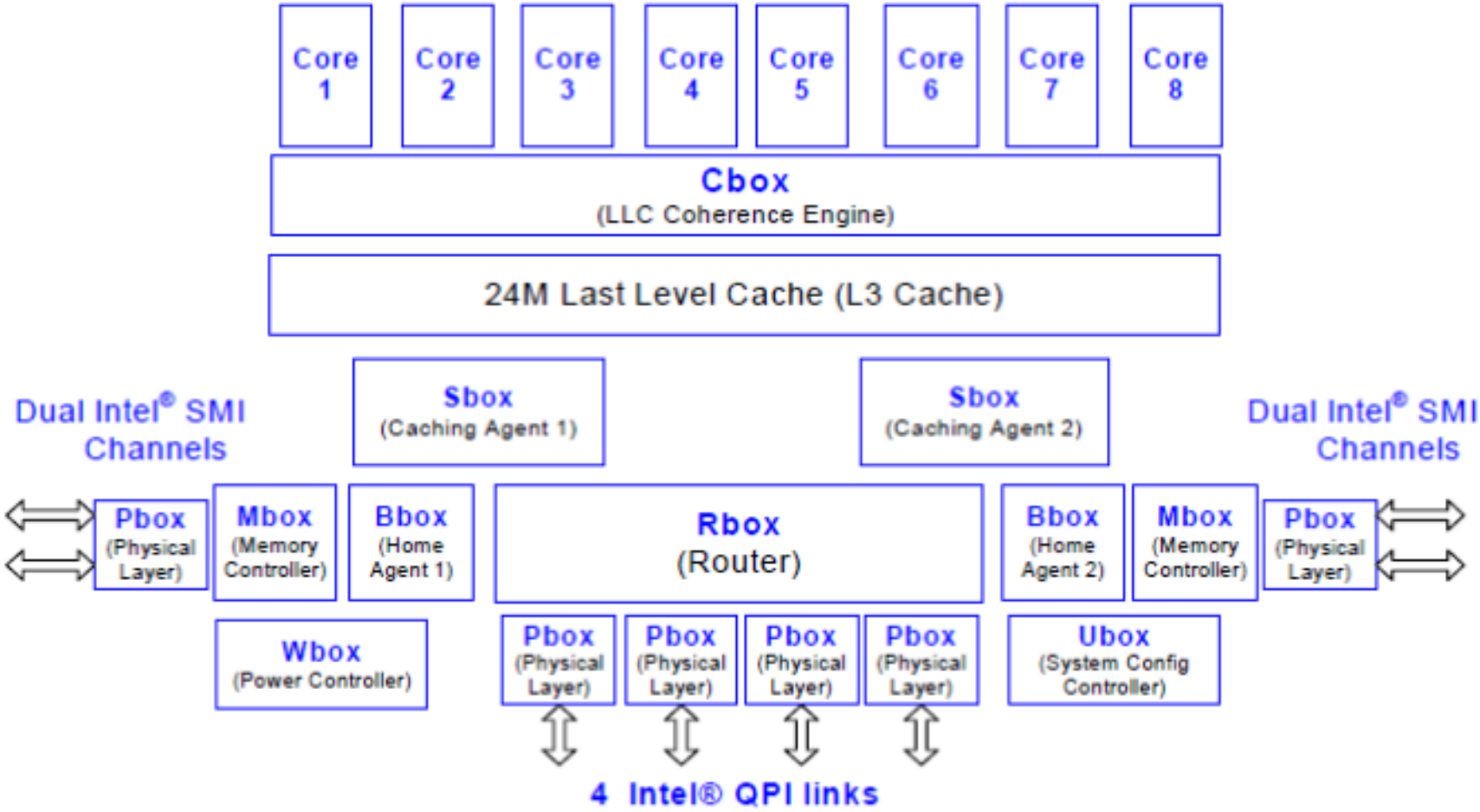
Intel Xeon 5600 đế và các thành phần chính

7.1.3 Các VXL họ Intel Xeon

Intel Xeon E7: 10 nhân, 20 luồng xử lý



7.1.3 Các VXL họ Intel Xeon



Intel Xeon 7500: 8 nhân, 16 luồng xử lý

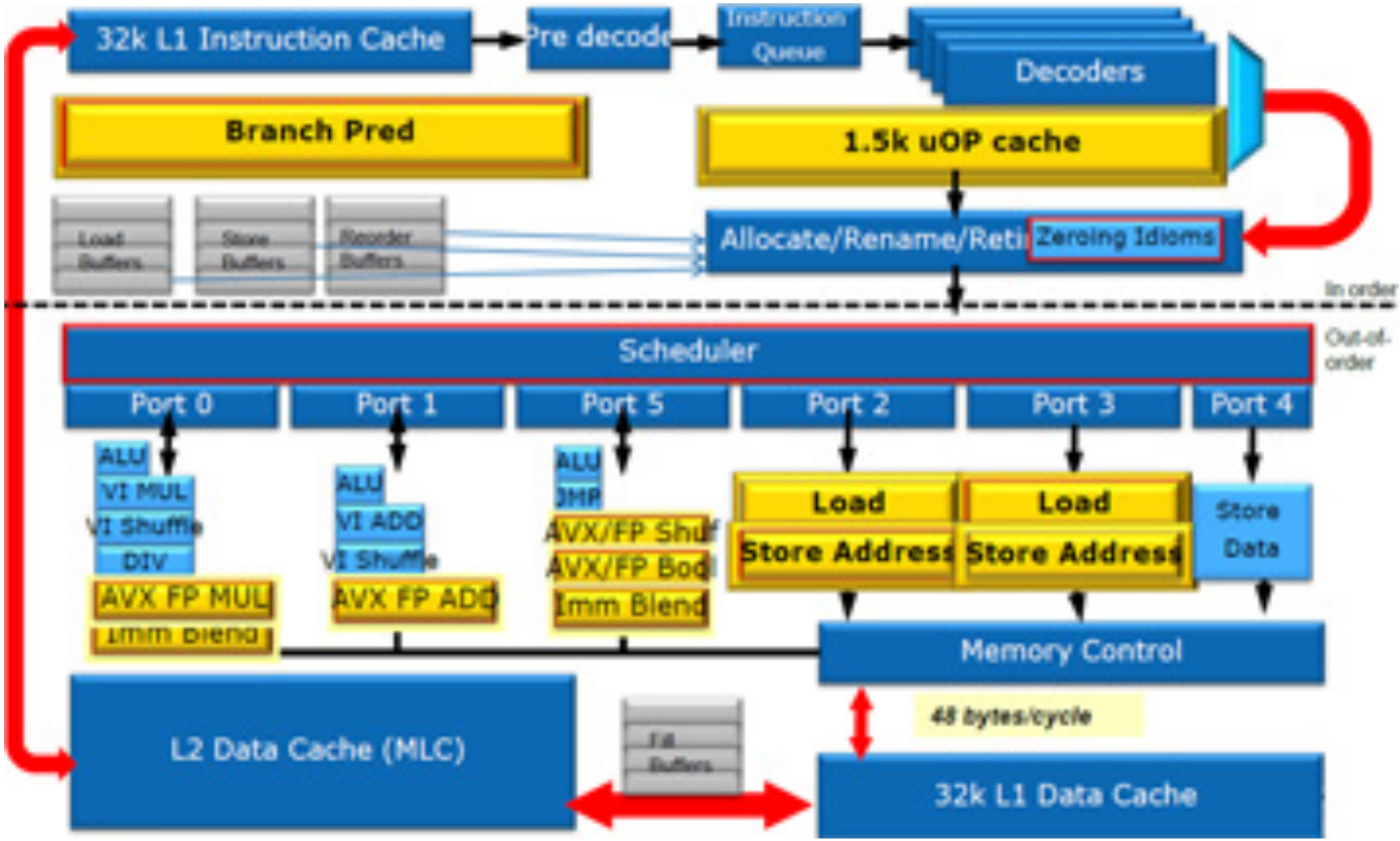
7.1.4 Các VXL họ Intel Core i3, i5, i7

- Các VXL họ Core i3, i5, i7 ra đời từ năm 2010 tiếp sau sự kết thúc của các VXL họ Core 2.
  - Quy ước đặt tên mới: tên VXL không liên quan trực tiếp đến công nghệ và số nhân;
  - Các tên i3, i5, i7 được quy ước theo khả năng xử lý, kiểu "sao" của khách sạn:
    - i3 (3 sao) – năng lực xử lý mức thấp
    - i5 (4 sao) – năng lực xử lý mức trung bình
    - i7 (5 sao) – năng lực xử lý mức cao
- Các VXL họ Core i3, i5, i7 dựa trên 3 thế hệ vi kiến trúc:
  - Nehalam (2008): thế hệ 1
  - Sandy Bridge (2011): thế hệ 2
  - Ivy Bridge (2012): thế hệ 3

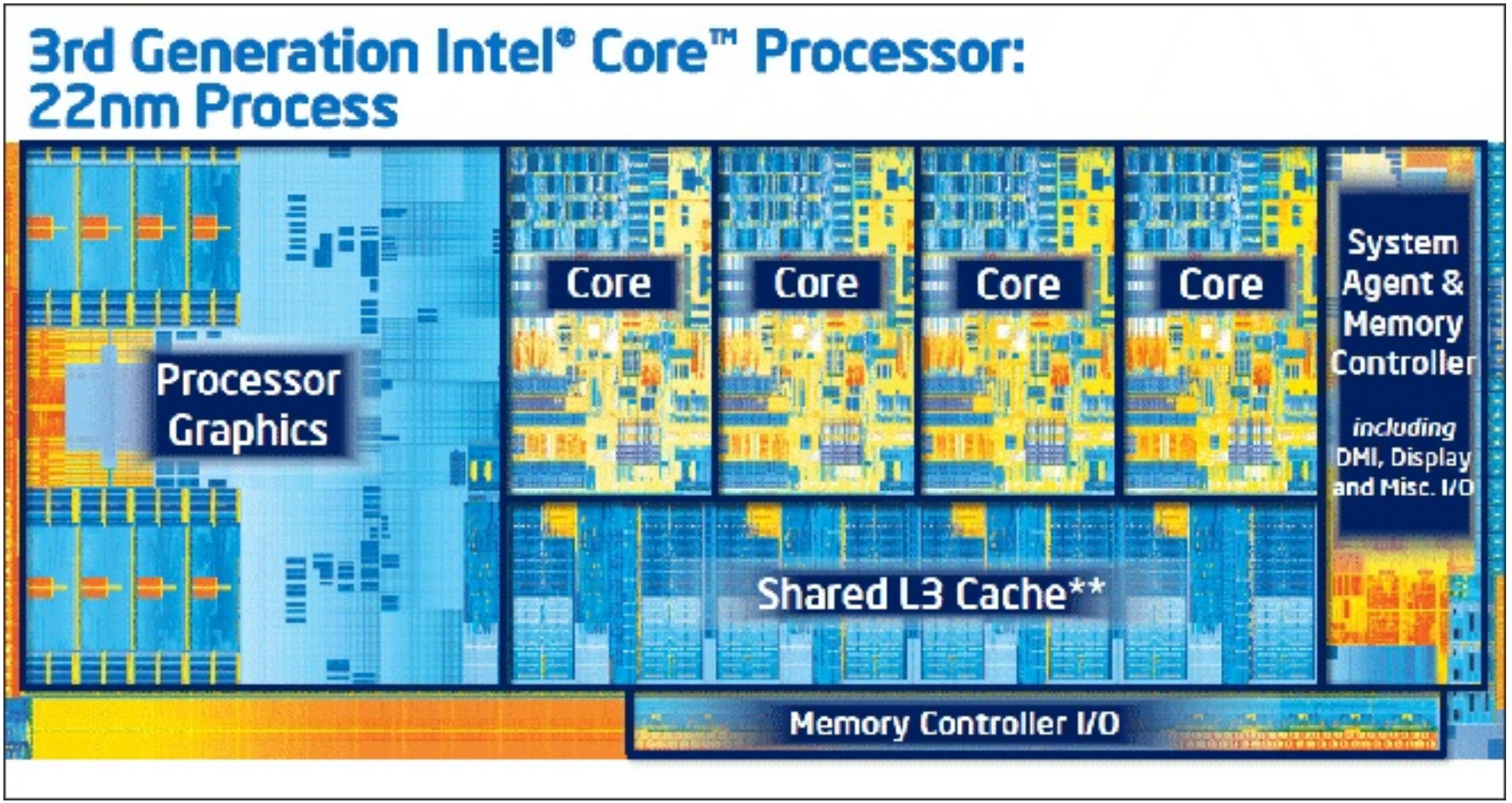
7.1.4 Các VXL họ Intel Core i3, i5, i7

- Bổ sung thêm nhân đồ hoạ (GPU) vào CPU:
  - GPU năm trên cùng một đế (die) với CPU
  - GPU có khả năng truy nhập bộ nhớ cache L3 → giảm thời gian truy nhập bộ nhớ RAM.
  - GPU hỗ trợ các thư viện đồ hoạ mới nhất như DirectX 11.0, OpenGL7.1 và OpenCL 1.1.
- Thay bus phía trước (FSB) tốc độ thấp bằng bus tốc độ cao hơn (QPI-Quick Path Interconnect) kết nối CPU với RAM.
- Bổ sung thêm công nghệ tự ép xung (Turbo Boost – i5, i7)
- Thay bus PCI bằng bus DMI (Direct Media Interface) kết nối CPU với chipset cầu Nam.
- Hỗ trợ bộ nhớ cache L3 lớn: 3-8MB.

