**Manual do Desenvolvedor de Software das Arquiteturas Intel® 64 e IA-32 Volumes Combinados: 1, 2A, 2B, 2C, 2D, 3A, 3B, 3C, 3D e 4**

**Sobre:**

Traduzi este artigo utilizando o ChatGPT, unicamente para fins de estudo

NOTA: Este documento contém os quatro volumes do Manual do Desenvolvedor de Software das Arquiteturas Intel 64 e IA-32: Arquitetura Básica, Número de Pedido 253665; Referência de Conjunto de Instruções A-Z, Número de Pedido 325383; Guia de Programação do Sistema, Número de Pedido 325384; Registradores Específicos do Modelo, Número de Pedido 335592. Consulte os quatro volumes ao avaliar suas necessidades de design.

**Manual do Desenvolvedor de Software das Arquiteturas Intel® 64 e IA-32**

**Volume 1:** Arquitetura Básica

**Capítulo 1**

Fornece uma visão geral do Manual do Desenvolvedor de Software das Arquiteturas Intel® 64 e IA-32, Volume 1: Arquitetura Básica. Este volume faz parte de um conjunto maior de manuais que descrevem coletivamente a arquitetura e o ambiente de programação dos processadores da arquitetura Intel® 64 e IA-32.

**Sobre Este Manual:** Esta seção introduz o propósito e o escopo do manual. Ela explica que o Volume 1 se concentra na arquitetura básica e no ambiente de programação dos processadores Intel 64 e IA-32. Também lista os outros volumes do conjunto, que abrangem referências ao conjunto de instruções, guias de programação do sistema e registros específicos do modelo.

**Descrição de Outros Volumes:** Ele descreve brevemente o conteúdo e o propósito de outros volumes no conjunto:

Volumes 2A, 2B, 2C e 2D: Estes volumes descrevem o conjunto de instruções do processador e a estrutura do código de operação, principalmente para programadores de aplicativos e aqueles que escrevem sistemas operacionais ou executáveis.

Volumes 3A, 3B, 3C e 3D: Estes volumes descrevem o ambiente de suporte ao sistema operacional dos processadores Intel 64 e IA-32, direcionando principalmente designers de sistemas operacionais e BIOS. O Volume 3B também aborda o ambiente de programação para software que hospeda sistemas operacionais.

Volume 4: Este volume fornece detalhes sobre os registros específicos do modelo dos processadores Intel 64 e IA-32.

Em essência, o Volume 1 serve como uma introdução às arquiteturas Intel® 64 e IA-32, enquanto os outros volumes exploram aspectos mais específicos dessas arquiteturas, tornando-os referências úteis para vários tipos de programadores e projetistas de sistemas.

**1.2 OVERVIEW OF VOLUME 1: BASIC ARCHITECTURE**

A description of this manual’s content follows:

Chapter 1 — About This Manual. Gives an overview of all volumes of the Intel® 64 and IA-32 Architectures Soft-

ware Developer’s Manual. It also describes the notational conventions in these manuals and lists related Intel

manuals and documentation of interest to programmers and hardware designers.

Chapter 2 — Intel® 64 and IA-32 Architectures. Introduces the Intel 64 and IA-32 architectures along with the

families of Intel processors that are based on these architectures. It also gives an overview of the common features

found in these processors and brief history of the Intel 64 and IA-32 architectures.

Chapter 3 — Basic Execution Environment. Introduces the models of memory organization and describes the

register set used by applications.

Chapter 4 — Data Types. Describes the data types and addressing modes recognized by the processor; provides

an overview of real numbers and floating-point formats and of floating-point exceptions.

Capítulo 5 - Resumo do Conjunto de Instruções: Lista todas as instruções Intel 64 e IA-32, divididas em grupos de tecnologia.

Capítulo 6 - Chamadas de Procedimento, Interrupções e Exceções: Descreve a pilha de procedimentos e os mecanismos fornecidos para fazer chamadas de procedimentos e para atender interrupções e exceções.

Capítulo 7 - Programação com Instruções de Uso Geral: Descreve instruções básicas de carga e armazenamento, controle de programa, aritmética e instruções de cadeia que operam em tipos de dados básicos, registros de uso geral e de segmento; também descreve instruções de sistema executadas no modo protegido.

Capítulo 8 - Programação com a Unidade de Ponto Flutuante x87: Descreve a unidade de ponto flutuante x87 (FPU), incluindo registros e tipos de dados de ponto flutuante; fornece uma visão geral do conjunto de instruções de ponto flutuante e descreve as condições de exceção de ponto flutuante do processador.

Capítulo 9 - Programação com a Tecnologia Intel® MMX™: Descreve a tecnologia Intel MMX, incluindo registros e tipos de dados MMX; também fornece uma visão geral do conjunto de instruções MMX.

Capítulo 10 - Programação com as Extensões Intel® Streaming SIMD (Intel® SSE): Descreve as extensões SSE, incluindo registros XMM, o registro MXCSR e tipos de dados de ponto flutuante de precisão simples empacotados; fornece uma visão geral do conjunto de instruções SSE e diretrizes para escrever código que acessa as extensões SSE.

Capítulo 11 - Programação com as Extensões Intel® Streaming SIMD 2 (Intel® SSE2): Descreve as extensões SSE2, incluindo registros XMM e tipos de dados de ponto flutuante de precisão dupla empacotados; fornece uma visão geral do conjunto de instruções SSE2 e diretrizes para escrever código que acessa as extensões SSE2. Este capítulo também descreve exceções de ponto flutuante SIMD que podem ser geradas com instruções SSE e SSE2 e fornece diretrizes gerais para incorporar suporte para as extensões SSE e SSE2 em código de sistema operacional e aplicativos.

Capítulo 12 - Programação com as Extensões Intel® Streaming SIMD 3 (Intel® SSE3), Extensões Suplementares Intel® Streaming SIMD 3 (SSSE3), Extensões Intel® Streaming SIMD 4 (Intel® SSE4) e Instruções Intel® AES New (Intel® AES-NI): Fornece uma visão geral do conjunto de instruções SSE3, SSE4, instruções AESNI e diretrizes para escrever código que acessa essas extensões.

Capítulo 13 - Gerenciamento de Estado Usando o Conjunto de Recursos XSAVE: Descreve as instruções do conjunto de recursos XSAVE e explica como o software pode habilitar o conjunto de recursos XSAVE e recursos habilitados pelo XSAVE.

Capítulo 14 - Programação com Intel® AVX, FMA e Intel® AVX2: Fornece uma visão geral do conjunto de instruções Intel® AVX, FMA e Intel® AVX2 e fornece diretrizes para escrever código que acessa essas extensões.

Capítulo 15 - Programação com Intel® AVX-512: Fornece uma visão geral das extensões de conjunto de instruções Intel® AVX-512 e fornece diretrizes para escrever código que acessa essas extensões.

Capítulo 16 - Programação com as Extensões de Sincronização Transacional da Intel: Descreve as extensões de instrução que suportam técnicas de elisão de bloqueio para melhorar o desempenho de software multithreaded com bloqueios contended.

Capítulo 17 - Tecnologia de Aplicação de Controle de Fluxo: Fornece uma visão geral da Tecnologia de Aplicação de Controle de Fluxo (CET) e diretrizes para escrever código que acessa essas extensões.

Capítulo 18 - Programação com as Extensões Avançadas de Matriz da Intel: Fornece uma visão geral das Extensões Avançadas de Matriz da Intel e diretrizes para escrever código que acessa essas extensões.

Capítulo 19 - Entrada/Saída: Descreve o mecanismo de E/S do processador, incluindo endereçamento de porta de E/S, instruções de E/S e mecanismos de proteção de E/S.

Capítulo 20 - Identificação e Determinação de Recursos do Processador: Descreve como determinar o tipo de CPU e os recursos disponíveis no processador.

Apêndice A - Referência Cruzada EFLAGS: Resume como as instruções IA-32 afetam as flags no registro EFLAGS.

Apêndice B - Códigos de Condição EFLAGS: Resume como instruções de salto condicional, movimento e "byte set on condition code" usam as flags de condição (OF, CF, ZF, SF e PF) no registro EFLAGS.

Apêndice C - Resumo de Exceções de Ponto Flutuante: Resume exceções geradas pelas instruções de ponto flutuante da FPU x87 e SSE/SSE2/SSE3.

Apêndice D - Diretrizes para Escrever Manipuladores de Exceção de Ponto Flutuante SIMD: Fornece diretrizes para escrever manipuladores de exceção para exceções geradas por instruções de ponto flutuante SIMD SSE/SSE2/SSE3.

Apêndice E - Extensões de Proteção de Memória da Intel: Fornece uma visão geral das Extensões de Proteção de Memória da Intel, um recurso que foi obsoleto e não estará disponível em processadores futuros.

**1.3 CONVENÇÕES NOTACIONAIS**

Este manual utiliza notações específicas para formatos de estrutura de dados, representação simbólica de instruções e números hexadecimais e binários. Essa notação é descrita abaixo.

**1.3.1 Ordem de Bits e Bytes**

Em ilustrações de estruturas de dados na memória, os endereços menores aparecem na parte inferior da figura; os endereços aumentam em direção ao topo. As posições dos bits são numeradas da direita para a esquerda. O valor numérico de um bit definido é igual a dois elevado à potência da posição do bit. Os processadores Intel 64 e IA-32 são máquinas "little endian"; isso significa que os bytes de uma palavra são numerados a partir do byte menos significativo. Consulte a Figura 1-1.

