EXPLICADORES.NET
08/08/2022
FLÁVIO BRAGANÇA
HARDWARE

Capítulo 5 – Modos de operação

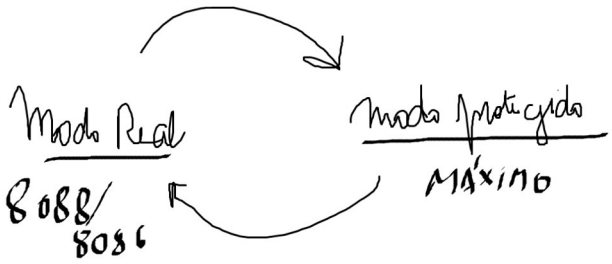
- O PROCESSADOR PODE TRABALHAR EM VÁRIOS MODOS DE OPERAÇÃO;
- OS PROCESSADORES EM ALGUNS DOS MODOS CITADOS ABAIXO;

Processadores podem trabalhar em diversos modos de operação. A seguir estaremos estudando alguns deles.

Modo REAL

No modo real o processador opera como se fosse um processador 8086, possuindo exatamente as mesmas características, com a finalidade de compatibilizar hardware e software que sejam mais antigos.

- O PROCESSADOR SE COMPORTAVA COMO UM 8088/8086;
- PERDIA PERFORMANCE;
- CONSEGUIA A COMPATIBILIDADE;



OBJETIVO:

- COMPATIBILIDADE

UM DOS PROCESSADORES LANÇADOS: 8086 /8088 (PRIMEIRA GERAÇÃO);

8086/8088 – PRIMEIRA GERAÇÃO
80286 – SEGUNDA GERAÇÃO
80386 – TERCEIRA GERAÇÃO
80486 – QUARTA GERAÇÃO

Modo PROTEGIDO de 16 bits

- MODO ONDE O PROCESSADOR FICA NA PERFORMANCE MÁXIMA;
- INSTRUÇÕES TEM NO MÁXIMO 16 BITS;
- TODA INSTRUÇÃO FICA LIMITADA A 16BITS;
- QUANTIDADE DE MEMÓRIA MÁXIMA ACESSADA 2^{16} = 1MB NO MÁXIMO;

Foi criado no processador 286. Neste, o processador trabalhava com os seguintes recursos:

Instruções: Possibilidade de rodar instruções dos processadores 8086 e 286 sem a necessidade de sair do modo protegido, DO TAMANHO DE 16B;

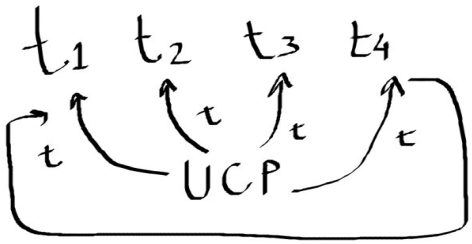
Proteção de memória: Possibilidade de proteger cada programa na sua área em uma porção separada, impedindo que um programa invada a área do outro.

- RECURSO QUE NÃO PERMITE QUE UM PROGRAMA INVADA A ÁREA DO OUTRO NA MEMÓRIA;

- GPF = GENERAL PROTECTION FAILURE (FALHA GERAL NA PROTEÇÃO DE MEMÓRIA), MESMO QUE O HARDWARE ATIVE A PROTEÇÃO DE MEMÓRIA O SISTEMA OPERACIONAL PODE DEIXAR UM INVADIR A ÁREA DO OUTRO);

Multitarefa: Capacidade de executar um pouco da cada programa por vez, alternando o processamento entre os programas existentes.

- EXECUÇÃO DE PROGRAMAS “SIMULTANEAMENTE”;
- O PROCESSADOR SÓ É CAPAZ DE EXECUTAR UMA TAREFA POR VEZ (PROCESSADOR DE SOMENTE UM NÚCLEO);
- O FUNCIONAMENTO DA MULTITAREFA FUNCIONA COM UM REVEZAMENTO ENTRE AS TAREFAS;
- TIME SLICE = FATIA DE TEMPO QUE O PROCESSADOR RESERVA PARA CADA TAREFA;



Memória: Acesso até 1MiB de memória RAM

Memória Virtual: Possibilidade de simular mais memória RAM do que realmente possui, criando um arquivo no disco rígido e trocando porções de memória com o conteúdo deste arquivo (swap file). Neste sistema de 16 bits é possível acessar até 1 GiB de memória total (RAM+Virtual).