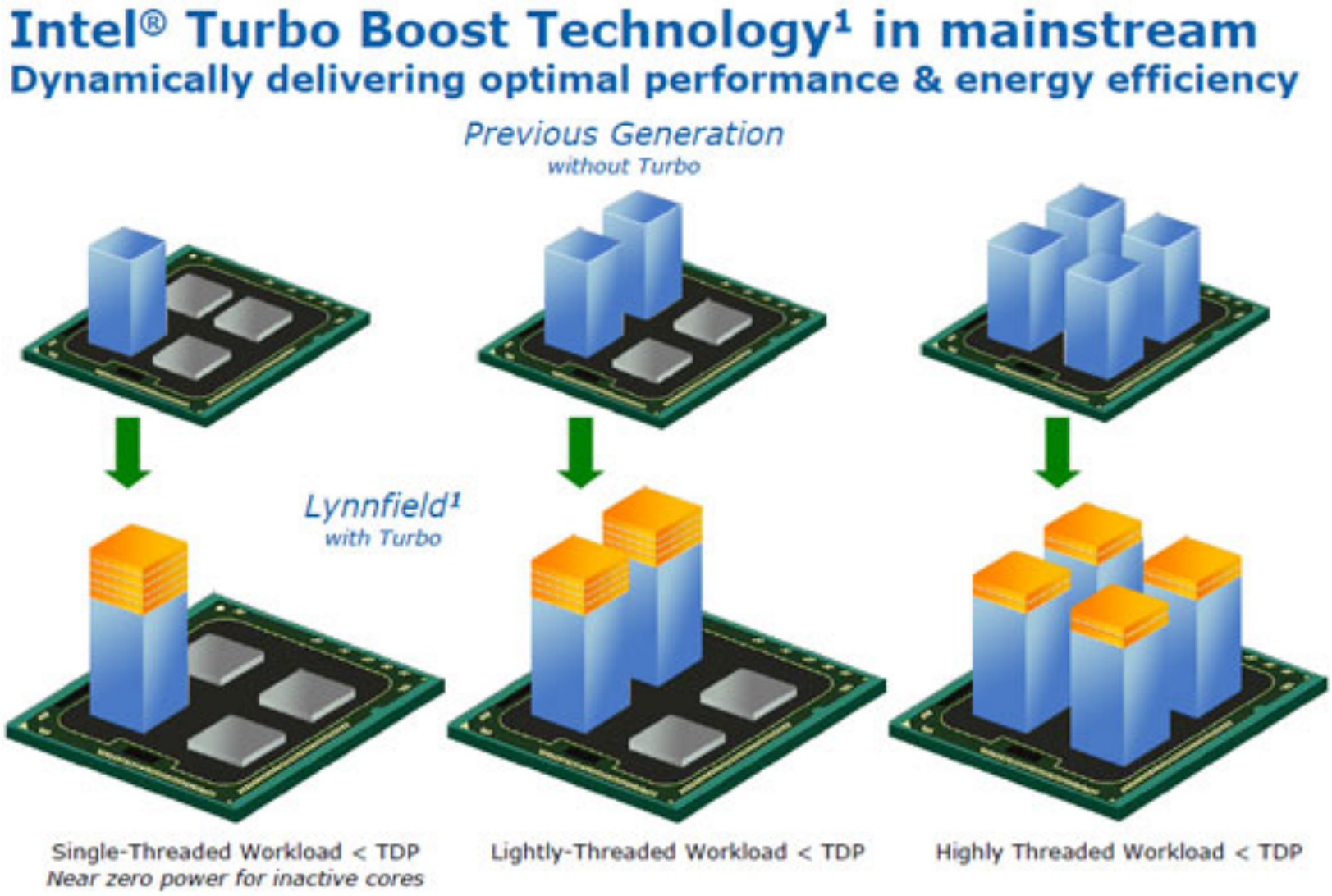
7.1.4 Các VXL họ Intel Core i3, i5, i7-Sandy Bridge



7.1.4 Các VXL họ Intel Core i5, i7 – Ivy Bridge



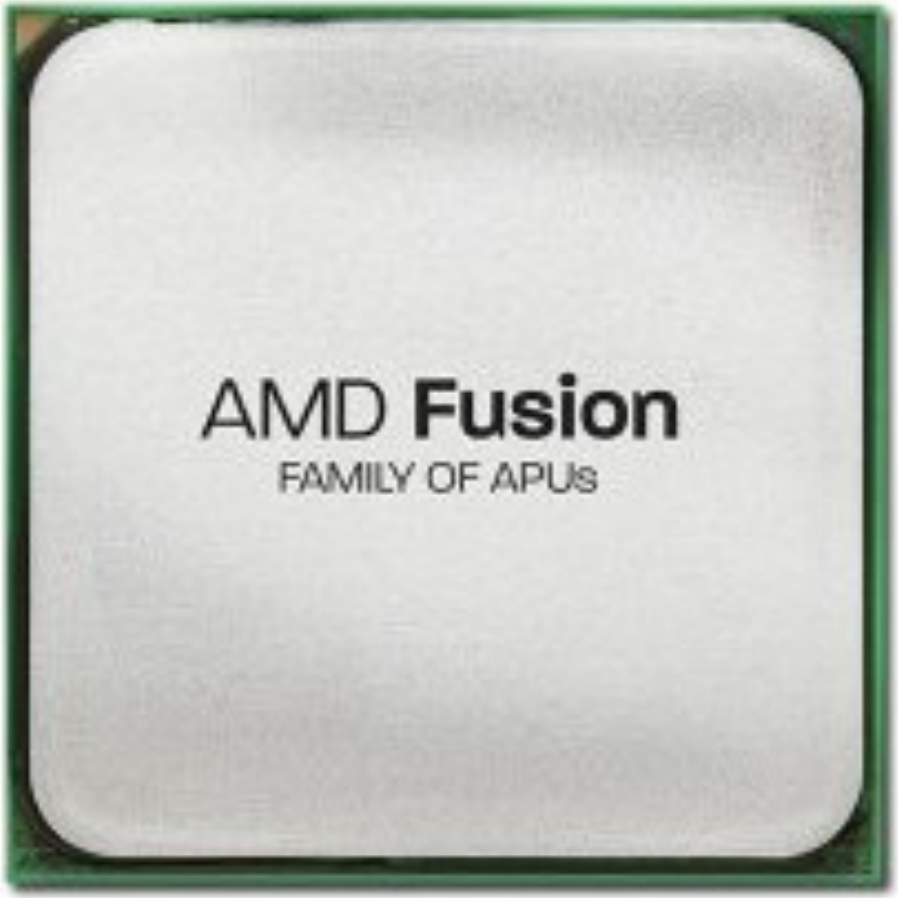
7.1.4 Các VXL họ Intel Core i3, i5, i7-Turbo Boost



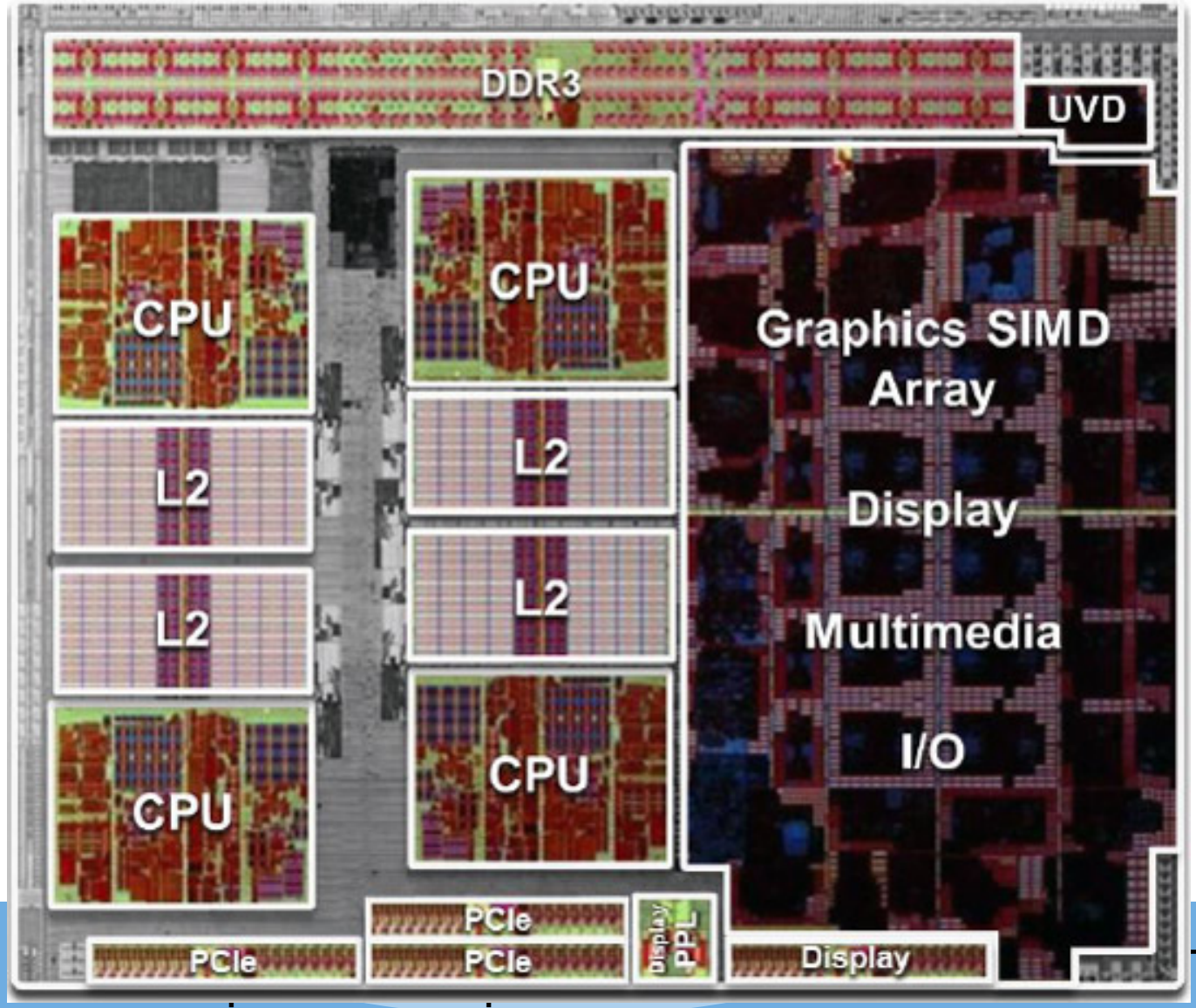
7.1.5 Các VXL họ AMD A-Series

- AMD A-Series hoặc còn gọi là AMD Fusion là dòng CPU mới của hãng AMD (Advanced Micro Devices):
  - Hiệu năng cao;
  - Tiêu thụ điện năng thấp;
  - Tích hợp nhân đồ hoạ GPU mạnh mẽ vào CPU trên cùng 1 đế (die);
- AMD gọi họ VXL này là *bộ xử lý tăng tốc* (Accelarated Processing Unit - APU).
- Công nghệ chế tạo: 32nm.
- Hỗ trợ các thư viện xử lý đồ hoạ mới nhất: DirectX 11.0, OpenGL7.1 và OpenCL 1.1.