Tabela

Descrição gerada automaticamente

**1.3.2 Bits Reservados e Compatibilidade de Software**

Em muitas descrições de registros e leiautes de memória, certos bits são marcados como reservados. Quando bits são marcados como reservados, é essencial, para compatibilidade com futuros processadores, que o software trate esses bits como tendo um efeito futuro, embora desconhecido. O comportamento dos bits reservados deve ser considerado não apenas indefinido, mas imprevisível.

O software deve seguir estas diretrizes ao lidar com bits reservados:

* Não dependa dos estados de quaisquer bits reservados ao testar os valores de registros que contenham tais bits. Máscare os bits reservados antes do teste.
* Não dependa dos estados de quaisquer bits reservados ao armazenar na memória ou em um registro.
* Não dependa da capacidade de reter informações escritas em quaisquer bits reservados.
* Ao carregar um registro, sempre carregue os bits reservados com os valores indicados na documentação, se houver, ou recarregue-os com os valores lidos anteriormente do mesmo registro.

**NOTA:** Evite qualquer dependência de software em relação ao estado de bits reservados em registros Intel 64 e IA-32. Depender dos valores de bits de registro reservados tornará o software dependente da maneira não especificada pela qual o processador trata esses bits. Programas que dependem de valores reservados correm o risco de incompatibilidade com processadores futuros.

**1.3.2.1 Operandos de Instrução**

Quando as instruções são representadas de forma simbólica, é usada uma parte da linguagem Assembly IA-32. Nessa parte, uma instrução tem o seguinte formato:

rótulo: mnemônico argumento1, argumento2, argumento3

onde:

• Um rótulo é um identificador seguido de dois pontos.

• Um mnemônico é um nome reservado para uma classe de códigos de operação de instrução que têm a mesma função.

• Os operandos argumento1, argumento2 e argumento3 são opcionais. Pode haver de zero a três operandos, dependendo do código de operação. Quando presentes, eles têm a forma de literais ou identificadores de itens de dados. Os identificadores de operandos são nomes reservados de registros ou são assumidos como atribuídos a itens de dados declarados em outra parte do programa (que podem não ser mostrados no exemplo).

Quando dois operandos estão presentes em uma instrução aritmética ou lógica, o operando à direita é a fonte e o operando à esquerda é o destino.

Por exemplo:

LOADREG: MOV EAX, SUBTOTAL

Neste exemplo, LOADREG é um rótulo, MOV é o identificador mnemônico de um código de operação, EAX é o operando de destino e SUBTOTAL é o operando de origem. Algumas linguagens Assembly colocam a origem e o destino na ordem inversa.

**1.3.3 Números Hexadecimais e Binários**

Números na base 16 (hexadecimais) são representados por uma sequência de dígitos hexadecimais seguida pelo caractere H (por exemplo, 0F82EH). Um dígito hexadecimal é um caractere do seguinte conjunto: 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E e F.

Números na base 2 (binários) são representados por uma sequência de 1s e 0s, às vezes seguidos pelo caractere B (por exemplo, 1010B). A designação "B" é usada apenas em situações em que possa haver confusão quanto ao tipo de número.

**1.3.4 Endereçamento Segmentado**

O processador utiliza o endereçamento por byte. Isso significa que a memória é organizada e acessada como uma sequência de bytes. Independentemente de um ou mais bytes estarem sendo acessados, um endereço de byte é usado para localizar o byte ou bytes na memória. A faixa de memória que pode ser endereçada é chamada de espaço de endereço.

O processador também suporta o endereçamento segmentado. Este é uma forma de endereçamento em que um programa pode ter muitos espaços de endereço independentes, chamados segmentos. Por exemplo, um programa pode manter seu código (instruções) e pilha em segmentos separados. Os endereços de código sempre se refeririam ao espaço de código, e os endereços de pilha sempre se refeririam ao espaço de pilha. A seguinte notação é usada para especificar um endereço de byte dentro de um segmento:

Registrador-de-segmento: Endereço-de-byte

Por exemplo, o seguinte endereço de segmento identifica o byte no endereço FF79H no segmento apontado pelo registrador DS:

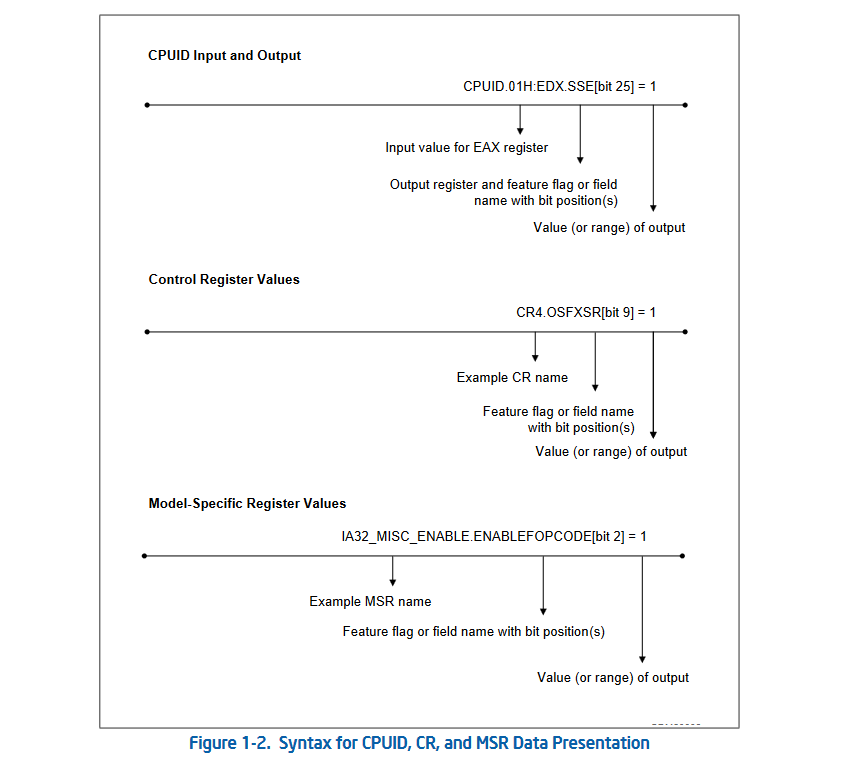
DS:FF79H

O seguinte endereço de segmento identifica um endereço de instrução no segmento de código. O registro CS aponta para o segmento de código e o registro EIP contém o endereço da instrução.

CS:EIP

**1.3.5 Uma Nova Sintaxe para Valores de CPUID, CR e MSR**

Obtenha informações sobre recursos, status e informações do sistema usando a instrução CPUID, verificando os bits dos registradores de controle e lendo registradores específicos do modelo. Estamos adotando uma nova sintaxe para representar essas informações. Consulte a Figura 1-2.



**1.3.6 Exceções**

Uma exceção é um evento que normalmente ocorre quando uma instrução causa um erro. Por exemplo, uma tentativa de dividir por zero gera uma exceção. No entanto, algumas exceções, como pontos de interrupção (breakpoints), ocorrem em outras condições. Alguns tipos de exceções podem fornecer códigos de erro. Um código de erro relata informações adicionais sobre o erro. Um exemplo da notação usada para mostrar uma exceção e um código de erro é mostrado abaixo:

#PF(código de falha)

Este exemplo se refere a uma exceção de falha de página em condições em que um código de erro que nomeia um tipo de falha é relatado. Em algumas condições, exceções que produzem códigos de erro podem não ser capazes de relatar um código preciso. Nesse caso, o código de erro é zero, como mostrado abaixo para uma exceção de proteção geral:

#GP(0)

**1.4 LITERATURA RELACIONADA**

A literatura relacionada aos processadores Intel 64 e IA-32 está listada e disponível online em:

https://software.intel.com/en-us/articles/intel-sdm

Veja também:

• As informações mais recentes sobre segurança dos produtos Intel®:

https://www.intel.com/content/www/us/en/security-center/default.html

• Recursos, orientações e informações para desenvolvedores de software sobre avisos de segurança:

https://software.intel.com/security-software-guidance/

• A ficha técnica de um processador Intel 64 ou IA-32 específico

• A atualização de especificações para um processador Intel 64 ou IA-32 específico

• Documentação e ajuda online do Intel® C++ Compiler:

http://software.intel.com/en-us/articles/intel-compilers/

• Documentação e ajuda online do Intel® Fortran Compiler:

http://software.intel.com/en-us/articles/intel-compilers/

• Ferramentas de desenvolvimento de software da Intel®:

https://software.intel.com/en-us/intel-sdp-home

• Manual do Desenvolvedor de Software das Arquiteturas Intel® 64 e IA-32 (em um, quatro ou dez volumes):

https://software.intel.com/en-us/articles/intel-sdm

• Manual de Referência de Otimização das Arquiteturas Intel® 64 e IA-32:

https://software.intel.com/en-us/articles/intel-sdm#optimization

• Guia de Programação do Ambiente Inicial Medido da Tecnologia de Execução Confiável Intel® (Intel® TXT):

http://www.intel.com/content/www/us/en/software-developers/intel-txt-software-development-guide.html