- QUANDO O PROCESSADOR UTILIZA O DISCO COMO EXTENSÃO DA RAM;
- PARTES DOS PROGRAMAS QUE ESTÃO NA RAM MAS NÃO ESTÃO EM USO SÃO ENVIADOS PARA A ÁREA DE SWAP;
- GERANDO O SWAP FILE = ARQUIVO DE TROCA, ARQUIVO QUE CONTÉM PARTE DOS PROGRAMAS QUE ESTAVAM NA RAM EM EXECUÇÃO;
- ASSIM O ESPAÇO DE RAM É LIBERADO PARA OUTRO PROGRAMA SER EXECUTADO;

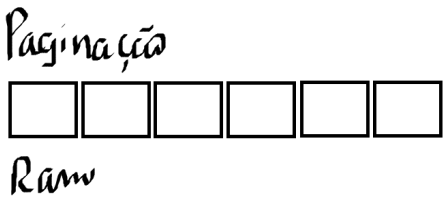
VANTAGENS:
- LIBERAR MAIS MEMÓRIA RAM;

DESVANTAGENS:
- MAIS LENTO QUE SE O USUÁRIO TIVESSE A MEMÓRIA RAM SUFICIENTE;

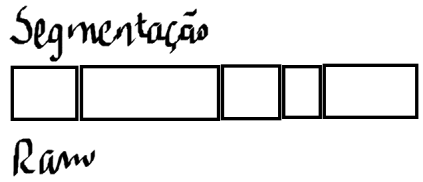
MEMÓRIA TOTAL = MEMÓRIA PRINCIPAL + SWAP

TIPOS :
- **POR PAGINAÇÃO;**
- **POR SEGMENTAÇÃO;**

POR PAGINAÇÃO
A MEMÓRIA RAM É DIVIDIDA EM BLOCOS DE TAMANHO FIXO CHAMADOS DE PÁGINAS;



POR SEGMENTAÇÃO
A MEMÓRIA RAM É DIVIDIDA EM BLOCOS DE TAMANHO VARIADO;



Modo PROTEGIDO de 32 bits
- MODO ONDE O PROCESSADOR FICA NA PERFORMANCE MÁXIMA;
- INSTRUÇÕES DE 32B = 2^{32} = 4GB TOTAL DE MEMÓRIA;

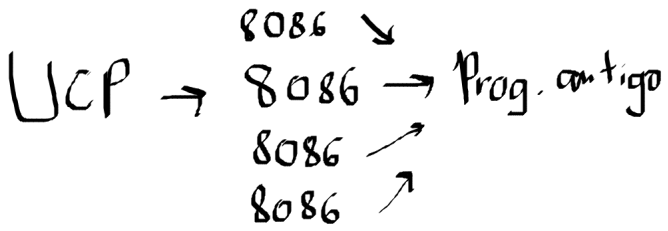
Esse é o modo de operação em que todos os sistemas operacionais de 32 bits trabalham, . sendo introduzido pelo 386. Possui as seguintes características:

- **Proteção de memória;**
- **Multitarefa;**
- **Memória:** Acesso até 4GiB de memória total (RAM + Virtual);
- **Paginação:** Mecanismo utilizado pela memória virtual;
- **Registradores:** Expansão de todos os registradores para 32 bits.
- **Modo virtual-8086:** Também chamado de V86 ou VM86.

Modo Virtual-8086

Permite que uma sessão simulando um processador 8086 seja aberta dentro do modo protegido. Modo utilizado para abrir uma janela DOS ou rodar um programa DOS a partir do sistema operacional.

- CONSEGUE COMPATIBILIZAR PROCESSADORES ANTIGOS E MANTER A PERFORMANCE;
- MISTURA DE MODO PROTEGIDO (MODO DE MELHOR PERFORMANCE) COM MODO REAL (MODO ONDE O PROCESSADOR REDUZIA SUAS CAPACIDADES PARA COMPATIBILIZAR COM PROGRAMAS VELHOS);



Modo de compatibilidade

Processadores que suportam as extensões de 64 bits (Chamadas de EM64T ou IA32 e pela Intel X86-64 pela AMD) podem funcionar em dois modos quando rodam um sistema operacional de 64 bits.