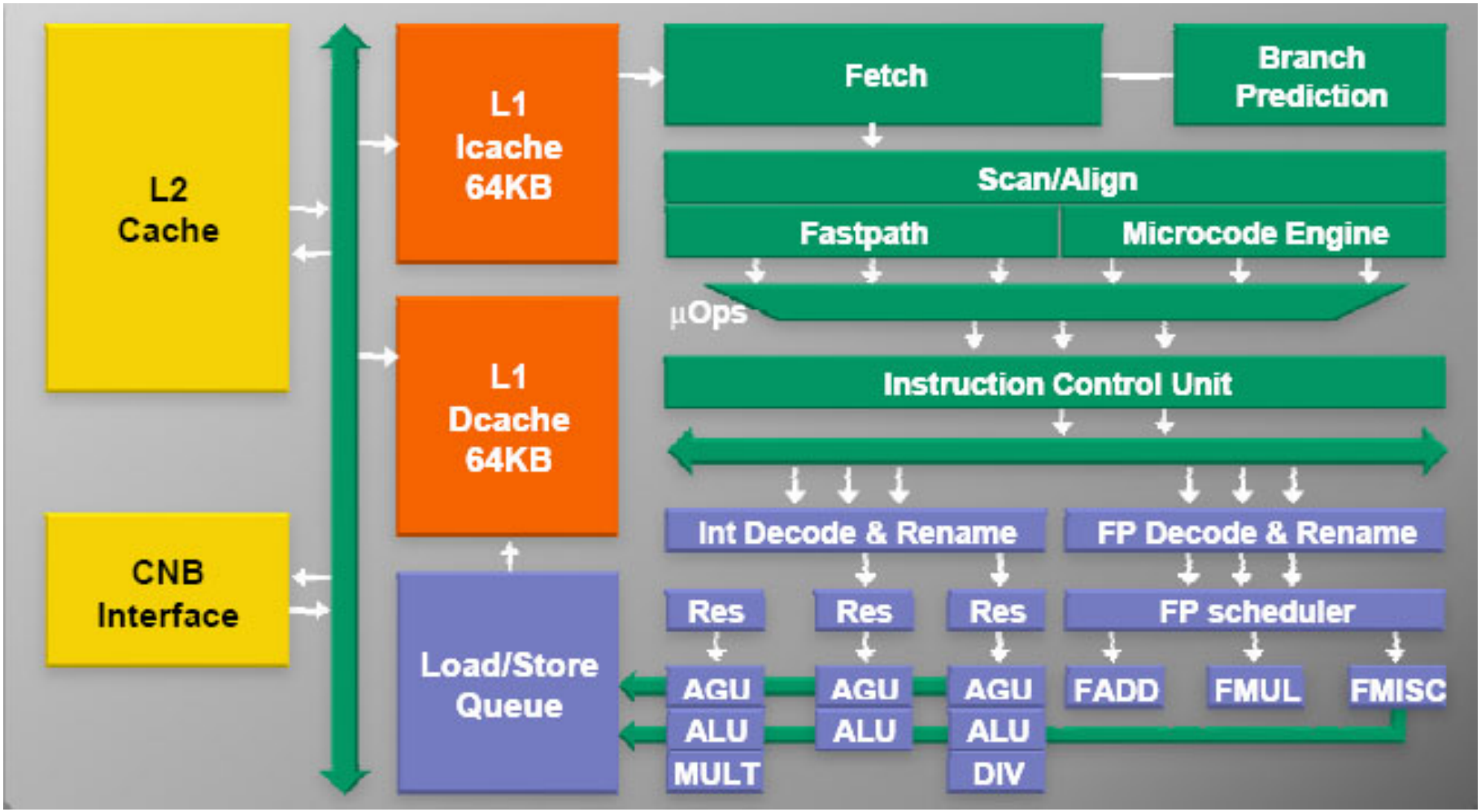
7.1.5 Các VXL họ AMD A-Series



7.1.5 Các VXL họ AMD A-Series-Các khối



7.1.5 Các VXL họ AMD A-Series-Sơ đồ khối



7.2.1 Công nghệ Intel Centrino

- Intel Centrino là công nghệ hướng di động được Intel đưa ra vào năm 2003 ứng dụng cho các máy tính xách tay;
- Centrino gồm 3 thành phần chính:
  - Intel CPU (Pentium M, Core 2, …)
  - Intel mobile chipset
  - Intel wireless network card

7.2.1 Công nghệ Intel Centrino

- Các phiên bản của Centrino:
  - 2003: Pen M /Chipset Mobile 855/ PRO/Wireless 2100/2200
  - 2005: Pen M /Chipset Mobile 915/ PRO/Wireless 2200BG
  - 2006: Core/Core 2 /Chipset Mobile 945/ PRO/Wireless 3945ABG
  - 2007: Core 2 Duo/Chipset GM965/ WiFi Link 4965AGN
  - 2008: Core 2 Duo/Mobile Express series 4/ WiFi Link 5350
  - 2009: Core i3, i5, i7/Mobile Express series 5/ Ultimate-N 6300 AGN
  - 2011: Sandy Bridge/Mobile Express series 6/ Ultimate-N 6300 AGN
  - 2012: Ivy Bridge/Mobile Express series 7/ Ultimate-N 6300

7.2.1 Intel Centrino – Phiên bản 2003

- Tên mã nền tảng: Carmel
- CPU:
  - Pentium M (Banias): 1MB cache, 400MT/s FSB
  - Pentium M (Dothan): 2MB cache, 400MT/s FSB
- Chipset:
  - Intel Mobile 855 Express series
  - Tích hợp nhân đồ hoạ Intel Extreme Graphics 2
  - Hỗ trợ RAM: PC-2100 (DDR-266) hoặc PC-2700 (DDR-333)
- Card không dây:
  - Intel PRO/Wireless 2100B
  - Intel PRO/Wireless 2200BG

7.2.1 Intel Centrino – Phiên bản 2005

- Tên mã nền tảng: Sonoma
- CPU:
  - Pentium M (Dothan): 2MB cache, 533MT/s FSB
- Chipset:
  - Intel Mobile 915 Express series
  - Tích hợp nhân đồ hoạ Intel GMA 900
  - Hỗ trợ RAM: PC2-4200 (DDR2-533)
- Card không dây:
  - Intel PRO/Wireless 2915ABG
  - Intel PRO/Wireless 2200BG

7.2.1 Intel Centrino – Phiên bản 2006

- Tên mã nền tảng: Napa
- CPU:
  - Core Solo, Core Duo
  - Core 2 Duo, 667MT/s FSB
- Chipset:
  - Intel Mobile 945 Express series
  - Tích hợp nhân đồ hoạ Intel GMA 950
  - Hỗ trợ RAM: PC2-4200(DDR2-533) và PC2-5300(DDR2-667)
- Card không dây:
  - Intel PRO/Wireless 3945ABG mini-PCIe
  - Intel PRO/Wireless 4965AGN

7.2.1 Intel Centrino – Phiên bản 2007

- Tên mã nền tảng: Santa Rosa
- CPU:
  - Core 2 Duo, 800MT/s FSB
- Chipset:
  - Intel Mobile 965 Express series
  - Tích hợp nhân đồ hoạ Intel GMA X3100
  - Hỗ trợ RAM: PC2-4200(DDR2-533) và PC2-5300(DDR2-667)
- Card không dây:
  - Intel WiFi Link 4965AGN

7.2.1 Intel Centrino – Phiên bản 2008

- Tên mã nền tảng: Montevina
- CPU:
  - Core 2 Duo, 800-1066MT/s FSB
- Chipset:
  - Intel Mobile Express series 4
  - Tích hợp nhân đồ hoạ Intel GMA X4500
  - Hỗ trợ RAM: PC2-5300 (DDR2-667), PC2-6400 (DDR2-800), PC3-6400 (DDR3-800), PC3-8500 (DDR3-1066)
- Card không dây:
  - Intel WiFi Link 5100 mini-PCIe
  - Intel WiFi Link 5150 mini-PCIe
  - Intel Ultimate N WiFi Link 5300 mini-PCIe

7.2.1 Intel Centrino – Phiên bản 2009

- Tên mã nền tảng: Calpella
- CPU:
  - Intel Core i3/Core i5/Core i7
  - Vi kiến trúc: Nehalem
- Chipset:
  - Intel Mobile Express series 5
  - Tích hợp nhân đồ hoạ Intel HD Graphics
  - Hỗ trợ RAM: PC3-6400 (DDR3-800), PC3-8500 (DDR3-1066), PC3-10600 (DDR3-1333) and PC3-12800 (DDR3-1600)
- Card không dây:
  - Intel Centrino Ultimate-N 6300 AGN mini-PCIe
  - Intel Centrino Wireless-N 1000 BGN mini-PCIe

7.2.1 Intel Centrino – Phiên bản 2011

- Tên mã nền tảng: Huron River
- CPU:
  - Intel Core i3/Core i5/Core i7
  - Vi kiến trúc: Sandy Bridge
- Chipset:
  - Intel Mobile Express series 6
  - Tích hợp nhân đồ hoạ Intel HD Graphics
  - Hỗ trợ RAM: PC3-6400 (DDR3-800), PC3-8500 (DDR3-1066), PC3-10600 (DDR3-1333) and PC3-12800 (DDR3-1600)
- Card không dây:
  - Intel Centrino Ultimate-N 6300 AGN mini-PCIe
  - Intel Centrino Wireless-N 1000 BGN mini-PCIe

7.2.1 Intel Centrino – Phiên bản 2012

- Tên mã nền tảng: Chief River
- CPU:
  - Intel Core i3/Core i5/Core i7
  - Vi kiến trúc: Ivy Bridge
- Chipset:
  - Intel Mobile Express series 7
  - Tích hợp nhân đồ hoạ Intel HD Graphics
  - Hỗ trợ RAM: PC3-6400 (DDR3-800), PC3-8500 (DDR3-1066), PC3-10600 (DDR3-1333) and PC3-12800 (DDR3-1600)
- Card không dây:
  - Intel Centrino Ultimate-N 6300 AGN mini-PCIe
  - Intel Centrino Wireless-N 2200

7.2.2 Các t.lệnh tiên tiến: MMX, SSE, AES & AVX

- MMX (Multi-Media Extention): tập lệnh xử lý số nguyên 64 bits, được giới thiệu năm 1996 trong Pentium II;
- SSE (Streaming SIMD Extension): tập lệnh xử lý số thực 128 bít, được giới thiệu năm 1999 trong Pentium III;
  - SSE2: mở rộng của SSE, giới thiệu năm 2001 trong Pen IV;
  - SSE3: mở rộng của SSE, giới thiệu năm 2004 trong Pen IV;
  - SSE4: mở rộng của SSE, giới thiệu năm 2006 trong VXL Core.
- AES (Advanced Encryption Standard): tập lệnh mã hoá dữ liệu, được giới thiệu năm 2008 trong các VXL Nehalem;
- AVX (Advanced Vector Extensions): tập lệnh mới được giới thiệu năm 2008 trong các VXL Sandy Bridge.