• Informações sobre as Extensões de Guarda de Software Intel® (Intel® SGX)

https://software.intel.com/en-us/isa-extensions/intel-sgx

• Desenvolvimento de Aplicações Multithread: Uma Abordagem Plataforma Consistente:

https://software.intel.com/sites/default/files/article/147714/51534-developing-multithreaded-applica-

tions.pdf

• Uso de Laços de Espera (Spin-Loops) nos Processadores Intel® Pentium® 4 e Intel® Xeon®:

https://software.intel.com/sites/default/files/22/30/25602

• Guia de Compartilhamento da Unidade de Monitoramento de Desempenho

http://software.intel.com/file/30388

A literatura relacionada a recursos selecionados em futuros processadores Intel está disponível em:

• Referência de Programação das Extensões de Conjunto de Instruções da Arquitetura Intel®:

https://software.intel.com/en-us/isa-extensions

Links mais relevantes:

• Zona de Desenvolvedores da Intel®:

<https://software.intel.com/en-us>

• Centros de desenvolvedores:

http://www.intel.com/content/www/us/en/hardware-developers/developer-centers.html

• Link geral de suporte de processadores:

http://www.intel.com/support/processors/

• Tecnologia Intel® Hyper-Threading (Tecnologia Intel® HT):

<http://www.intel.com/technology/platform-technology/hyper-threading/index.htm>

Capítulo 2 ARQUITETURAS INTEL® 64 E IA-32

**2.1 BREVE HISTÓRIA DA ARQUITETURA INTEL® 64 E IA-32**

As seções a seguir fornecem um resumo das principais evoluções técnicas da arquitetura desde o IA-32 até a arquitetura Intel 64, começando com o processador Intel 8086 até os processadores Intel® Core® 2 Duo, Core 2 Quad e Intel Xeon das séries 5300 e 7300. O código-objeto criado para processadores lançados a partir de 1978 ainda é executado nos processadores mais recentes nas famílias de arquitetura Intel 64 e IA-32.

**2.1.1 Processadores de 16 bits e Segmentação (1978)**

A família de arquitetura IA-32 foi precedida por processadores de 16 bits, o 8086 e o 8088. O 8086 possui registradores de 16 bits e um barramento de dados externo de 16 bits, com um espaço de endereçamento de 20 bits, proporcionando um espaço de endereço de 1 megabyte. O 8088 é semelhante ao 8086, exceto pelo barramento de dados externo de 8 bits.

O 8086/8088 introduziu a segmentação na arquitetura IA-32. Com a segmentação, um registro de segmento de 16 bits contém um ponteiro para um segmento de memória de até 64 KBytes. Usando quatro registros de segmento de cada vez, os processadores 8086/8088 podem endereçar até 256 KBytes sem alternar entre segmentos. Os endereços de 20 bits que podem ser formados usando um registro de segmento e um ponteiro adicional de 16 bits fornecem um intervalo total de endereço de 1 megabyte.

**2.1.2 O Processador Intel® 286 (1982)**

O processador Intel 286 introduziu a operação em modo protegido na arquitetura IA-32. O modo protegido usa o conteúdo do registro de segmento como seletores ou ponteiros em tabelas de descritores. Os descritores fornecem endereços de base de 24 bits com um tamanho de memória física de até 16 megabytes, suporte para gerenciamento de memória virtual com troca de segmentos e diversos mecanismos de proteção. Esses mecanismos incluem:

* Verificação de limite do segmento.
* Opções de segmento somente leitura e somente execução.
* Quatro níveis de privilégio.

**2.1.3 O Processador Intel386™ (1985)**

O processador Intel386 foi o primeiro processador de 32 bits na família de arquitetura IA-32. Ele introduziu registradores de 32 bits para uso tanto na manutenção de operandos quanto no endereçamento. A metade inferior de cada registro Intel386 de 32 bits mantém as propriedades dos registradores de 16 bits das gerações anteriores, permitindo a compatibilidade retroativa. O processador também fornece um modo virtual-8086 que permite uma eficiência ainda maior ao executar programas criados para processadores 8086/8088.

Além disso, o processador Intel386 oferece suporte para:

* Um barramento de endereços de 32 bits que suporta até 4 gigabytes de memória física.
* Um modelo de memória segmentada e um modelo de memória plana.
* Paginação, com um tamanho de página fixo de 4 kilobytes, fornecendo um método para gerenciamento de memória virtual.
* Suporte para estágios paralelos.

**2.1.4 O Processador Intel486™ (1989)**

O processador Intel486™ adicionou mais capacidade de execução paralela, expandindo as unidades de decodificação e execução de instruções do processador Intel386 em cinco estágios pipelined. Cada estágio opera em paralelo com os outros em até cinco instruções em diferentes estágios de execução.

**2.1.5 O Processador Intel® Pentium® (1993)**

A introdução do processador Intel Pentium adicionou um segundo pipeline de execução para alcançar um desempenho superscalar (dois pipelines, conhecidos como u e v, juntos podem executar duas instruções por ciclo de clock). A memória cache de primeiro nível on-chip duplicou, com 8 KBytes dedicados a código e mais 8 KBytes dedicados a dados. A cache de dados utiliza o protocolo MESI para suportar uma cache de escrita de volta mais eficiente, além da cache de escrita direta anteriormente usada pelo processador Intel486. A previsão de desvio com uma tabela de desvios on-chip foi adicionada para aumentar o desempenho em construções de loops.

Além disso, o processador adicionou:

* Extensões para tornar o modo virtual-8086 mais eficiente e permitir páginas de 4 MBytes, além de 4 KBytes.
* Caminhos internos de dados de 128 e 256 bits para acelerar as transferências internas de dados.
* O barramento de dados externo burst foi aumentado para 64 bits.
* Um APIC para suportar sistemas com múltiplos processadores.
* Um modo de processador duplo para suportar sistemas de dois processadores sem a necessidade de um circuito adicional.

Uma versão subsequente da família Pentium introduziu a tecnologia Intel MMX (o processador Pentium com tecnologia MMX da Intel). A tecnologia Intel MMX utiliza o modelo de execução de instruções múltiplas, dados múltiplos (SIMD) para realizar cálculos paralelos em dados inteiros compactados contidos em registradores de 64 bits. Consulte a Seção 2.2.7, "Instruções SIMD".

**2.1.6 A Família de Processadores P6 (1995-1999)**

A família de processadores P6 foi baseada em uma microarquitetura superscalar que estabeleceu novos padrões de desempenho; consulte também a Seção 2.2.1, "Microarquitetura da Família P6". Um dos objetivos no design da microarquitetura da família P6 era superar significativamente o desempenho do processador Pentium, enquanto usava o mesmo processo de fabricação BICMOS de quatro camadas de 0,6 micrômetros. Os membros desta família incluem:

* O processador Intel Pentium Pro é superscalar de três vias. Usando técnicas de processamento paralelo, o processador é capaz, em média, de decodificar, despachar e concluir a execução de (retirar) três instruções por ciclo de clock. O Pentium Pro introduziu a execução dinâmica (análise de microdados de fluxo, execução fora de ordem, previsão de desvio superior e execução especulativa) em uma implementação superscalar. O processador foi ainda aprimorado por suas caches. Ele possui as mesmas duas caches de primeiro nível de 8 KBytes on-chip que o processador Pentium e uma cache de segundo nível de 256 KBytes no mesmo pacote do processador.
* O processador Intel Pentium II adicionou a tecnologia Intel MMX aos processadores da família P6, juntamente com novos invólucros e várias melhorias de hardware. O núcleo do processador é embalado na cápsula de contato de borda única (SECC). As caches de dados e instruções de primeiro nível foram ampliadas para 16 KBytes cada, e são suportados tamanhos de cache de segundo nível de 256 KBytes, 512 KBytes e 1 MByte. Um barramento de backside de meia frequência conecta a cache de segundo nível ao processador. Múltiplos estados de baixo consumo de energia, como AutoHALT, Stop-Grant, Sleep e Deep Sleep, são suportados para economizar energia durante a ociosidade.
* O processador Pentium II Xeon combinou as características premium das gerações anteriores de processadores Intel. Isso inclui escalabilidade de 4 vias, 8 vias (e superior) e uma cache de segundo nível de 2 MBytes em execução em um barramento de backside de frequência total.
* A família de processadores Intel Celeron concentrou-se no segmento de mercado de PCs de valor. Sua introdução oferece 128 KBytes de cache de segundo nível integrada e um fator de forma de matriz de pinos de plástico (P.P.G.A.) para reduzir o custo de design do sistema.
* O processador Intel Pentium III introduziu as Extensões Streaming SIMD (SSE) na arquitetura IA-32. As extensões SSE expandem o modelo de execução SIMD introduzido com a tecnologia Intel MMX, fornecendo um novo conjunto de registradores de 128 bits e a capacidade de realizar operações SIMD em valores de ponto flutuante de precisão simples compactados. Consulte a Seção 2.2.7, "Instruções SIMD".
* O processador Pentium III Xeon estendeu os níveis de desempenho dos processadores IA-32 com o aprimoramento de uma cache de transferência avançada no chip e em velocidade total.