No modo de compatibilidade o processador pode operar nos modos protegidos de 16 bits ou 32 bits quando estão rodando sistemas operacionais de 64 bits. Para compatibilizar com programas antigos.

- OS PROCESSADORES AMD TEM ALGUMAS INSTRUÇÕES PRÓPRIAS;
- ATUALMENTE OS PROCESSADORES NÃO TRABALHAM COM MODO REAL;
- COMPATIBILIZAR PROGRAMAS 32BITS RODANDO EM SISTEMAS OPERACIONAIS/PROCESSADORES 64BITS;

Modo de 64 bits
Também chamado de modo longo pela AMD, o processador passa a ter as seguintes características adicionais além de apresentadas pelo modo protegido de 32 bits:

- Os registradores de 32 bits são expandidos para 64 bits.
- Oito novos registradores de uso geral de 64 bits, chamados de R8 a R15, são adicionados;
- POSSUI MAIS REGISTRADORES DO QUE O MODO 32BITS;
- Oito novos registradores de controle de 64 bits, chamados de CR8 a CR15, são adicionados;
- Oito novos registradores SIMD de 128 bits, chamados XMM8 a XMM15, são adicionados.
- Acesso a 256 TiB de memória por programa e até 4 PiB de memória total;
- MODO ATUAL;

Modo gerenciamento do sistema
Mais conhecido como SMM (System Managment Mode), é usado para o processador lidar com uma interrupção de hardware chamada de interrupção de gerenciamento do sistema (SMI) que é geralmente gerada pela placa mãe (chipset).

- MODO ONDE O PROCESSADOR TRABALHA ESPECIFICAMENTE PARA ATENDER A UMA SOLICITAÇÃO DA PLACA MÃE;

Capítulo 6 – Organização da memória

Introdução
Na arquitetura X86, por motivos históricos, considera-se que cada endereço de memória armazena dados de oito bits, e é por isso que continuamos nos referindo á capacidade de memória em bytes.

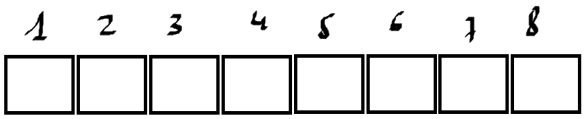
- ARQUITETURA X86 = ARQUITETURA QUE OS NOSSO PROCESSADORES SÃO BASEADOS;

Representação de endereços

Há duas formas de se representar endereços.

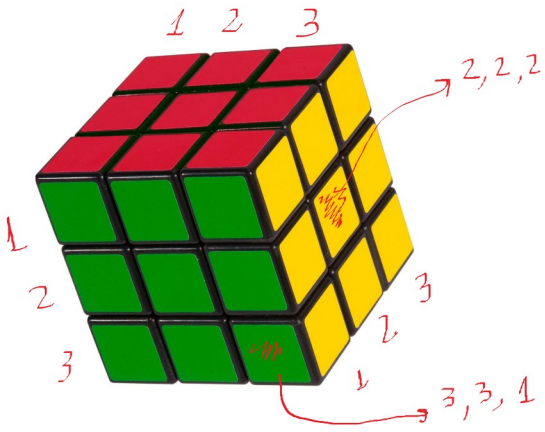
Endereçamento linear – Endereços numerados sequencialmente, funcionando no modo protegido e no modo de 64 bits.

- ENDEREÇOS NUMERADOS SEQUENCIALMENTE;
- FUNCIONA NO MODO PROTEGIDO E MODO 64BITS;
- A MEMÓRIA SE COMPORTA COMO UMA FITA;



Endereçamento segmentado – Neste sistema, os endereços são representados no formato segmento:offset. Um seguimento é um pedaço da memória do computador, enquanto que o offset (deslocamento) é a posição do dado a ser lido ou armazenado dentro desse bloco de memória.

- TEMOS ENDEREÇOS FORMADOS POR TRÊS PARTES : COLUNA, LINHA E OFFSET (PROFUNDIDADE);
- SE COMPORTA COMO UM CUBO;



Organização da memória no modo real

No modo real a memória é dividida em segmentos de 64KiB. No modo de endereçamento segmentado.