7.2.2 Các tập lệnh tiên tiến: MMX

- MMX là tập lệnh thuộc họ SIMD (Single Instruction Multiple Data) – đơn lệnh đa dữ liệu;
  - Gồm 57 lệnh mới.
- MMX định nghĩa 8 thanh ghi 64 bits: MM0-MM7; Mỗi thanh ghi của MMX có thể được sử dụng theo nhiều kích cỡ:
  - Như là một thanh ghi 64 bít, hoặc
  - 2 thanh ghi 32 bít, 4 thanh ghi 16 bít, hoặc 8 thanh ghi 8 bit.
- MMX chỉ hỗ trợ các phép tính số nguyên kiểu SIMD được sử dụng nhiều trong các ứng dụng đồ hoạ 2D và 3D.
  - Tuy nhiên, chip đồ hoạ cũng hỗ trợ mạnh tính toán số nguyên SIMD cho các ứng dụng đồ hoạ 2D và 3D, nên việc hỗ trợ tính toán số nguyên SIMD của CPU không thực sự hữu ích.

7.2.2 Các tập lệnh tiên tiến: SSE

- SSE là tập lệnh thuộc họ SIMD (Single Instruction Multiple Data) – đơn lệnh đa dữ liệu;
  - Gồm 70 lệnh mới.
- SSE định nghĩa 8 thanh ghi 128 bits: XMM0-XMM7; Mỗi thanh ghi XMM chỉ có thể được sử dụng để lưu 4 số thực 32 bít độ chính đơn;
- SSE hỗ trợ thêm 8 thanh ghi 128 bit: XMM8-XMM15 trong các kiến trúc Intel-64 và AMD64;
- SSE hỗ trợ:
  - Các thao tác với số thực dấu phảy động (Floating-Point Numbers);
  - Các thao tác với số nguyên (Integer Numbers);

7.2.2 Các tập lệnh tiên tiến: SSE2

- SSE2 là tập lệnh mở rộng thứ nhất của tập lệnh SSE;
  - Gồm 144 lệnh mới.
- SSE2 cũng mở rộng các lệnh MMX, cho phép chúng thao tác trực tiếp trên các thanh ghi XMM 128 bit, giúp cho việc xử lý các số nguyên SIMD và số thực trên cùng 1 mô tơ thực hiện, không phải chuyển đổi chế độ giữa MMX và xử lý số thực;
- SSE2 cung cấp một số lệnh điều khiển cache, giúp nâng cao hiệu quả sử dụng không gian cache;
  - Giúp giảm hiện tượng làm ô nhiễm cache (cache pollution). Đó là hiện tượng một chương trình đang chạy nạp các dữ liệu không cần thiết vào cache, dẫn đến việc phải đẩy các dữ liệu đang sử dụng ra bộ nhớ chính → giảm hiệu năng cache.

7.2.2 Các tập lệnh tiên tiến: SSE3

- SSE3 là mở rộng của tập lệnh SSE2;
- SSE3 còn được gọi là Prescott New Instructions (PNI);
- Gồm 13 lệnh mới.
- Bổ sung các lệnh tối ưu hoá các ứng dụng đa luồng, nâng cao hiệu quả của công nghệ Hyper Threading.

7.2.2 Các tập lệnh tiên tiến: SSE3

- SSE3 là mở rộng của tập lệnh SSE2;
- SSE3 còn được gọi là Prescott New Instructions (PNI);
- Gồm 13 lệnh mới.
- Bổ sung các lệnh tối ưu hoá các ứng dụng đa luồng, nâng cao hiệu quả của công nghệ Hyper Threading.

7.2.2 Các tập lệnh tiên tiến: SSE4

- SSE4 còn được gọi là SSSE3 (Suplemental SSE3) được giới thiệu trong vi kiến trúc Core năm 2006;
  - Bổ sung thêm 54 lệnh mới;
  - Các lệnh của SSE4 thực thi các thao tác không phục vụ cụ thể cho các ứng dụng đa phương tiện.
- SSE4 gồm các tập lệnh con:
  - SSE7.1: gồm 47 lệnh được đưa vào VXL Penryn của vi kiến trúc Core.
  - SSE7.2: gồm 7 lệnh xử lý chuỗi và văn bản (STTNI - STring and Text New Instructions):
    - Tìm kiếm ký tự và và so sánh 2 chuỗi 16 bytes;
    - Lệnh tính chuỗi kiểm tra dư thừa mạch vòng (CRC), thường dùng trong truyền thông.

7.2.2 Các tập lệnh tiên tiến: AES

- AES (Advanced Encryption Standard) là tập lệnh cung cấp các lệnh mã hoá/giải mã theo chuẩn mã hoá tiên tiến (AES);
  - Được giới thiệu năm 2008 trong các vi kiến trúc Nehalem, Sandy Bridge và Ivy Bridge,…
  - Tăng tốc các ứng dụng mã hoá/giải mã theo chuẩn mã hoá tiên tiến.
  - Theo 1 thử nghiệm trên phần mềm Crypto++, tốc độ mã hoá chạy trên tập lệnh AES tăng đáng kể:
    - 28.0 chu kỳ đồng hồ/byte (không AES)
    - 3.5 chu kỳ đồng hồ/byte (có AES).

7.2.2 Các tập lệnh tiên tiến: AVX

- AVX (Advanced Vector Extensions) được giới thiệu năm 2011 trong vi kiến trúc Sandy Bridge;
- Các đặc tính mới:
  - Tăng độ rộng các thanh ghi SIMD từ 128 bít lên 256 bít và đổi tên thành YMM0–YMM15;
  - Các lệnh SSE cũ sẽ làm việc trên nửa thấp (128 bít) của các thanh ghi YMM.
  - Các lệnh AVX sẽ gồm 3 toán hạng trong đó toán hạng đích sẽ khác biệt hoàn toàn với các toán hạng nguồn.
  - VD: a ← a + b sẽ chuyển thành c ← a + b ➔ giúp bảo toàn giá trị các toán hạng nguồn.

7.2.2 Các tập lệnh tiên tiến: AVX

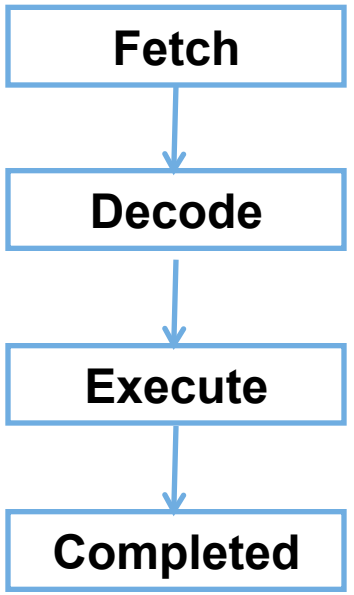
- Cách viết mã mới:
  - AVX đưa vào một tập các tiếp đầu ngữ mã (code prefix) để mở rộng không gian mã lệnh (opcode space);
  - Cho phép các lệnh có hơn 2 toán hạng;
  - Cho phép các thanh ghi véctơ SIMD dài hơn 128 bít.
- Ứng dụng:
  - Phù hợp với các ứng dụng đa phương tiện, tính toán khoa học và tài chính đòi hỏi nhiều tính toán số dấu chấm động;
  - Cải thiện vấn đề xử lý song song và thông lượng của các thao tác số dấu chấm động SIMD;
  - Giảm tải cho các thanh ghi nhờ khả năng bảo toàn giá trị các toán hạng nguồn của các lệnh AVX.

7.2.3 Công nghệ thực thi không theo trật tự

- Các lệnh của chương trình thường được thực thi theo 2 phương pháp:
  - Thực thi tĩnh (hay Thực thi theo trật tự – In Order Execution):
    - Các lệnh của chương trình được nạp, giải mã, thực hiện và kết thúc theo trật tự của chúng sau biên dịch.
  - Thực thi động (hay Thực thi không theo trật tự – Out Of Order Execution):
    - Các lệnh của chương trình được nạp và giải mã theo trật tự của chúng sau biên dịch;
    - Các lệnh của chương trình sau giải mã có thể được thực hiện theo trật tự khác với trật tự của chúng sau biên dịch.

7.2.3 Công nghệ thực thi không theo trật tự (tiếp)

- Thực thi theo trật tự (In order execution):
  - Các lệnh của chương trình được nạp, giải mã, thực hiện và kết thúc theo trật tự của các lệnh được viết ra;
  - Nếu có một lệnh bị dừng thực hiện, tất cả các lệnh phía sau đều bị dừng;
  - Các lệnh được lập lịch thực hiện tĩnh (static scheduling).



7.2.3 Công nghệ thực thi không theo trật tự (tiếp)

- Quá trình thực hiện lệnh theo trật tự:
  - Lệnh được đọc từ bộ nhớ và được giải mã;
  - Nếu các toán hạng của lệnh đã sẵn sàng (ở các thanh ghi), lệnh được chuyển đến đơn vị chức năng phù hợp để thực hiện;
  - Nếu các toán hạng của lệnh chưa sẵn sàng ở chu kỳ đồng hồ hiện tại (như toán hạng đang được đọc ở bộ nhớ), CPU sẽ dừng và chờ cho đến khi các toán hạng của lệnh sẵn sàng;
  - Lệnh được thực hiện bởi đơn vị chức năng;
  - Kết quả thực hiện lệnh được lưu vào tập thanh ghi.

7.2.3 Công nghệ thực thi không theo trật tự (tiếp)

- Ưu, nhược điểm của thực hiện lệnh theo trật tự:
  - Ưu điểm: tổ chức thực thi đơn giản do có thể dùng kỹ thuật lập lịch thực thi tĩnh (static scheduling);
  - Nhược điểm:
    - Chậm do nếu một lệnh nào đó bị dừng (stall) do các toán hạng của nó chưa sẵn sàng thì tất cả các lệnh phía sau phải chờ;
    - Nếu lệnh được thực thi theo cơ chế ống lệnh thì lệnh bị dừng có thể làm ngưng trệ hoạt động cả ống lệnh và làm giảm đáng kể hiệu suất thực hiện lệnh.

7.2.3 Công nghệ thực thi không theo trật tự (tiếp)

- Thực thi không theo trật tự (Out of order execution):
  - Các lệnh của chương trình được nạp và giải mã theo trật tự của chúng sau biên dịch;
  - Các lệnh của chương trình sau giải mã có thể được thực hiện theo trật tự khác với trật tự của chúng sau biên dịch;
  - Các lệnh của chương trình sau thực hiện được sắp xếp lại để kết thúc theo trật tự như khi chúng được nạp vào;
  - Nếu có một lệnh bị dừng thực hiện, các lệnh độc lập ở phía sau có thể được đẩy lên để thực hiện trước;
  - Các lệnh được lập lịch thực hiện động (dynamic scheduling);

7.2.3 Công nghệ thực thi không theo trật tự (tiếp)

- Ý tưởng chính của công nghệ thực thi không theo trật tự:
  - Cho phép các lệnh được thực hiện (execute) *không theo trật tự chương trình*, nếu các tham số/toán hạng đầu vào của chúng đã sẵn sàng;
  - Các lệnh phải được hoàn tất (commit) ở giai đoạn lưu kết quả *theo trật tự chương trình* để đảm bảo kết quả thực hiện lệnh và kết quả cả chương trình là đúng.
- Cần phải tách giai đoạn thực hiện lệnh (execution) và giai đoạn hoàn tất (committment):
  - Giai đoạn thực hiện lệnh (execution) có thể kết thúc rất sớm nhưng giai đoạn hoàn tất (committment) có thể chưa sẵn sàng.
  - Cần bổ sung thêm module phần cứng Reorder Buffer và Retirement Unit để thực hiện giai đoạn hoàn tất.