**2.1.7 A Família de Processadores Intel® Pentium® 4 (2000-2006)**

A família de processadores Intel Pentium 4 é baseada na microarquitetura Intel NetBurst; consulte a Seção 2.2.2, "Microarquitetura Intel NetBurst®". O processador Intel Pentium 4 introduziu as Extensões de Conjunto de Instruções SIMD 2 (SSE2); consulte a Seção 2.2.7, "Instruções SIMD". O processador Intel Pentium 4 de 3,40 GHz, que suporta a Tecnologia Hyper-Threading, introduziu as Extensões de Conjunto de Instruções SIMD 3 (SSE3); consulte a Seção 2.2.7, "Instruções SIMD". A arquitetura Intel 64 foi introduzida no processador Intel Pentium 4 Extreme Edition, que suporta a Tecnologia Hyper-Threading, e nas sequências de processadores Intel Pentium 4 6xx e 5xx. A Tecnologia de Virtualização Intel® (Intel® VT) foi introduzida nos processadores Intel Pentium 4 672 e 662.

**2.1.8 O Processador Intel® Xeon® (2001-2007)**

Os processadores Intel Xeon (com exceção do processador Intel Xeon dual-core LV e da série Intel Xeon 5100) são baseados na microarquitetura Intel NetBurst; consulte a Seção 2.2.2, "Microarquitetura Intel NetBurst®". Como família, esse grupo de processadores IA-32 (mais recentemente processadores Intel 64) foi projetado para uso em sistemas de servidor multiprocessador e estações de trabalho de alto desempenho. O processador Intel Xeon MP introduziu suporte para a Tecnologia Intel® Hyper-Threading; consulte a Seção 2.2.8, "Tecnologia Intel® Hyper-Threading". O processador Intel Xeon de 64 bits com 3,60 GHz (com um Barramento do Sistema de 800 MHz) foi usado para introduzir a arquitetura Intel 64. O processador Intel Xeon dual-core inclui tecnologia de núcleo duplo. A série de processadores Intel Xeon 70xx inclui a Tecnologia de Virtualização Intel. A série de processadores Intel Xeon 5100 introduz uma arquitetura de microarquitetura Intel Core eficiente em termos de energia e alto desempenho. Este processador é baseado na arquitetura Intel 64; ele inclui a Tecnologia de Virtualização Intel e tecnologia de núcleo duplo. A série de processadores Intel Xeon 3000 também é baseada na microarquitetura Intel Core. A série de processadores Intel Xeon 5300 introduz quatro núcleos de processador em um pacote físico, eles também são baseados na microarquitetura Intel Core.

**2.1.9 O Processador Intel® Pentium® M (2003-2006)**

A família de processadores Intel Pentium M é uma família de processadores móveis de alto desempenho e baixo consumo de energia com aprimoramentos micro-arquitetônicos em relação às gerações anteriores de processadores móveis Intel IA-32. Essa família foi projetada para estender a vida útil da bateria e integração perfeita com inovações de plataforma que permitem novos modelos de uso (como mobilidade estendida, formatos ultrafinos e redes sem fio integradas).

Sua microarquitetura aprimorada inclui:

* Suporte para a Arquitetura Intel com Execução Dinâmica.
* Um núcleo de alto desempenho e baixo consumo de energia fabricado com a tecnologia de processo avançada da Intel com interconexão de cobre.
* Cache de instruções de 32 KBytes de primeiro nível e cache de dados de 32 KBytes de escrita de volta no chip.
* Cache de segundo nível no chip (até 2 MBytes) com Arquitetura de Cache de Transferência Avançada.
* Lógica de Previsão de Desvio Avançada e Lógica de Pré-busca de Dados.
* Suporte para a tecnologia MMX, instruções SIMD de Streaming e conjunto de instruções SSE2.
* Barramento do Sistema do Processador Síncrono com a Fonte de 400 ou 533 MHz.
* Gerenciamento de energia avançado usando a tecnologia Enhanced Intel SpeedStep®.

**2.1.10 O Processador Intel® Pentium® Processor Extreme Edition (2005)**

O processador Intel Pentium Processor Extreme Edition introduziu a tecnologia de núcleo duplo. Essa tecnologia oferece suporte avançado de multithreading de hardware. O processador é baseado na microarquitetura Intel NetBurst e suporta as tecnologias Intel SSE, SSE2, SSE3, Intel Hyper-Threading Technology e Intel 64 architecture.

**2.1.11 Os Processadores Intel® Core™ Duo e Intel® Core™ Solo (2006-2007)**

O processador Intel Core Duo oferece desempenho de núcleo duplo com eficiência energética, projetado para estender a vida útil da bateria. Essa família e o processador Intel Core Solo de núcleo único oferecem aprimoramentos microarquitetônicos em relação à família de processadores Pentium M. Sua microarquitetura aprimorada inclui:

* Intel® Smart Cache, que permite o compartilhamento eficiente de dados entre dois núcleos de processador.
* Decodificação e execução SIMD melhoradas.
* Coordenação de Energia Dinâmica Intel® e Intel® Deeper Sleep aprimorada para reduzir o consumo de energia.
* Intel® Advanced Thermal Manager, que apresenta interfaces de sensor térmico digital.
* Suporte para barramento otimizado para energia de 667 MHz.

O processador Intel Xeon dual-core LV é baseado na mesma microarquitetura que o processador Intel Core Duo e suporta a arquitetura IA-32.

**2.1.12 O Processador Intel® Xeon® 5100, Série 5300 e Família de Processadores Intel® Core™ 2 (2006)**

Os processadores Intel Xeon 3000, 3200, 5100, 5300 e 7300 series, Intel Pentium Dual-Core, Intel Core 2 Extreme, Intel Core 2 Quad e a família de processadores Intel Core 2 Duo suportam a arquitetura Intel 64; eles são baseados na microarquitetura Intel® Core eficiente em termos de energia construída com tecnologia de processo de 65 nm. A microarquitetura Intel Core inclui os seguintes recursos inovadores:

* Intel® Wide Dynamic Execution para aumentar o desempenho e a taxa de execução.
* Intel® Intelligent Power Capability para reduzir o consumo de energia.
* Intel® Smart Cache Avançado, que permite o compartilhamento eficiente de dados entre dois núcleos de processador.
* Intel® Smart Memory Access para aumentar a largura de banda de dados e ocultar a latência dos acessos à memória.
* Intel® Advanced Digital Media Boost, que melhora o desempenho de aplicativos usando várias gerações de extensões SIMD de Streaming.

O processador Intel Xeon da série 5300, o processador Intel Core 2 Extreme da série QX6800 e os processadores Intel Core 2 Quad suportam a tecnologia Intel de quatro núcleos.

**2.1.13 O Processador Intel® Xeon® Série 5200, 5400, 7400 e Família de Processadores Intel® Core™ 2 (2007)**

Os processadores Intel Xeon da série 5200, 5400 e 7400, o processador Intel Core 2 Quad da série Q9000 e o processador Intel Core 2 Duo da série E8000 suportam a arquitetura Intel 64; eles são baseados na Enhanced Intel® Core microarchitecture com tecnologia de processo de 45 nm. A Enhanced Intel Core microarchitecture oferece as seguintes melhorias:

* Um divisor radix-16, que acelera ainda mais o desempenho da Intel® Wide Dynamic Execution.
* Melhora o Intel® Advanced Smart Cache com até 50% de cache de nível dois maior e até 50% de aumento na associatividade do conjunto.
* Um mecanismo de embaralhamento de 128 bits melhora significativamente o desempenho do Intel® Advanced Digital Media Boost e do SSE4.

Os processadores Intel Xeon da série 5400 e o processador Intel Core 2 Quad da série Q9000 suportam a tecnologia Intel de quatro núcleos. O processador Intel Xeon da série 7400 oferece até seis núcleos de processador e uma memória cache L3 de até 16 MBytes.

**2.1.14 Família de Processadores Intel Atom® (2008)**

A primeira geração de processadores Intel Atom® é construída com tecnologia de processo de 45 nm. Eles são baseados em uma nova microarquitetura, a microarquitetura Intel Atom®, otimizada para dispositivos de ultra baixa potência. A microarquitetura Intel Atom® apresenta dois pipelines de execução em ordem que minimizam o consumo de energia, aumentam a vida útil da bateria e permitem fatores de forma ultra pequenos. A família inicial de processadores Intel Atom e gerações subsequentes, incluindo os processadores Intel Atom D2000, N2000, E2000, Z2000, série C1000, oferecem as seguintes características:

* Tecnologia Enhanced Intel® SpeedStep®.
* Tecnologia Intel® Hyper-Threading.
* Tecnologia Deep Power Down com Dimensionamento Dinâmico de Cache.
* Suporte para extensões do conjunto de instruções, incluindo Streaming SIMD Extensions 3 (SSSE3).
* Suporte para Tecnologia de Virtualização Intel®.
* Suporte para Arquitetura Intel® 64 (exceto Intel Atom série Z5xx).

**2.1.15 Família de Processadores Intel Atom® Baseada na Microarquitetura Silvermont (2013)**

Os processadores Intel Atom da série C2xxx, E3xxx e S1xxx são baseados na microarquitetura Silvermont. Processadores baseados na microarquitetura Silvermont suportam extensões de conjunto de instruções até SSE4.2, AESNI e PCLMULQDQ.