- SEGMENTOS DE 64BITS;
- SEGMENTADO;

Organização da memória no modo protegido

No modo protegido a memória pode ser acessada de uma das seguintes maneiras por programas:

Modo Plano básico: Neste modo, a memória é acessada como uma entidade única, sem qualquer tipo de segmentação.

- A MEMÓRIA É UM BLOCO ÚNICO;
- OBSOLETO;

Modo plano protegido: Igual ao anterior, porém o processador é configurado para que uma exceção (mensagem de erro) seja dada caso o processador tente acessar uma área de memória acima da que está fisicamente instalada no computador.

- A MEMÓRIA É UM BLOCO ÚNICO;
- POSSUI O RECURSO QUE DEIXA O PROCESSADOR ACESSAR MAIS MEMÓRIA DO QUE DEVERIA;
- OBSOLETO;

Modo multissegmentado: É o modelo normalmente usado quando estamos trabalhando no modo protegido. Neste modo a memória é dividida em segmentos de tamanho variado, e estes segmentos podem ser protegidos, ou amarrados a um programa específico. Fazendo que um programa não invada a área de memória que está sendo utilizada por outro.

- SEGMENTADO;
- COM PROTEÇÃO DE MEMÓRIA;
- MODO DE OPERAÇÃO ATUAL;

Capítulo 7 – Proteção de memória

Introdução

- QUANDO UM PROGRAMA NÃO PODE INVADIR A ÁREA DO OUTRO;

No modo protegido cada segmento é uma área protegida de memória, que só pode ser acessada por um programa específico. Com isso, para cada segmento de memória, o sistema operacional precisa saber:
A tarefa a qual ele pertence;

- O seu endereço inicial;
- O seu tamanho;
- Como ele pode ser acessado;
- O nível de privilégio mínimo que o programa precisa ter para acessá-lo;
- Se o seu conteúdo é código, dados ou um tipo especial que só pode ser usado pelo sistema operacional;
- Se ele está no momento armazenado na memória RAM ou em dispositivo de memória de massa;

Capítulo 8 – Paginação

- QUANDO A MEMÓRIA É DIVIDADE EM PEDAÇOS DE TAMANHO FIXO;
- UTILIZADA NA MEMÓRIA VIRTUAL;

O sistema de paginação permite o uso de memória virtual, permitindo que o processador acesse mais memória ram do que existe no computador quando ele está no modo protegido ou quando ele está no modo de 64 bits, simulando a memória faltosa em um disco de armazenamento em massa, como por exemplo o HD.
Quando o sistema de memória virtual está desabilitado, cada endereço linear interno do processador corresponderá a um endereço físico externo da memória ram.
Porém quando o sistema está habilitado, a memória ram é dividida em blocos chamados páginas. No disco um arquivo chamado arquivo de troca ou swap file é criado e dividido em blocos de igual tamanho.

Modos de paginação:

Paginação de 32 bits: Pode usar páginas e 4KiB ou de 4 MiB (se o processador tiver a extensão PSE. Page Size Extensions.

- PÁGINAS DE 4KB OU 4MB;

Paginação PAE (Physical Address Extensions): Pode usar páginas de 4 KiB ou 2 MiB;

- PÁGINAS DE 4KB OU 2MB;

Paginação IA-32e (modo 64 bits): Pode usar páginas de 4 KiB, 2MiB ou 1GiB (nem todos os processadores suportam páginas de 1GiB);

- PÁGINAS DE 4KB, 2MB OU 1GB;

O modo de paginação utilizado dependerá do sistema operacional.

Capítulo 9 – Multitarefa

- QUANDO O PROCESSADOR FICA UM TEMPO EM CADA TAREFA;
- TIME SLICE = FATIA DE TEMPO QUE O PROCESSADOR FICA EM CADA TAREFA;
- SÓ TEMOS MULTITAREFA NO MODO PROTEGIDO;
- NO MODO 64BITS O CONTROLE DE MULTITAREFA É FEITO PELO SOFTWARE;

A multitarefa é um recurso que permite que o processador execute um pouco de cada programa que está carregando por vez, importante lembrar que neste tipo de contexto o sistema operacional também é um programa.