7.2.3 Công nghệ thực thi không theo trật tự (tiếp)

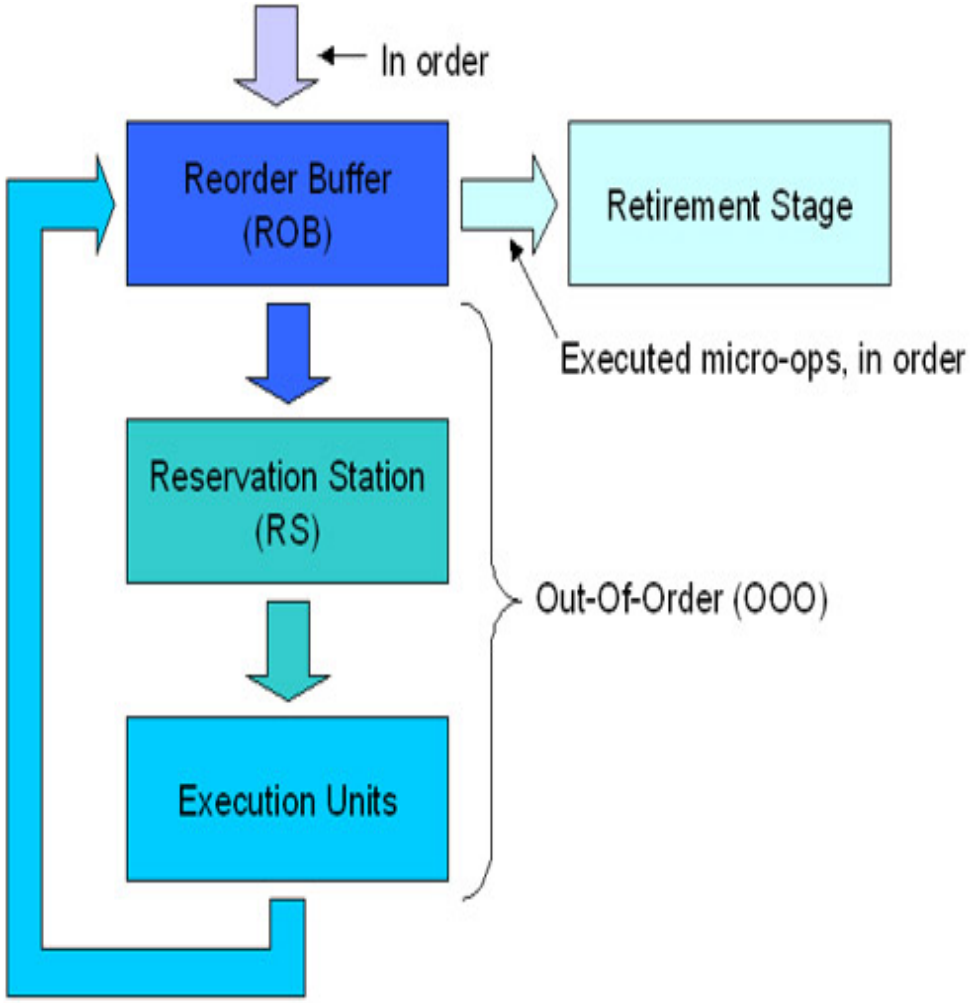
- Quá trình thực thi không theo trật tự:
  - Lệnh được đọc từ bộ nhớ và được giải mã;
  - Lệnh được gửi đến hàng đợi lệnh – thường gọi là trạm dự phòng (reservation stations);
  - Lệnh chờ ở hàng đợi lệnh cho đến khi các toán hạng đầu vào của nó sẵn sàng. Sau đó lệnh được phép dời khỏi hàng đợi lệnh, có thể trước cả các lệnh đứng trước;
  - Lệnh được gửi đến đơn vị chức năng và được thực hiện;
  - Các kết quả thực hiện lệnh được xếp hàng;
  - Chỉ sau khi kết quả của các lệnh đứng trước được ghi vào tập thanh ghi, kết quả của lệnh mới được ghi vào tập thanh ghi. Đây được gọi là giai đoạn thu hồi kết quả (retirement).

7.2.3 Công nghệ thực thi không theo trật tự (tiếp)

- Ưu điểm của thực thi không theo trật tự: tăng tốc độ thực hiện lệnh nhờ:
  - Giảm đến tối thiểu thời gian chờ thực hiện;
  - Tận dụng tối đa năng lực của đơn vị thực hiện lệnh;
  - Nếu có một lệnh phải dừng do chưa đủ điều kiện thực hiện, các lệnh phía sau nếu đủ điều kiện sẽ được đẩy lên thực hiện trước.
- Nhược điểm:
  - Phức tạp hơn thực thi theo trật tự, do phải bổ sung thêm:
    - Khối cấp phát & đổi tên thanh ghi
    - Bộ lập lịch động
    - Bộ sắp xếp lại và bộ thu hồi kết quả.

7.2.3 Công nghệ thực thi không theo trật tự

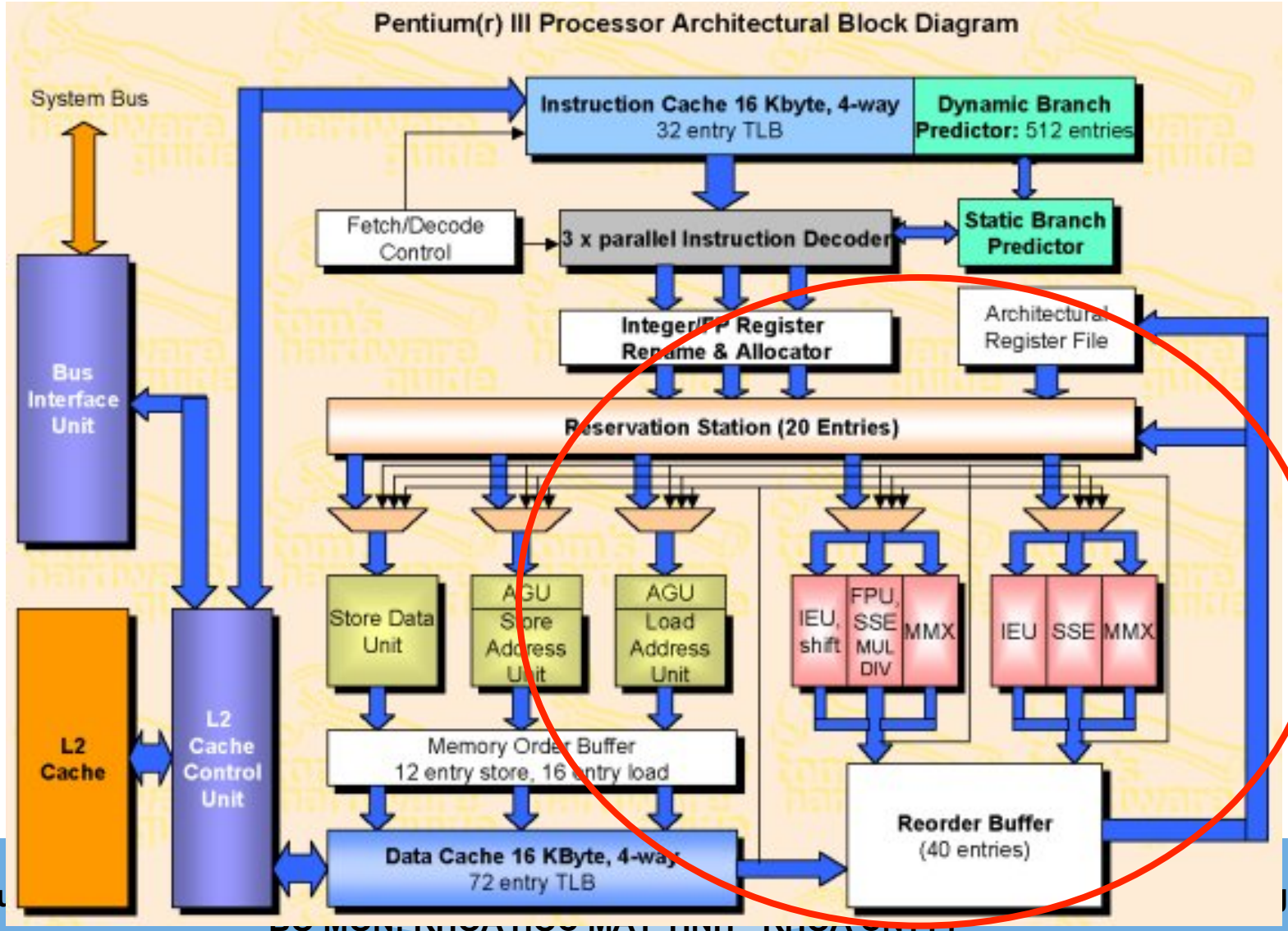
- In order: các lệnh được chuyển xuống theo trật tự được nạp vào;
- Out Of Order: thực thi không theo trật tự;
- Reorder Buffer (ROB): Khối sắp xếp lại trật tự;
- Reservation Station (RS): Trạm dự phòng;
- Execution Units: các đơn vị thực hiện;
- Retirement Stage: Giai đoạn thu hồi kết quả;
- micro-ops: các vi lệnh.



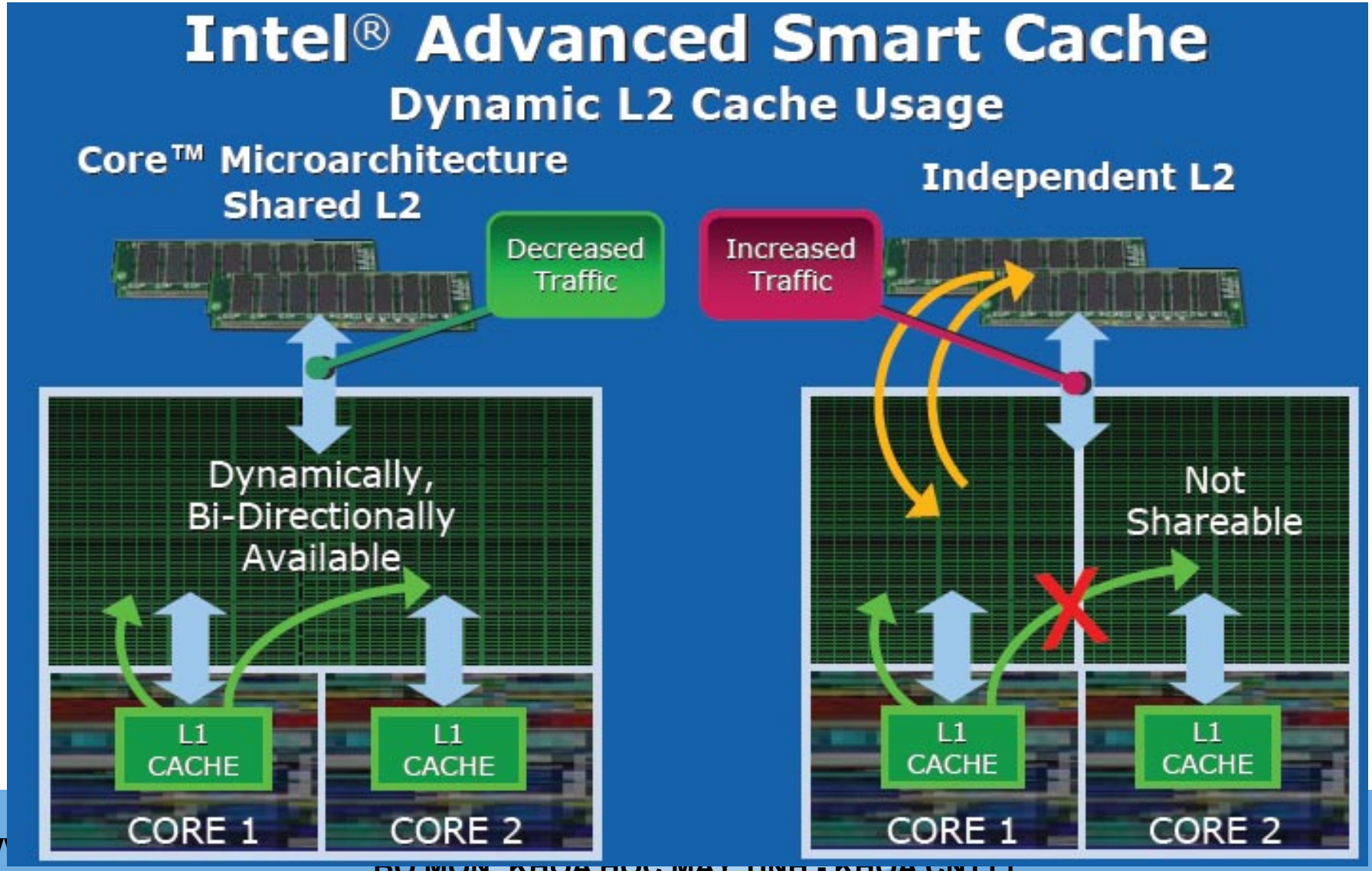
7.2.3 Công nghệ thực thi không theo trật tự