**2.1.16 Família de Processadores Intel® Core™ i7 (2008)**

O processador Intel Core i7 da série 900 suporta a arquitetura Intel 64 e é baseado na microarquitetura Nehalem usando tecnologia de processo de 45 nm. O processador Intel Core i7 e o processador Intel Xeon da série 5500 incluem as seguintes características:

* Tecnologia Intel® Turbo Boost converte a capacidade térmica em desempenho superior.
* Tecnologia Intel® Hyper-Threading em conjunto com o Quadcore para fornecer quatro núcleos e oito threads.
* Unidade de controle de energia dedicada para reduzir o consumo de energia ativo e ocioso.
* Controlador de memória integrado no processador com suporte para três canais de memória DDR3.
* 8 MB de cache Intel® Smart Cache inclusa.
* Interconexão Intel® QuickPath (QPI) fornecendo uma conexão ponto a ponto com o chipset.
* Suporte para conjuntos de instruções SSE4.2 e SSE4.1.
* Segunda geração de Tecnologia de Virtualização Intel.

**2.1.17 Série de Processadores Intel® Xeon® 7500 (2010)**

Os processadores Intel Xeon da série 7500 e 6500 são baseados na microarquitetura Nehalem usando tecnologia de processo de 45 nm. Esses processadores suportam as mesmas características descritas na Seção 2.1.16, além das seguintes características:

* Até oito núcleos por pacote de processador físico.
* Até 24 MB de Cache Intel® Smart Cache inclusa.
* Fornece canais de Interconexão de Memória Intel® Scalable (Intel® SMI) com Intel® 7500 Scalable Memory Buffer para conectar à memória do sistema.
* RAS avançado com suporte à arquitetura de verificação de máquina recuperável por software.

**2.1.18 Família de Processadores Intel® Core™ de 2010 (2010)**

A família de processadores Intel Core de 2010 abrange os processadores Intel Core i7, i5 e i3. Esses processadores são baseados na microarquitetura Westmere usando tecnologia de processo de 32 nm. As características podem incluir:

* Oferece desempenho inteligente usando a Tecnologia Intel Hyper-Threading junto com a Tecnologia Intel Turbo Boost.
* Cache Intel Smart Cache aprimorado e controlador de memória integrado.
* Gateamento de energia inteligente.
* Plataforma reparticionada com integração em matriz de 45 nm.
* Suporte a conjuntos de instruções até AESNI, PCLMULQDQ, SSE4.2 e SSE4.1.

**2.1.19 Série de Processadores Intel® Xeon® 5600 (2010)**

Os processadores Intel Xeon da série 5600 são baseados na microarquitetura Westmere usando tecnologia de processo de 32 nm. Eles suportam as mesmas características descritas na Seção 2.1.16, além das seguintes características:

* Até seis núcleos por pacote de processador físico.
* Até 12 MB de Cache Intel® Smart Cache aprimorado.
* Suporte para conjuntos de instruções AESNI, PCLMULQDQ, SSE4.2 e SSE4.1.
* Tecnologias de virtualização Intel flexíveis em processador e E/S.

**2.1.20 Família de Processadores Intel® Core™ de Segunda Geração (2011)**

A família de processadores Intel Core de segunda geração abrange os processadores Intel Core i7, i5 e i3 baseados na microarquitetura Sandy Bridge. Esses processadores são construídos com tecnologia de processo de 32 nm e possuem recursos, incluindo:

* Tecnologia Intel Turbo Boost para processadores Intel Core i5 e i7.
* Tecnologia Intel Hyper-Threading.
* Cache Intel Smart Cache aprimorado e controlador de memória integrado.
* Gráficos do processador e recursos visuais integrados, como Intel® Quick Sync Video, Intel® InsiderTM, etc.
* Suporte a conjuntos de instruções até AVX, AESNI, PCLMULQDQ, SSE4.2 e SSE4.1.

O processador Intel Xeon da família de produtos E3-1200 também é baseado na microarquitetura Sandy Bridge.

As famílias de produtos Intel Xeon E5-2400/1400 são baseadas na microarquitetura Sandy Bridge-EP.

As famílias de produtos Intel Xeon E5-4600/2600/1600 são baseadas na microarquitetura Sandy Bridge-EP e oferecem suporte para vários soquetes.

**2.1.21 Família de Processadores Intel® Core™ de Terceira Geração (2012)**

A família de processadores Intel Core de terceira geração abrange os processadores Intel Core i7, i5 e i3 baseados na microarquitetura Ivy Bridge. As famílias de produtos Intel Xeon E7-8800/4800/2800 v2 e Intel Xeon E3-1200 v2 também são baseadas na microarquitetura Ivy Bridge.

Os processadores Intel Xeon da série E5-2400/1400 v2 são baseados na microarquitetura Ivy Bridge-EP. As famílias de produtos Intel Xeon E5-4600/2600/1600 v2 são baseadas na microarquitetura Ivy Bridge-EP e oferecem suporte para vários soquetes.

**2.1.22 Família de Processadores Intel® Core™ de Quarta Geração (2013)**

A família de processadores Intel Core de quarta geração abrange os processadores Intel Core i7, i5 e i3 baseados na microarquitetura Haswell. A família de produtos Intel Xeon E3-1200 v3 também é baseada na microarquitetura Haswell.

**2.2 MAIS SOBRE AVANÇOS ESPECÍFICOS**

As seções a seguir fornecem mais informações sobre inovações importantes.

**2.2.1 Microarquitetura da Família P6**

O processador Pentium Pro introduziu uma nova microarquitetura comumente chamada de microarquitetura do processador P6. A microarquitetura do processador P6 foi posteriormente aprimorada com um cache de nível 2 integrado, chamado de Advanced Transfer Cache.

A microarquitetura é uma arquitetura pipeline superscalar de três vias. Superscalar de três vias significa que, usando técnicas de processamento paralelo, o processador é capaz, em média, de decodificar, despachar e concluir a execução (encerrar) de três instruções por ciclo de clock. Para lidar com esse nível de taxa de instruções, a família de processadores P6 usa um superpipeline de 12 estágios desacoplados que suporta a execução de instruções fora de ordem.

A Figura 2-1 mostra uma visão conceitual do pipeline da microarquitetura do processador P6 com o aprimoramento Advanced Transfer Cache.

(Por favor, avance para a próxima seção específica ou forneça mais detalhes específicos sobre o que você gostaria de saber.)Diagrama

Descrição gerada automaticamente

Para garantir um fornecimento constante de instruções e dados para o pipeline de execução de instruções, a microarquitetura do processador P6 incorpora dois níveis de cache. O cache de Nível 1 fornece um cache de instruções de 8 KBytes e um cache de dados de 8 KBytes, ambos intimamente acoplados ao pipeline. O cache de Nível 2 fornece 256 KBytes, 512 KBytes ou 1 MByte de SRAM estático que está acoplado ao processador central por meio de um barramento de cache de 64 bits com velocidade total de clock.

O elemento central da microarquitetura do processador P6 é um mecanismo de execução fora de ordem chamado execução dinâmica. A execução dinâmica incorpora três conceitos de processamento de dados:

• Previsão profunda de branches permite que o processador decodifique instruções além dos branches para manter o pipeline de instruções cheio. A família de processadores P6 implementa algoritmos de previsão de branches altamente otimizados para prever a direção da instrução.

• Análise dinâmica do fluxo de dados requer análise em tempo real do fluxo de dados pelo processador para determinar dependências e detectar oportunidades para a execução de instruções fora de ordem. O núcleo de execução fora de ordem pode monitorar muitas instruções e executá-las na ordem que melhor otimiza o uso das unidades de execução múltipla do processador, mantendo a integridade dos dados.

• Execução especulativa refere-se à capacidade do processador de executar instruções que estão além de um branch condicional que ainda não foi resolvido e, finalmente, confirmar os resultados na ordem original da sequência de instruções. Para tornar a execução especulativa possível, a microarquitetura do processador P6 desacopla o despacho e a execução de instruções da confirmação de resultados. O núcleo de execução fora de ordem do processador usa análise de fluxo de dados para executar todas as instruções disponíveis no pool de instruções e armazenar os resultados em registradores temporários. A unidade de aposentadoria, em seguida, pesquisa linearmente o pool de instruções em busca de instruções concluídas que não possuem mais dependências de dados com outras instruções ou previsões de branches não resolvidas. Quando instruções concluídas são encontradas, a unidade de aposentadoria confirma os resultados dessas instruções na memória e/ou nos registradores IA-32 (os oito registradores de propósito geral e oito registradores de dados x87 FPU do processador) na ordem em que foram originalmente emitidas e aposenta as instruções do pool de instruções.

**2.2.2 Intel Microarquitetura Intel NetBurst®**

A microarquitetura Intel NetBurst® oferece:

* O Motor de Execução Rápida.
* Unidades Lógicas Aritméticas (ALUs) operam a uma frequência duas vezes maior que a do processador.
* Operações inteiras básicas podem ser despachadas em 1/2 ciclo de clock do processador.
* Tecnologia Hiper-Pipelined.
* Pipeline profundo para permitir taxas de clock líderes na indústria para PCs desktop e servidores.
* Margem de frequência e escalabilidade para continuar liderando no futuro.
* Execução Dinâmica Avançada.
* Motor de execução especulativa profunda e fora de ordem.
* Até 126 instruções em execução.
* Até 48 carregamentos e 24 armazenamentos no pipeline¹.
* Capacidade de previsão de branches aprimorada.
* Reduz a penalidade de previsão incorreta associada a pipelines mais profundos.
* Algoritmo de previsão de branches avançado.
* Tabela de destino de branch de 4.000 entradas.
* Novo subsistema de cache.
* Caches de primeiro nível.
  + Cache de Execução Avançada armazena instruções decodificadas.
  + Cache de Rastro de Execução remove a latência do decodificador dos loops de execução principal.
  + Cache de Rastro de Execução integra o caminho do fluxo de execução do programa em uma única linha.
  + Cache de dados de baixa latência.
* Cache de segundo nível.
  + Cache de Transferência Avançada no-die de 8 vias em velocidade total e unificada.
  + Largura de banda e desempenho aumentam com a frequência do processador.