A técnica empregada é a técnica de time slicing (fatiando o tempo) onde cada programa será executado em uma fatia de tempo.

O controle da multitarefa pode ser feito por hardware ou por software.

- O SISTEMA OPERACIONAL CONTROLANDO A MULTITAREFA (POR SOFTWARE);
- O PROCESSADOR CONTROLANDO A MULTITAREFA (POR HARDWARE);

O controle de multitarefa por hardware só existe no modo protegido.

O modo 64 bits faz o controle de multitarefa por software.

Capítulo 10 – Registradores

- SÃO AS MENORES MEMÓRIAS DO COMPUTADOR;
- MEMÓRIAS MAIS RÁPIDAS DO COMPUTADOR;
- MEMÓRIAS INTERNAS DO PROCESSADOR;

Registradores de uso geral

Registradores que podem ser usados livremente pelo programador. Também chamados de **GPR** (General Purpose Registrer).

- REGISTRADORES QUE PODEM SER UTILIZADOS PELOS PROGRAMADORES;

A arquitetura x86 possui 4 registradores e uso geral, são eles:

- **A** (Acumulador): Normalmente usado para armazenar dados a serem manipulados e resultados de operações.
- **B** (Base) : Normalmente usado para armazenar informações de endereçamento.
- **C** (Contador) : Normalmente usado como contador de lações (loops).
- **D** (Dados) : Normalmente usado para armazenar informações de entrada e saída.

Flags

- REGISTRADORES QUE INDICAM SITUAÇÕES QUE OCORRERAM NO PROCESSADOR;

A arquitetura X86 possui um registrador de 32bits chamado de EFLAGS que armazena diversos FLAGS.

Registradores de controle

- ARMAZENAM O MODO DE OPERAÇÃO DO PROCESSADOR;

São utilizados para armazenar o modo de operação do processador e a caracteística da tarefa a sendo executada no momento.
Os principais tipos são :

(CR1, CR2, CR3, CR4, CR5, CR6, CR7, CR8 e EFER)

Registradores de Debug

- UTILIZADOS NO DEBUG DOS CÓDIGOS;
- DEBUG = EXECUTAR O CÓDIGO LINHA A LINHA A PROCURA DE ERROS;

Os processadores X86 tem suporte a Debugs (encontrar falhas e problemas em programas), estas informações ficam armazenadas em registradores de debug chamados de DR0 a DR7.

(DR0 DR1 DR2 DR3 DR4 DR5 DR6 DR7)

Registradores de gerenciamento do memória

Responsáveis pelo controle de operações na memória, são eles:

(GDTR, LDTR, IDTR, TR)

Outros registradores

Cada processador poderá ter outros registradores específicos.

Capítulo 11 – Interrupções e exceções

Interrupções

- QUANDO UM DISPOSITIVO NECESSITA DO AUXILIO DO PROCESSADOR O MESMO GERA UMA INTERRUPÇÃO;

São procedimentos executados pelos dispositivos que pedem a atenção do processador.
Existem três tipos de Interrupções:

Interrupção de hardware mascarável

- INTERRUPÇÕES GERADAS POR DISPOSITIVOS QUE PODEM SER IGNORADAS;
- GERADAS PELO PINO INTR;

Interrupções de dispositivos. O fato do processador possuir apenas uma linha para requisições de interrupções exige que exista um controlador de interrupções externo, que faz o papel de árbitro das isntruções que por ventura utilizarão este referido pino do processador. Utilizam o pino INTR.

Interrupções de hardware não mascarável

- INTERRUPÇÕES GERADAS PELO HARDWARE QUE NÃO PODEM SER IGNORADAS;
- GERADAS EM UM PINO NMI;

Utilizam o pino NMI para pedidos de interrupções

Interrupções de software

- GERADA PELOS PROGRAMAS;
- GERADAS POR UM PINO INT;

Utilizam o pino INT para pedidos de interrupções.

APIC (Advanced Programmable Interrupt Controller)

- PARTE DO PROCESSADOR RESPONSÁVEL POR CONTROLAR AS INTERRUPÇÕES;

Controlador interno do processador responsável por lidar com estas interrupções.

OBS.: Ainda existe um quarto tipo de interrupção chamada de IPI (Interprocessor Interruption) , que é utilizada em sistemas multiprocessados.