- Các bước thực hiện theo sơ đồ:
  1. Các vi lệnh (micro operations) sau giải mã được chuyển đến ROB (Reorder Buffer). Chúng được ghi nhận trật tự và tiếp tục được chuyển đến RS (Reservation Stations);
  2. Tại RS, lệnh chờ cho đến khi các toán hạng đầu vào của nó sẵn sàng. Tiếp theo vi lệnh được chuyển đến đơn vị thực hiện;
  3. Vi lệnh được thực hiện bởi đơn vị thực hiện. Sau đó nó được chuyển trở lại ROB;
  4. Vi lệnh chờ tại ROB cho đến khi tất cả các vi lệnh đứng trước hoàn tất việc lưu kết quả; Sau đó nó được chuyển sang Retirement Unit để thực hiện lưu kết quả;
  5. Kết thúc quá trình thực hiện lệnh.

7.2.3 Thực thi không trật tự trong Intel Pentium III



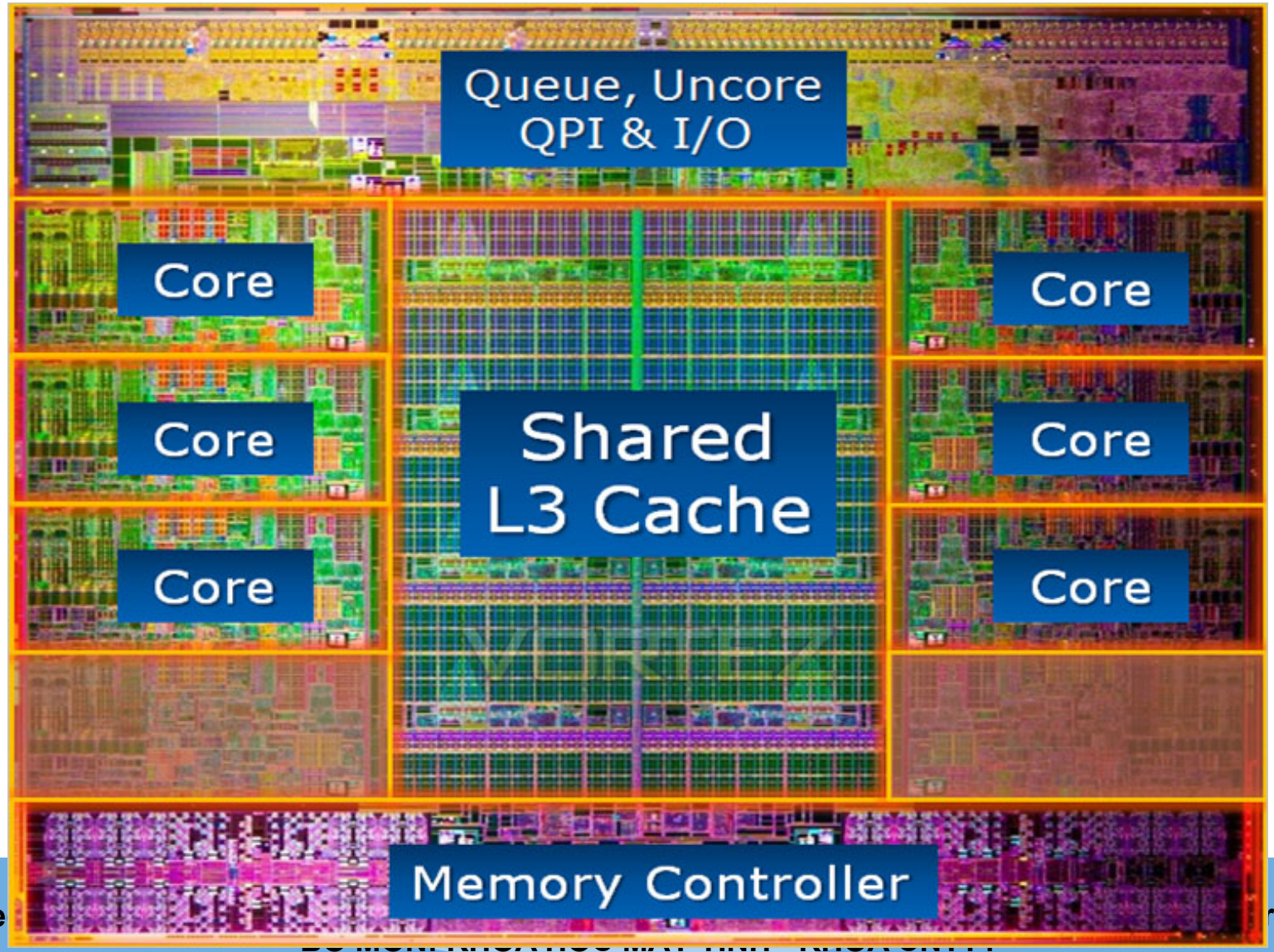
7.2.4 Công nghệ cache thông minh



7.2.4 Công nghệ cache thông minh (tiếp)

- Cache chia sẻ (mức L2 hoặc L3) giữa các nhân cho phép:
  - Chia sẻ dữ liệu: Nếu các nhân có nhu cầu xử lý cùng một đơn vị dữ liệu, chỉ 1 copy của dữ liệu được nạp vào cache chia sẻ.
  - Giảm lưu lượng vận chuyển trên bus hệ thống: Yêu cầu tải dữ liệu trên bus giảm do các nhân có thể dùng chung dữ liệu.
  - Dung lượng cache được sử dụng hiệu quả hơn:
    - Không có biên giới cứng phân chia cache giữa các nhân;
    - Nếu một nhân có yêu cầu dữ liệu xử lý lớn hơn các nhân khác, nó sẽ được cấp dung lượng cache nhiều hơn → tận dụng được không gian rảnh rỗi của cache.
  - Tăng hiệu năng: Do không gian cache được sử dụng hiệu quả hơn → không gian cache hiệu dụng lớn hơn → cạnh tranh trong cache giảm → tăng hệ số hit → tăng hiệu năng hệ thống.

7.2.4 Công nghệ cache thông minh (tiếp)



7.2.5 Công nghệ tiết kiệm điện Intel Speedstep

- Intel Speedstep là công nghệ cho phép tự động thay đổi xung nhịp làm việc của CPU bằng phần mềm;
  - Xung nhịp và điện áp CPU được tự động điều chỉnh cho phù hợp với tải hệ thống, giúp giảm tiêu hao điện năng.
- Hầu hết các hệ điều hành đều hỗ trợ công nghệ Speedstep:
  - Windows
  - Linux
  - Unix (BSD, Solaris, …)
  - Mac OS

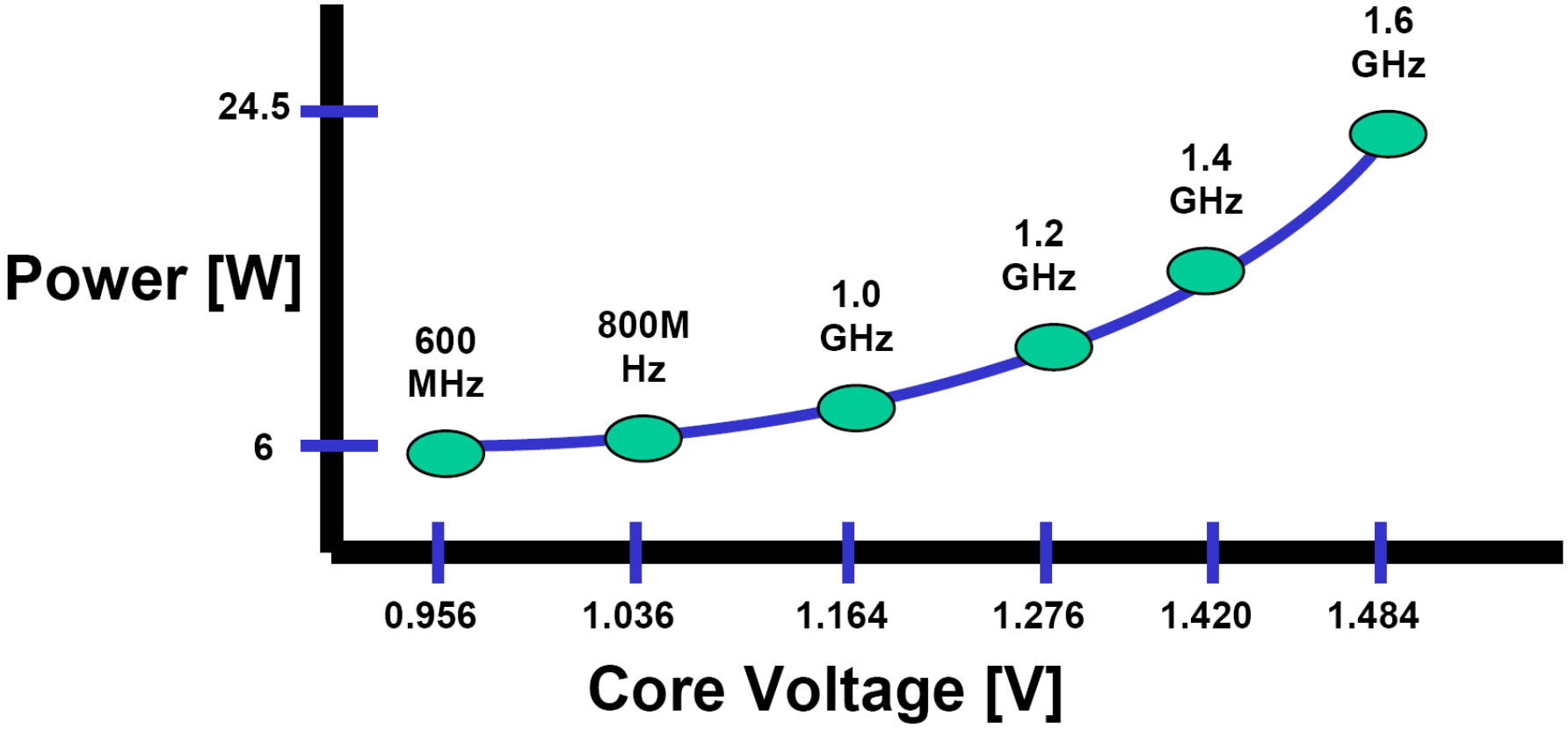
7.2.5 Công nghệ tiết kiệm điện Intel Speedstep

- Các phiên bản của Speedstep:
  - V1.1 trong Pentium III: hỗ trợ 2 chế độ làm việc thông qua việc điều chỉnh hệ số nhân xung nhịp CPU:
    - Tải cao: CPU hoạt động với xung nhịp 1GHz, tiêu thụ 20W;
    - Tải thấp: CPU hoạt động với xung nhịp 600MHz, tiêu thụ 6W.
  - V2.1 (Enhanced Speedstep) trong Pentium III mobile: tương tự V1.1, nhưng đồng thời giảm điện áp CPU trong chế độ tải thấp.
  - V2.2 trong Pentium 4-M: hỗ trợ 2 chế độ làm việc:
    - Tải cao: CPU hoạt động với xung nhịp 1.8GHz, tiêu thụ 30W;
    - Tải thấp: CPU hoạt động với xung nhịp 1.2MHz, tiêu thụ 20W.