¹ Processadores Intel 64 e IA-32 baseados na microarquitetura Intel NetBurst a 90 nm de processo podem lidar com mais de 24 armazenamentos em execução.

• Interface de barramento de alto desempenho com quádrupla bomba para o barramento do sistema da microarquitetura Intel NetBurst.

— Suporta clock de barramento escalável com quádrupla bomba para atingir velocidade efetiva até 4X.

— Capaz de fornecer até 8,5 gigabytes de largura de banda por segundo.

• Emissão superescalar para permitir o paralelismo.

• Registros de hardware expandidos com renomeação para evitar limitações no espaço de nomes dos registros.

• Tamanho de linha de cache de 64 bytes (transfere dados de até duas linhas por setor).

A Figura 2-2 é uma visão geral da microarquitetura Intel NetBurst. Esta pipeline de microarquitetura é composta por três seções: (1) a pipeline de entrada, (2) o núcleo de execução fora de ordem e (3) a unidade de aposentadoria.

Diagrama

Descrição gerada automaticamente

**2.2.2.1 A Pipeline da Etapa de Entrada**

A etapa de entrada fornece instruções em ordem de programa para o núcleo de execução fora de ordem. Ela realiza várias

funções:

• Busca instruções que provavelmente serão executadas.

• Recupera instruções que ainda não foram buscadas.

• Decodifica instruções em microoperações.

• Gera microcódigo para instruções complexas e código de propósito especial.

• Entrega instruções decodificadas do cache de rastreamento de execução.

• Prevê bifurcações usando um algoritmo altamente avançado.

A pipeline foi projetada para resolver problemas comuns em microprocessadores pipelined de alta velocidade. Dois desses

problemas contribuem para importantes fontes de atrasos:

• Tempo para decodificar instruções recuperadas do destino.

• Desperdício de largura de banda de decodificação devido a bifurcações ou alvos de bifurcação no meio de linhas de cache.

A operação do cache de rastreamento da pipeline aborda esses problemas. Instruções estão constantemente sendo buscadas e decodificadas pelo mecanismo de tradução (parte da lógica de busca/decodificação) e montadas em sequências de microoperações chamadas de rastreamentos. A qualquer momento, vários rastreamentos (que representam bifurcações pré-buscadas) estão sendo armazenados no cache de rastreamento. O cache de rastreamento é pesquisado em busca da instrução que segue a bifurcação ativa. Se a instrução também aparecer como a primeira instrução em uma bifurcação pré-buscada, a busca e decodificação de instruções na hierarquia de memória cessam, e a bifurcação pré-buscada se torna a nova fonte de instruções (consulte a Figura 2-2).

O cache de rastreamento e o mecanismo de tradução possuem hardware de previsão de bifurcação cooperativa. Os alvos de bifurcação são previstos com base em seus endereços lineares usando buffers de alvo de bifurcação (BTBs) e são buscados o mais cedo possível.

**2.2.2.2 Núcleo de Execução Fora de Ordem**

A capacidade do núcleo de execução fora de ordem de executar instruções fora de ordem é um fator-chave para permitir o paralelismo. Essa característica permite que o processador reordene as instruções de modo que, se uma microoperação for atrasada, outras microoperações possam continuar ao seu redor. O processador utiliza vários buffers para suavizar o fluxo de microoperações.

O núcleo foi projetado para facilitar a execução em paralelo. Ele pode despachar até seis microoperações por ciclo (isso excede a largura de banda do cache de rastreamento e das microoperações de aposentadoria). A maioria das pipelines pode começar a executar uma nova microoperação a cada ciclo, de modo que várias instruções podem estar em execução ao mesmo tempo para cada pipeline. Várias instruções de unidade lógica e aritmética (ALU) podem começar duas por ciclo; muitas instruções de ponto flutuante podem começar uma a cada dois ciclos.

**2.2.2.3 Unidade de Aposentadoria**

A unidade de aposentadoria recebe os resultados das microoperações executadas pelo núcleo de execução fora de ordem e processa os resultados para que o estado arquitetural seja atualizado de acordo com a ordem original do programa.

Quando uma microoperação é concluída e escreve seu resultado, ela é aposentada. Até três microoperações podem ser aposentadas por ciclo. O Buffer de Reordenação (ROB) é a unidade no processador que armazena as microoperações concluídas, atualiza o estado arquitetural na ordem e gerencia a ordenação de exceções. A seção de aposentadoria também acompanha as bifurcações e envia informações atualizadas de destino de bifurcação para o BTB. O BTB, por sua vez, elimina os rastreamentos pré-buscados que não são mais necessários.

**2.2.3 Intel® Core™ Microarchitecture**

A microarquitetura Intel Core introduz as seguintes características que permitem um alto desempenho e eficiência energética para cargas de trabalho de única e múltiplas threads:

* A Execução de Amplo Alcance da Intel permite que cada núcleo do processador busque, despache e execute em larguras de banda elevadas para suportar a aposentadoria de até quatro instruções por ciclo.
* Quatorze estágios eficientes na pipeline.
* Três unidades lógicas e aritméticas.
* Quatro decodificadores para decodificar até cinco instruções por ciclo.
* Macro-fusão e micro-fusão para melhorar o rendimento da parte frontal.
* Taxa máxima de emissão de até seis microoperações por ciclo.
* Largura de banda máxima de aposentadoria de até 4 microoperações por ciclo.
* Previsão avançada de bifurcações.
* Rastreador de ponteiro de pilha para melhorar a eficiência da execução de entradas e saídas de funções/procedimentos.
* O Cache Inteligente Avançado da Intel oferece maior largura de banda do segundo nível de cache para o núcleo e desempenho e flexibilidade ideais para aplicativos de única e múltiplas threads.
* Grande cache de segundo nível de até 4 MB e associatividade de 16 vias.
* Otimizado para ambientes de execução multicore e de única thread.
* Caminho de dados interno de 256 bits para melhorar a largura de banda do L2 para o cache de dados de primeiro nível.
* Intel® Smart Memory Access faz pré-busca de dados na memória em resposta a padrões de acesso a dados e reduz a exposição a cache-miss da execução fora de ordem.

— Pré-busca de hardware para reduzir a latência efetiva das falhas de cache de segundo nível.

— Pré-busca de hardware para reduzir a latência efetiva das falhas de cache de dados de primeiro nível.

— Desambiguação de memória para melhorar a eficiência do mecanismo de execução especulativa.

* Intel® Advanced Digital Media Boost melhora a maioria das instruções SIMD de 128 bits com taxa de transferência de um único ciclo e operações de ponto flutuante.

— Taxa de transferência de um único ciclo para a maioria das instruções SIMD de 128 bits.

— Até oito operações de ponto flutuante por ciclo.

— Três portas de emissão disponíveis para despachar instruções SIMD para execução.

Os processadores Intel Core 2 Extreme, Intel Core 2 Duo e Intel Xeon da série 5100 implementam dois núcleos de processamento com base na microarquitetura Intel Core. A funcionalidade dos subsistemas em cada núcleo está representada na Figura 2-3.

Diagrama

Descrição gerada automaticamente

**2.2.3.1 A Frente**

A frente da microarquitetura Intel Core oferece várias melhorias para alimentar o mecanismo de execução de alto desempenho Intel Wide Dynamic Execution:

* A unidade de busca de instruções pré-busca instruções em uma fila de instruções para manter um fornecimento constante de instruções para as unidades de decodificação.
* A unidade de decodificação de quatro vias pode decodificar 4 instruções por ciclo ou 5 instruções por ciclo com Macrofusion.
* A Macrofusion funde uma sequência comum de duas instruções como uma instrução decodificada (micro-ops) para aumentar o rendimento da decodificação.
* A Microfusion funde uma sequência comum de dois micro-ops como um único micro-ops para melhorar o rendimento da aposentadoria.
* A fila de instruções fornece em cache de loops curtos para melhorar a eficiência.
* O rastreador de ponteiro de pilha melhora a eficiência da execução de entradas e saídas de procedimentos/funções.
* A unidade de previsão de ramificação emprega hardware dedicado para lidar com diferentes tipos de ramificações para uma melhor previsão de ramificação.
* O algoritmo de previsão de ramificação avançada direciona a unidade de busca de instruções para buscar instruções prováveis no caminho de código arquitetural para a decodificação.

**2.2.3.2 Núcleo de Execução**

O núcleo de execução da microarquitetura Intel Core é superscalar e pode processar instruções fora de ordem para aumentar a taxa geral de instruções executadas por ciclo (IPC). O núcleo de execução emprega os seguintes recursos para melhorar o rendimento e a eficiência da execução:

* Até seis micro-ops podem ser despachados para execução por ciclo.
* Até quatro instruções podem ser aposentadas por ciclo.
* Três unidades lógicas aritméticas completas.
* Instruções SIMD podem ser despachadas por meio de três portas de emissão.
* A maioria das instruções SIMD tem um throughput de 1 ciclo (incluindo instruções SIMD de 128 bits).
* Até oito operações de ponto flutuante por ciclo.
* Muitas operações de computação de latência longa são pipelined em hardware para aumentar o rendimento geral.
* Redução da exposição a atrasos de acesso a dados usando o Intel Smart Memory Access.