Exceções

- SITUAÇÕES QUE NECESSITAM DA ATENÇÃO DO PROCESSADOR (ANOMALIAS);
- QUANDO UMA EXCEÇÃO É ATIVADA É ACIONADO UM REGISTRADOR DE FLAG INDICANDO QUE A MESMA ACONTECEU...

Outra maneira de fazer o processador parar a execução do programa atual é através da exceção de software. Funciona como uma mensagem de erro interna do processador.
Exceções possíveis dos processadores X86:

Divisão por zero: Uma instrução tentou executar uma divisão por zero;

- QUANDO UM NÚMERO QUALQUER É DIVIDIDO POR ZERO;

Debug: O contador de programa atingiu um dos endereços de parada.

- QUANDO UM PROGRAMA COMEÇA A EXECUTAR DEBUG;

Parada: O programa atingiu uma instrução de parada;

- INSTRUÇÃO QUE PARALISA O PROCESSAMENTO;

Overflow: Ocorre quando o resultado de uma expressão não cabe no registrador destino;

- QUANDO HÁ UM EXCESSO NO TAMANHO DA INFORMAÇÃO;

```
    1   1
    1   1   1   (3 BITS)
+   1   1   1   (3 BITS)
1   1   1   0
```

Valor fora dos limites: Quando o valor está fora dos limites permitidos;

- O VALOR É MAIOR QUE OS LIMITES DO COMPUTADOR;

Opcode inválido: Gerada quando o processador encontra um valor que foi dado a ele como se fosse uma instrução, mas não corresponde a nenhuma instrução no conjunto de instruções;

- INSTRUÇÃO INVÁLIDA, QUANDO O PROCESSADOR NÃO CONSEGUE COMPREENDER A INSTRUÇÃO;

Dispositivo não disponível: Quando o processador recebe uma instrução multimedia e o mesmo não possui co-processador matemático;

Falha dupla encontrada: Quando o processador encontra uma falha ao tentar executar o código responsável por lidar com a exceção encontrada;

TSS inválido: A tabela TSS de uma tarefa é inválida;
Segmento não presente : Quando o segmento de um registrador é inválidoo;

Exceção de pilha: Ocorre quando a pilha estoura ou está vazia;

Falha geral de proteção: Quando um programa invade a área de outro programa;

Falha de página: Quando uma tabela ou página não está presente;

Exceção da unidade de ponto flutuante: Quando a unidade de ponto flutuante do computador encontra um erro;

Verificação de alinhamento : Gerada quando o endereço de memória não está alinhado;

Exceção SIMD: Gerada quando uma instrução SIMD gerou um erro.

Capítulo 12 – Unidade de ponto flutuante

- FPU – FLOAT POINT UNIT
- PARTE DO PROCESSADOR QUE EXECUTA CÁLCULOS MATEMÁTICOS
- ERA CHAMADA DE UNIDADE DE INTEIROS QUANDO EXECUTAVA SOMENTE CÁLCULOS COM NÚMEROS INTEIROS;
- ATUALMENTE CHAMADA DE CO-PROCESSADOR MATEMÁTICO;
- POSSIBILITAM OS JOGOS 3D;

GERAÇÃO DE PROCESSADORES DE 1 A 3

- CO-PROCESSADOR / FPU FICAVA NA PLACA MÃE;
- NÃO POSSIBILITAVAM A CRIAÇÃO DE 3D;

GERAÇÃO DE PROCESSADORES A PARTIR DA 4

- CO-PROCESSADOR / FPU PASSOU A SER PARTE INTEGRANTE DO PROCESSADOR;
- POSSIBILITA A CRIAÇÃO DE 3D;

Os processadores 8086, 8088, 286, 386 e 486SX, não eram capazes de executar instruções matemáticas complexas. Com isso foi inserido no sistema ou processador auxiliar, que receberia estes cálculos complexos direcionados pelos programadores, passando a se chamar co-processador matemático.

A partir do processador 486DX , processador e co-processador passaram a habitar no mesmo chip, onde o co-processador passou a ser chamado de unidade de ponto flutuante ou FPU (Float Point Unit), como os antigos co-processadores tinham nomenclaturas quer terminavam em 87, a expressão X87, também posse ser usada para designar esta unidade.