7.2.5 Công nghệ tiết kiệm điện Intel Speedstep

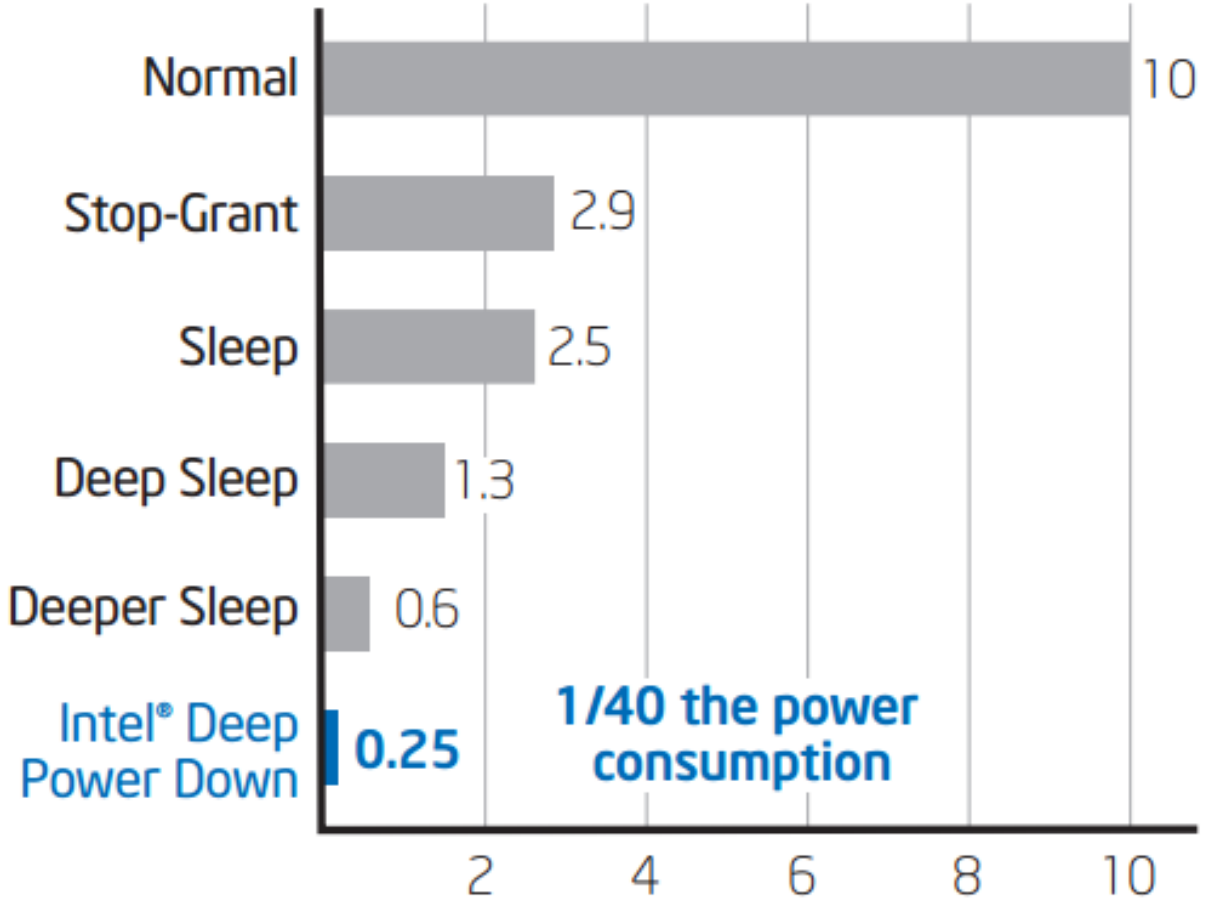
- Các phiên bản của Speedstep:
  - V3.1 (Enhanced Intel Speedstep-EIST) trong Pentium M:
    - Tự động điều chỉnh xung nhịp và điện áp theo bước (100MHz với lõi Banias và 133MHz với lõi Dothan) trong khoảng 40-100% xung nhịp chuẩn;
    - Bổ sung thêm khả năng điều chỉnh dung lượng hoạt động thực của bộ nhớ cache (ngắt điện bớt một phần cache) khi tải thấp.
  - V3.2 (Enhanced EIST):
    - Cơ chế hoạt động tương tự V3.1;
    - Hỗ trợ CPU nhiều nhân.