**2.2.4 Microarquitetura Intel Atom®**

A microarquitetura Intel Atom maximiza o desempenho eficiente em termos de energia para cargas de trabalho de thread único e multithread, fornecendo:

• Execução Avançada de Micro-Op

— Execução de instrução de micro-op única, desde a decodificação até a aposentadoria, incluindo instruções apenas com semântica de registro, carga e armazenamento.

— Pipeline de dezesseis estágios em ordem, otimizado para throughput e redução do consumo de energia.

— Duas pipelines para permitir a decodificação, emissão, execução e aposentadoria de duas instruções por ciclo.

— Ponteiro de pilha avançado para melhorar a eficiência da entrada e saída de funções.

• Intel® Smart Cache

— O cache de segundo nível possui 512 KB e associatividade de 8 vias.

— Otimizado para ambientes de execução com várias threads e thread único.

— Caminho de dados interno de 256 bits entre o cache de dados L2 e L1 melhora o alto desempenho.

• Acesso à Memória Eficiente

— Pré-buscas de hardware eficientes para L1 e L2, carregando especulativamente dados que provavelmente serão solicitados pelo processador para reduzir o impacto das falhas de cache.

• Intel® Digital Media Boost

— Duas portas de emissão para instruções SIMD para unidades de execução.

— Throughput de um ciclo para a maioria das instruções SIMD de inteiros de 128 bits.

— Até seis operações de ponto flutuante por ciclo.

— Até duas operações SIMD de inteiros de 128 bits por ciclo.

— Reconhecimento de Instrução Segura (SIR) para permitir que operações de ponto flutuante de latência longa se aposentem fora de ordem em relação às instruções de inteiros.

**2.2.5 Microarquitetura Nehalem**

A microarquitetura Nehalem fornece a base para muitos recursos dos processadores Intel Core i7. Ela se baseia no sucesso da microarquitetura Intel Core de 45 nm e oferece as seguintes melhorias:

• Núcleo do processador aprimorado

— Melhor previsão de ramificação e recuperação de erros de previsão incorreta.

— Aprimoramento do loop streaming para melhorar o desempenho da frente de execução e reduzir o consumo de energia.

— Buffers mais profundos no mecanismo fora de ordem para extrair paralelismo.

— Unidades de execução aprimoradas para fornecer aceleração em CRC, processamento de strings/texto e embaralhamento de dados.

• Acesso à Memória Inteligente

— O controlador de memória integrado fornece acesso de baixa latência à memória do sistema e largura de banda de memória escalonável.

— Nova organização hierárquica de cache com cache L3 compartilhado e inclusivo para reduzir o tráfego de varredura.

— Dois TLBs de nível e tamanho de TLB aumentado.

— Acesso rápido à memória desalinhada.

• Tecnologia HyperThreading

— Fornece dois threads de hardware (processadores lógicos) por núcleo.

— Aproveita o mecanismo de execução de 4 vias, o cache L3 grande e a largura de banda de memória massiva.

• Inovações de Gerenciamento de Energia Dedicadas

— Microcontrolador integrado com firmware incorporado otimizado para gerenciar o consumo de energia.

— Sensores embutidos em tempo real para temperatura, corrente e energia.

— Portão de energia integrado para ligar/desligar o consumo de energia por núcleo.

— Versatilidade para reduzir o consumo de energia da memória, subsistemas de link.

**2.2.6 Microarquitetura Sandy Bridge**

A microarquitetura Sandy Bridge baseia-se nos sucessos da microarquitetura Intel® Core™ e Nehalem. Ela oferece os seguintes recursos:

• Extensões Avançadas de Vetor Intel (Intel AVX).

— Extensões de conjunto de instruções de ponto flutuante de 256 bits para as Extensões de Conjunto de Instruções Intel de 128 bits (SSE), fornecendo benefícios de desempenho de até 2X em relação ao código de 128 bits.

— Codificação de destino não destrutiva oferece técnicas de codificação mais flexíveis.

— Suporta migração e coexistência flexíveis entre código AVX de 256 bits, código AVX de 128 bits e código SSE de 128 bits legado.

• Front-end e mecanismo de execução aprimorados.

— Componente de cache de instruções decodificadas que melhora a largura de banda da frente de execução e reduz a penalidade de previsão incorreta de ramificação.

— Previsão de ramificação avançada.

— Suporte adicional à macro-fusão.

— Janela de execução dinâmica maior.

— Aprimoramentos na aritmética de inteiros de precisão múltipla (ADC/SBB, MUL/IMUL).

— Melhoria na largura de banda do LEA.

— Redução das paradas gerais de execução (portas de leitura, conflitos de gravação, latência de desvio).

— Manipulação rápida de exceções de ponto flutuante.

— Melhorias de desempenho XSAVE/XRSTORE e nova instrução XSAVEOPT.

• Melhorias na hierarquia de cache para maior largura de banda de dados.

— Duplicação da largura de banda habilitada por duas portas simétricas para operações de memória.

— Manuseio simultâneo de mais cargas e armazenamentos em voo, habilitado pelo aumento de buffers.

— Largura de banda interna de duas cargas e uma gravação a cada ciclo.

— Melhoria na pré-busca.

— Arquitetura de LLC de baixa latência e alta largura de banda.

— Arquitetura de anel de alta largura de banda para interconexão em die.

Para informações adicionais sobre as Extensões Avançadas de Vetor Intel (AVX), consulte a Seção 5.13, "Extensões Avançadas de Vetor Intel (Intel AVX)" e o Capítulo 14, "Programação com Intel AVX, FMA e Intel AVX2" no Manual de Desenvolvimento de Software das Arquiteturas Intel ® 64 e IA-32, Volume 1.

**2.2.7 Instruções SIMD**

A partir das famílias de processadores Pentium II e Pentium com tecnologia Intel MMX, foram introduzidas seis extensões nas arquiteturas Intel 64 e IA-32 para realizar operações de única instrução em dados múltiplos (SIMD). Essas extensões incluem a tecnologia MMX, extensões SSE, extensões SSE2, extensões SSE3, Extensões Suplementares de Streaming SIMD 3 e SSE4. Cada uma dessas extensões fornece um grupo de instruções que realizam operações SIMD em elementos de dados inteiros compactados e/ou de ponto flutuante compactados.

As operações SIMD de inteiros podem usar os registradores MMX de 64 bits ou os registradores XMM de 128 bits. As operações de ponto flutuante SIMD usam registradores XMM de 128 bits. A Figura 2-4 mostra um resumo das várias extensões SIMD (tecnologia MMX, Intel SSE, Intel SSE2, Intel SSE3, SSSE3 e Intel SSE4), os tipos de dados em que operam e como os tipos de dados são compactados nos registradores MMX e XMM.

A tecnologia Intel MMX foi introduzida nas famílias de processadores Pentium II e Pentium com tecnologia MMX. As instruções MMX realizam operações SIMD em bytes compactados, palavras ou inteiros de dupla palavra localizados em registradores MMX. Essas instruções são úteis em aplicativos que operam em matrizes de inteiros e fluxos de dados inteiros que se prestam ao processamento SIMD.

A Intel SSE foi introduzida na família de processadores Pentium III. As instruções Intel SSE operam em valores de ponto flutuante de precisão simples compactados em registradores XMM e em inteiros compactados em registradores MMX. Várias instruções Intel SSE fornecem gerenciamento de estado, controle de cache e operações de ordenação de memória. Outras instruções Intel SSE são direcionadas a aplicativos que operam em matrizes de elementos de dados de ponto flutuante de precisão simples (geometria 3D, renderização 3D e aplicativos de codificação e decodificação de vídeo).

A Intel SSE2 foi introduzida nos processadores Pentium 4 e Intel Xeon. As instruções Intel SSE2 operam em valores de ponto flutuante de dupla precisão compactados em registradores XMM e em inteiros compactados em registradores MMX e XMM. As instruções de inteiros Intel SSE2 estendem as operações SIMD IA-32 adicionando novas operações de inteiros SIMD de 128 bits e expandindo as operações de inteiros SIMD de 64 bits existentes para a capacidade de 128 bits XMM. As instruções Intel SSE2 também fornecem novas operações de controle de cache e ordenação de memória.

A Intel SSE3 foi introduzida com o processador Pentium 4 que suporta a Tecnologia Hyper-Threading (construída com tecnologia de processo de 90 nm). A Intel SSE3 oferece 13 instruções que aceleram o desempenho da tecnologia de Extensões de Conjunto de Instruções de Streaming SIMD, tecnologia de Extensões de Conjunto de Instruções de Streaming SIMD 2 e capacidades de matemática x87-FP.

A SSSE3 foi introduzida com o processador Intel Xeon série 5100 e a família de processadores Intel Core 2. A SSSE3 oferece 32 instruções para acelerar o processamento de dados inteiros SIMD.

A Intel SSE4 oferece 54 instruções. 47 delas são chamadas de instruções Intel SSE4.1. A Intel SSE4.1 foi introduzida com o processador Intel Xeon série 5400 e o processador Intel Core 2 Extreme QX9650. As outras sete instruções Intel SSE4 são chamadas de instruções Intel SSE4.2.

O Intel AES-NI e o PCLMULQDQ introduziram sete novas instruções. Seis delas são primitivas para acelerar algoritmos com base no padrão de criptografia/descriptografia AES e são chamadas de Intel AES-NI.

A instrução PCLMULQDQ acelera a criptografia de blocos de propósito geral, que pode realizar multiplicação sem transporte para dois números binários de até 64 bits de largura. A arquitetura Intel 64 permite que quatro gerações de extensões SIMD de 128 bits acessem até 16 registradores XMM. A arquitetura IA-32 fornece oito registradores XMM.

As Extensões de Vetor Avançadas da Intel oferecem aprimoramentos arquitetônicos abrangentes em relação às gerações anteriores de Extensões de Conjunto de Instruções de Streaming SIMD. A Intel AVX introduz os seguintes aprimoramentos arquitetônicos:

• Suporte para vetores de 256 bits de largura e conjunto de registradores SIMD.

• Aprimoramento do conjunto de instruções de ponto flutuante de 256 bits com ganho de desempenho de até 2X em relação às extensões de Conjunto de Instruções de Streaming SIMD de 128 bits.

• Suporte à sintaxe de instrução de três operandos generalizados para melhorar a flexibilidade de programação de instruções e codificação eficiente de novas extensões de instrução.

• Aprimoramento das extensões de instrução SIMD de 128 bits legadas para suportar sintaxe de três operandos e simplificar a vetorização do compilador de expressões de linguagem de alto nível.

• Suporte para implantação flexível de código AVX de 256 bits, código AVX de 128 bits, código AVX de 128 bits legado e código escalar.

Além das considerações de desempenho, os programadores também devem estar cientes das implicações das instruções AVX codificadas em VEX com as expectativas dos componentes de software do sistema que gerenciam os componentes de estado do processador habilitados por XCR0. Para obter informações adicionais, consulte a Seção 2.3.10.1, "Transição de Comprimento de Vetor e Considerações de Programação" no Manual de Desenvolvimento de Software das Arquiteturas Intel ® 64 e IA-32, Volume 2A.

Veja também:

• Seção 5.4, "Instruções MMX" e Capítulo 9, "Programação com a Tecnologia Intel MMX."

• Seção 5.5, "Instruções Intel SSE" e Capítulo 10, "Programação com as Extensões de Conjunto de Instruções de Streaming SIMD Intel (Intel SSE)."

• Seção 5.6, "Instruções Intel SSE2" e Capítulo 11, "Programação com as Extensões de Conjunto de Instruções de Streaming SIMD 2 Intel (Intel SSE2)."

• Seção 5.7, "Instruções Intel SSE3", Seção 5.8, "Extensões Suplementares de Streaming SIMD 3 (SSSE3) Instruções", Seção 5.9, "Instruções Intel SSE4" e Capítulo 12, "Programação com Intel SSE3, SSSE3, Intel SSE4 e Intel AES-NI."

Diagrama, Tabela

Descrição gerada automaticamente

**2.2.8 Tecnologia Intel® Hyper-Threading**

Intel Hyper-Threading Technology (Tecnologia Intel Hyper-Threading), desenvolvida para melhorar o desempenho dos processadores IA-32 ao executar código de sistema operacional e aplicativos multi-threaded ou aplicativos de thread única em ambientes multi-tarefa. A tecnologia permite que um único processador físico execute dois ou mais fluxos de código separados (threads) simultaneamente usando recursos de execução compartilhados.

A Tecnologia Intel HT é uma forma de capacidade de multi-threading de hardware nas famílias de processadores IA-32. Ela difere da capacidade de multiprocessamento que utiliza pacotes fisicamente distintos separados, com cada pacote de processador físico conectado a um soquete físico. A Tecnologia Intel HT fornece capacidade de multi-threading de hardware com um único pacote físico, usando recursos de execução compartilhados em um núcleo de processador.

Arquitetonicamente, um processador IA-32 que suporta a Tecnologia Intel HT é composto por dois ou mais processadores lógicos, cada um dos quais possui seu próprio estado arquitetural IA-32. Cada processador lógico consiste em um conjunto completo de registradores de dados IA-32, registradores de segmento, registradores de controle, registradores de depuração e a maioria dos MSR (registros de modelo específico). Cada um também possui seu próprio controlador de interrupção programável avançado (APIC).

A Figura 2-5 mostra uma comparação entre um processador que suporta a Tecnologia Intel HT (implementado com dois processadores lógicos) e um sistema de processador duplo tradicional.

Diferentemente de uma configuração tradicional de sistema com múltiplos processadores (MP) que utiliza dois ou mais processadores IA-32 físicos separados, os processadores lógicos em um processador IA-32 que suporta a Tecnologia Intel HT compartilham os recursos centrais do processador físico. Isso inclui a unidade de execução e a interface do barramento do sistema. Após a inicialização e a alimentação, cada processador lógico pode ser direcionado de forma independente para executar uma thread específica, ser interrompido ou ser interrompido.

A Tecnologia Intel HT aproveita o paralelismo de nível de processo e thread encontrado em sistemas operacionais contemporâneos e em aplicativos de alto desempenho, fornecendo dois ou mais processadores lógicos em um único chip. Essa configuração permite que duas ou mais threads sejam executadas simultaneamente em cada processador físico. Cada processador lógico executa instruções de uma thread de aplicativo usando os recursos no núcleo do processador. O núcleo executa essas threads de forma concorrente, utilizando um escalonamento de instruções fora de ordem para maximizar o uso das unidades de execução durante cada ciclo de clock.

**2.2.8.1 Algumas Notas de Implementação**

Todas as configurações de Tecnologia Intel HT exigem:

Um processador que suporte a Tecnologia Intel HT.

Um chipset e BIOS que utilizem a tecnologia.

Otimizações no sistema operacional.

Consulte http://www.intel.com/products/ht/hyperthreading\_more.htm para obter informações adicionais.

No nível do firmware (BIOS), os procedimentos básicos para inicializar os processadores lógicos em um processador que suporta a Tecnologia Intel HT são os mesmos que os de uma plataforma tradicional DP (Dual Processor) ou MP (Multiprocessor). Os mecanismos descritos na Especificação de Multiprocessador, Versão 1.4, para ligar e inicializar processadores físicos em um sistema MP também se aplicam aos processadores lógicos em um processador que suporta a Tecnologia Intel HT.

Um sistema operacional projetado para rodar em uma plataforma DP ou MP tradicional pode usar a instrução CPUID para determinar a presença do recurso de suporte a múltiplos threads de hardware e o número de processadores lógicos que eles fornecem.

Embora o código existente de sistema operacional e aplicativos deva funcionar corretamente em um processador que suporta a Tecnologia Intel HT, algumas modificações no código são recomendadas para obter o máximo benefício. Essas modificações são discutidas no Capítulo 7, "Gerenciamento de Múltiplos Processadores," no Manual do Desenvolvedor de Software das Arquiteturas Intel® 64 e IA-32, Volume 3A.

**2.2.9 Tecnologia Multi-Core**

A tecnologia multi-core é outra forma de capacidade de multi-threading de hardware nas famílias de processadores IA-32. A tecnologia multi-core aprimora a capacidade de multi-threading de hardware ao fornecer dois ou mais núcleos de execução em um pacote físico.

O processador Intel Pentium Extreme Edition é o primeiro membro da família de processadores IA-32 a introduzir a tecnologia multi-core. O processador oferece suporte de multi-threading de hardware com dois núcleos de processador e a Tecnologia Intel Hyper-Threading. Isso significa que o processador Intel Pentium Extreme Edition fornece quatro processadores lógicos em um pacote físico (dois processadores lógicos para cada núcleo de processador). O processador Intel Xeon Dual-Core apresenta a tecnologia multi-core, a Tecnologia Intel Hyper-Threading e oferece suporte a plataformas de multiprocessador.

O processador Intel Pentium D também apresenta a tecnologia multi-core. Este processador oferece suporte de multi-threading de hardware com dois núcleos de processador, mas não oferece a Tecnologia Intel Hyper-Threading. Isso significa que o processador Intel Pentium D fornece dois processadores lógicos em um pacote físico, sendo que cada processador lógico possui todos os recursos de execução de um núcleo de processador completo.

A família de processadores Intel Core 2, a série de processadores Intel Xeon 3000, a série de processadores Intel Xeon 5100 e o processador Intel Core Duo oferecem tecnologia multi-core eficiente em termos de energia. O processador contém dois núcleos que compartilham um cache inteligente de segundo nível. O cache de nível 2 permite o compartilhamento eficiente de dados entre dois núcleos para reduzir o tráfego de memória no barramento do sistema.

Diagrama

Descrição gerada automaticamente

O processador Pentium® dual-core é baseado na mesma tecnologia da família de processadores Intel Core 2 Duo. Os processadores Intel Xeon das séries 7300, 5300 e 3200, o processador Intel Core 2 Extreme Quad-Core e os processadores Intel Core 2 Quad suportam a tecnologia quad-core da Intel. Os processadores Intel Xeon quad-core e a família de processadores Intel Core 2 Quad também estão representados na Figura 2-7.

Diagrama

Descrição gerada automaticamente