7.2.5 Công nghệ tiết kiệm điện Intel Speedstep



Tiêu thụ điện năng theo điện áp của Pentium M 1.6GHz

7.2.5 Công nghệ tiết kiệm điện Intel Speedstep

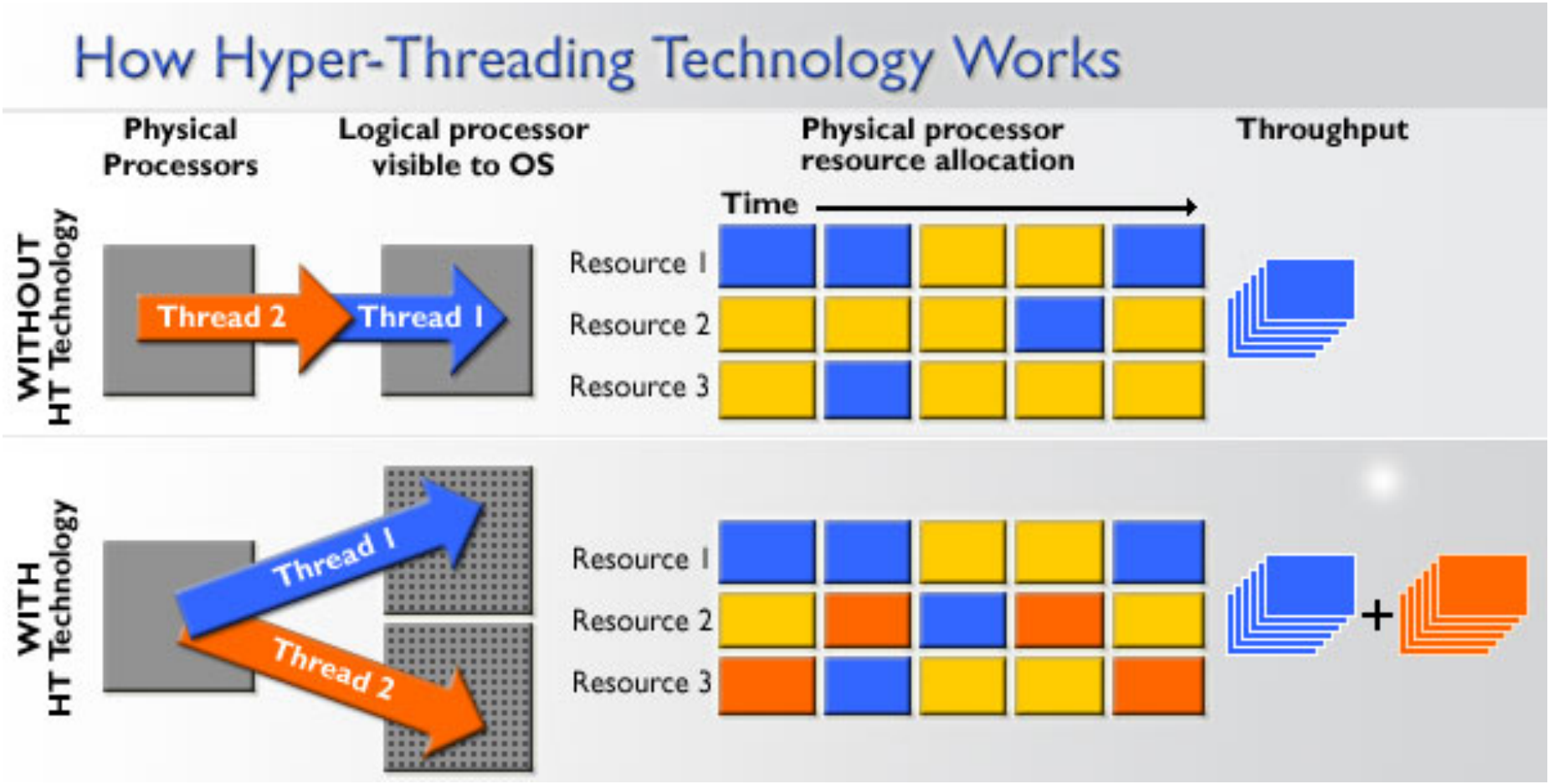


Tiêu thụ điện năng theo các trạng thái tiết kiệm điện

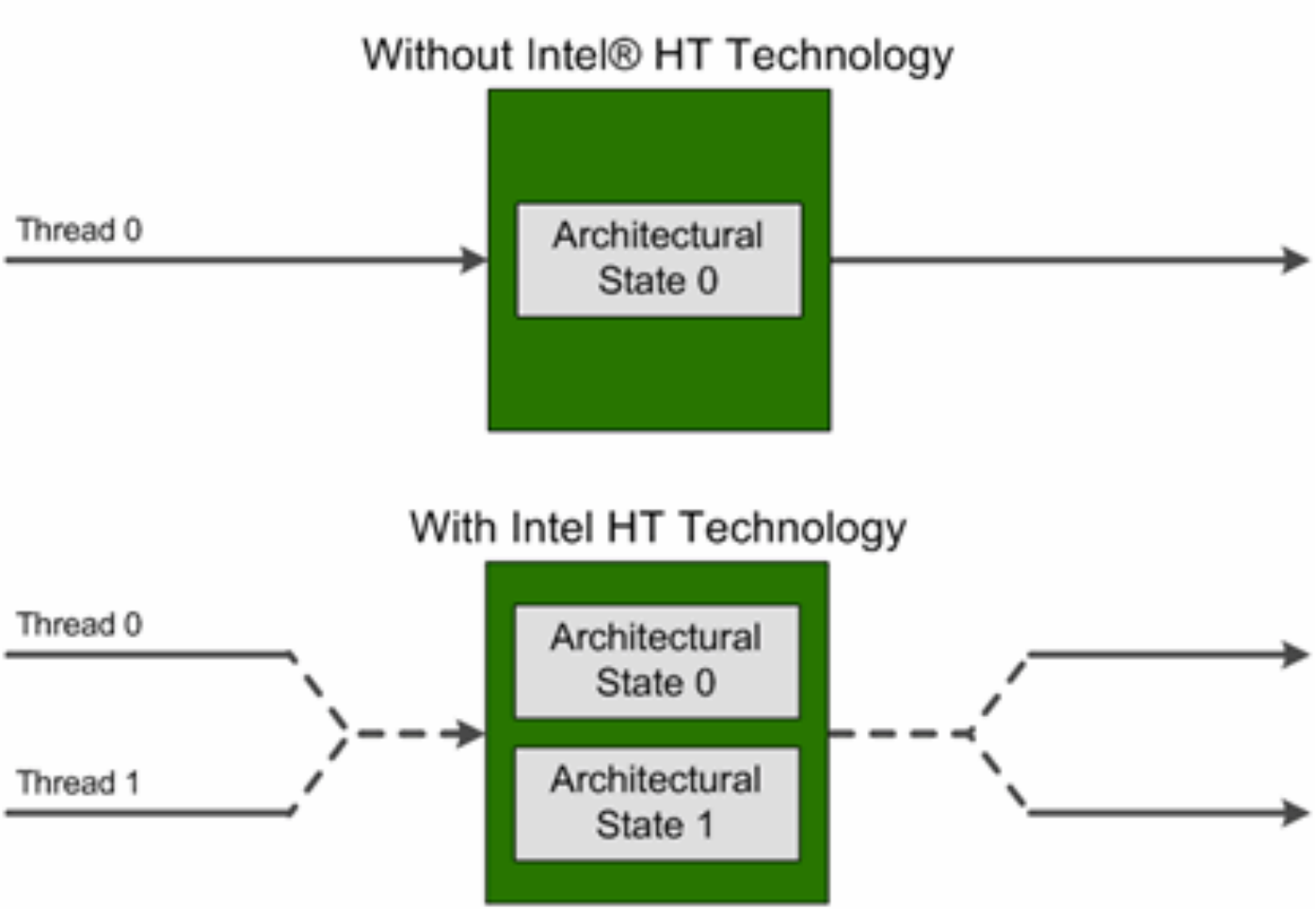
7.2.6 Công nghệ siêu phân luồng

- Công nghệ siêu phân luồng (Hyper-Threading Technology hoặc HT Technology) là công nghệ cho phép nhiều luồng thực hiện chạy đồng thời trên một CPU vật lý;
  - Intel đưa ra vào năm 2002 trên VXL Xeon và sau đó là Pen 7.
  - Công nghệ này được tiếp tục áp dụng cho các VXL họ Atom, Core I và nhiều họ VXL khác;
  - Đòi hỏi hệ điều hành phải hỗ trợ đa xử lý và nhiều luồng đồng thời (SMT-Simultaneous Multi-threading).
- Công nghệ siêu phân luồng được thiết kế nhằm cải thiện khả năng xử lý song song:
  - Mỗi CPU/nhân vật lý có khả năng thực hiện 2 luồng ảo;
  - Các luồng ảo có khả năng chia sẻ tài nguyên và công việc.

7.2.6 Công nghệ siêu phân luồng



7.2.6 Công nghệ siêu phân luồng



7.2.6 Công nghệ siêu phân luồng

- Công nghệ siêu phân luồng được thực hiện bằng cách:
  - Mỗi CPU ảo có một số thành phần riêng, thường là phần lưu trạng thái kiến trúc (Architectural state), gồm đầy đủ tập các thanh ghi của nó: thanh ghi dữ liệu, đoạn, điều khiển và debug;
  - Các CPU ảo chia sẻ thành phần thực hiện lệnh của CPU vật lý.
- Hệ điều hành "nhìn thấy" một CPU hỗ trợ công nghệ siêu phân luồng như 2 CPU logic:
  - Cho phép HĐH lập lịch xử lý các luồng song song trên các CPU ảo.
  - Khi một luồng bị dừng vì một lý do nào đó, HĐH có thể cấp phát tài nguyên của CPU vật lý cho luồng khác, giúp cải thiện hiệu năng.

7.2.6 Công nghệ siêu phân luồng

- Tối ưu hoá HĐH trong hệ thống hỗ trợ siêu phân luồng:
  - Một hệ thống có 2 CPU vật lý, mỗi CPU vật lý hỗ trợ 2 CPU ảo → tổng cộng có 4 CPU ảo;
  - Nếu bộ lập lịch (scheduler) của HĐH không hỗ trợ siêu phân luồng, nó sẽ coi 4 CPU ảo là ngang nhau;
  - Nếu tại một thời điểm chỉ có yêu cầu chạy 2 luồng thực hiện, HĐH có thể chọn 2 CPU ảo của cùng 1 CPU vật lý chạy 2 luồng này;
  - Kết quả là 1 CPU vật lý thì tải rất cao, còn CPU kia thì rỗi → hiệu năng có thể kém hơn hệ không hỗ trợ siêu phân luồng.
  - Để tránh hiện tượng này, HĐH phải có khả năng phân biệt CPU vật lý và CPU ảo để lập lịch cho phù hợp.

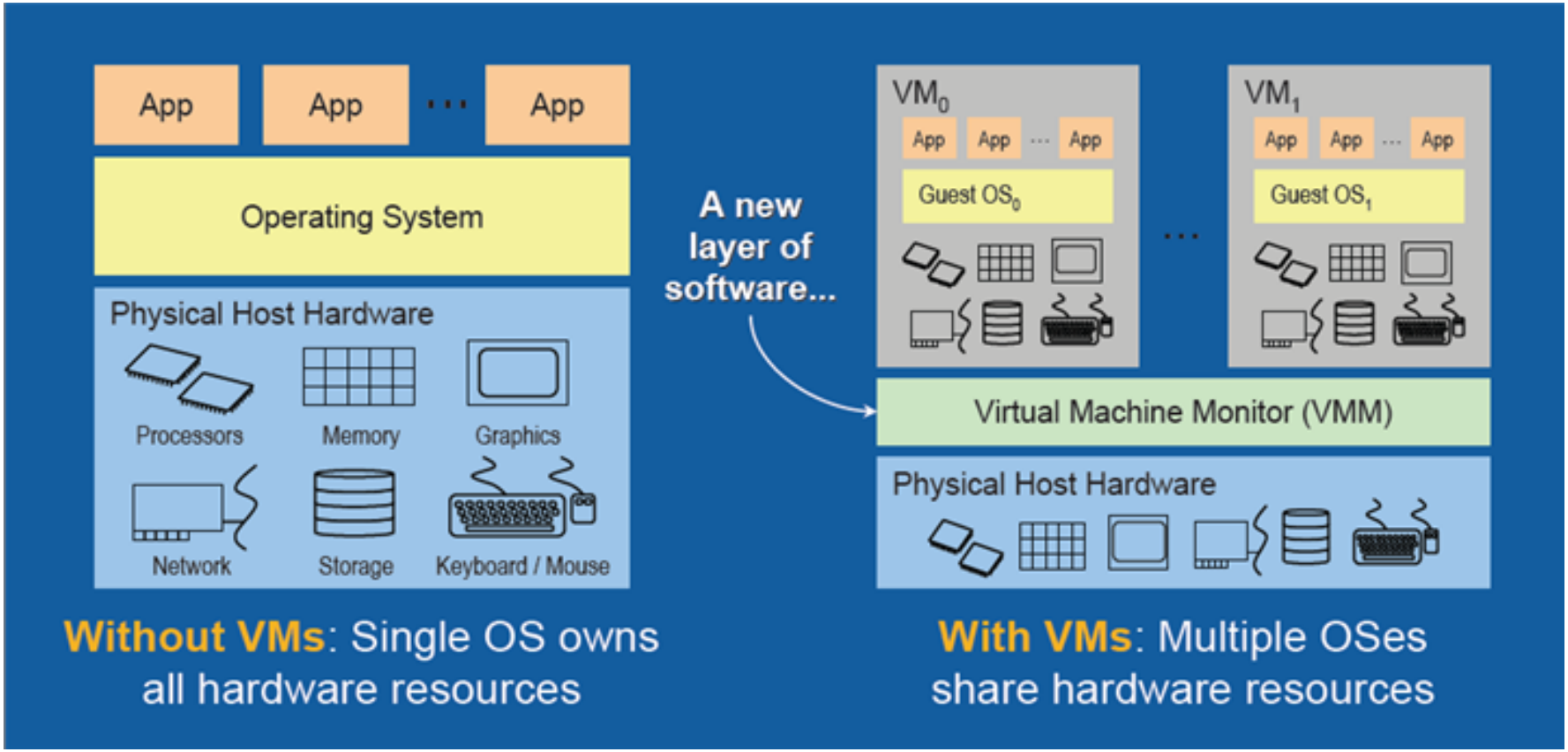
7.2.6 Công nghệ siêu phân luồng

- Hiệu năng của siêu phân luồng:
  - Cải thiện hiệu năng cho các ứng dụng đa luồng;
  - Cho phép nhiều luồng được thực hiện đồng thời;
  - Cải thiện được khả năng đáp ứng của ứng dụng.
- Số liệu thực nghiệm trên công nghệ siêu phân luồng:
  - Tăng diện tích đế CPU khoảng 5% so với CPU không hỗ trợ siêu phân luồng;
  - Hiệu năng theo Intel công bố tăng thêm khoảng 15-30%;
  - Theo thực nghiệm của Tom's Hardware, Pentium 4 3.0 GHz có HT nhanh hơn Pentium 4 3.6 GHz tắt HT.
  - Hiệu năng thực phụ thuộc vào ứng dụng: nếu chạy đồng thời 2 chương trình nặng tải, thì một hoặc cả 2 chạy chậm hơn khi có HT.

7.2.7 Công nghệ ảo hóa

- Công nghệ ảo hoá (Virtualization Technology):
  - Là sự kết hợp của các công nghệ phần cứng và phần mềm để tạo ra các máy ảo (Virtual Machines (VMs));
  - Cho phép trừu tượng hoá phần cứng để một máy tính có thể hoạt động giống như có nhiều máy tính.
- Ưu điểm của công nghệ ảo hoá:
  - Giảm số máy vật lý, nhưng vẫn đảm bảo số nền tảng đa dạng theo yêu cầu;
  - Tiết kiệm không gian vật lý, điện năng và các tiện ích phục vụ khác;
  - Hữu ích trong việc phát triển và kiểm thử phần mềm – cần nhiều môi trường để test;
  - Hỗ trợ việc cân bằng tải động và khôi phục sau sự cố;
  - Được sử dụng nhiều trong điện toán đám mây → dịch vụ hoá tài nguyên phần cứng.

7.2.7 Công nghệ ảo hóa



7.2.7 Công nghệ ảo hóa

- Virtual Machine Monitor (VMM)
  - VMM là thành phần trung tâm của công nghệ ảo hoá
  - Điểm khó khăn nhất trong thiết kế VMM là vấn đề điều khiển sử dụng tài nguyên vật lý một cách hiệu quả:
    - Vấn đề ánh xạ bộ nhớ
    - Vấn đề ánh xạ các thiết bị vào ra
- Hỗ trợ ảo hoá của CPU giúp cho:
  - Giảm tải cho các thao tác của VMM
  - Tăng tốc và năng lực của VMM
  - Giảm độ phức tạp khi phát triển VMM
  - Giúp VMM chia sẻ tài nguyên phần cứng hiệu quả hơn.

7.2.7 CN ảo hóa – Một số phần mềm tạo máy ảo

- Phần mềm tạo máy ảo chạy như một ứng dụng trên một hệ điều hành nền:
  - Microsoft Windows Virtual PC
  - VMWare Workstation, VMWare Server
  - Oracle VM
  - KVM
  - Sun xVM
  - VirtualBox
  - IBM VM
- Phần mềm tạo máy ảo thường chậm, hỗ trợ số lượng hạn chế máy ảo và phụ thuộc vào năng lực của hệ điều hành nền. Thích hợp với người sử dụng đơn lẻ.

7.2.7 CN ảo hóa – Một số phần mềm tạo máy ảo

- Phần mềm tạo máy ảo chạy như một hệ điều hành nền:
  - Microsoft Hyper-V
  - VMware vSphere Hypervisor
  - Linux-VServer
  - Solaris Containers
  - OpenVZ
  - FreeVPS
- Đặc điểm:
  - Được cài đặt trực tiếp lên phần cứng vật lý, trực tiếp quản lý và tối ưu hoá cho chia sẻ tài nguyên phần cứng;
  - Hỗ trợ nhiều máy ảo với tốc độ cao.
  - Thích hợp với ảo hoá máy chủ, tạo máy chủ ảo.

7.2.7 CN ảo hóa – Ví dụ