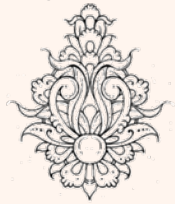
زبان ماشین و اسمبلی
(۰۰۵-۱۱-۱۳)
بخش چهارم

دانشگاه شهید بهشتی
دانشکده‌ی مهندسی برق و کامپیوتر
زمستان ۱۳۹۳
احمد محمودی ازناوه

http://faculties.sbu.ac.ir/~a_mahmoudi/

فهرست مطالب

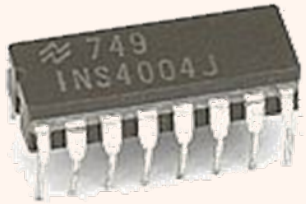
- تاریخچه
- انواع اسلوب‌های کاری
- آشنایی با ثبات‌های خانواده‌ی x86
  - ثبات‌های همه‌منظوره
  - ثبات‌های segment و شیوه‌ی دسترسی به حافظه



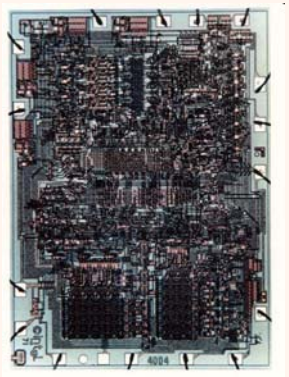
تاریخچه

- در سال ۱۹۴۵ ایده‌ی کامپیوتر با برنامه‌ی ذخیره شده (stored-program architecture) توسط Von Neumann مطرح شد.
- در سال ۱۹۴۸ ترانزیستور اختراع شد.
- در سال ۱۹۵۸ تراشه (IC) توسط Jack Kilby معرفی شد و در سال ۱۹۶۰ در کامپیوترها مورد استفاده قرار گرفت.
- در سال ۱۹۶۵، Moore پیش‌بینی کرد، در هر ۱۸ ماه تعداد ترانزیستورها بر روی تراشه دو برابر شود.

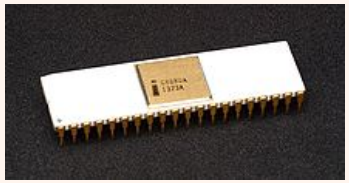
تاریخچه (ادامه...)



- در سال ۱۹۷۱ اینتل نخستین ریزپردازنده‌ی خود را معرفی کرد، 4004، پردازنده‌ای که دارای ۲۲۵۰ ترانزیستور بود.
- این ریزپردازنده‌ی چهاربیتی نخستین ریزپردازنده‌ی تجاری جهان می‌باشد.



- ماکزیمم فرکانس آن 740KHz بوده است.
- دارای دو حافظه‌ی جداگانه برای دستورها و داده‌ها
- دارای شانزده ثبات چهار بیتی
- دارای چهل‌ویک دستور هشت بیتی و پنج دستور شانزده‌بیتی بوده است،
- دارای دوازده خط آدرس

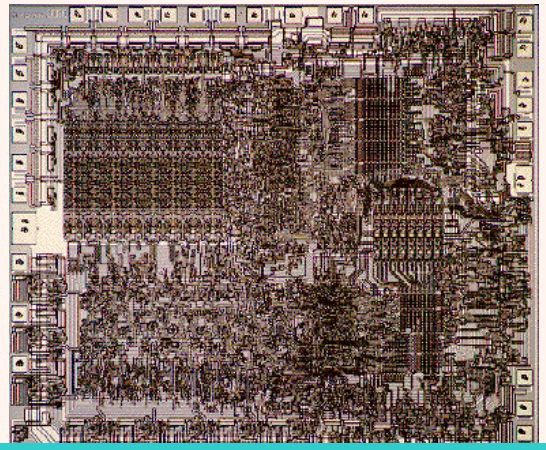


تاریخچه (ادامه...)

- در سال ۱۹۷۴ شرکت اینتل پردازنده‌ای هشت‌بیتی ۸۰۸۰ را ارائه کرد، این پردازنده که پایه‌ی کامپیوترهای شخصی اولیه شد، دومین پردازنده‌ی هشت‌بیتی اینتل بود که در عمل بهبود یافته‌ی ۸۰۰۸ بود، بدون این که با آن سازگاری کد دودویی داشته باشد.

Binary code compatibility

در صورتی که کد دودویی بر روی دو کامپیوتر قابل اجرا باشند می‌گوییم هماهنگی دودویی دارند. این مسأله زمانی دارای اهمیت است که بخواست یک برنامه بر روی کامپیوترهای مختلف اجرا شود



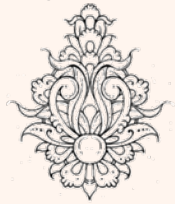
the first truly usable microprocessor

تاریخچه (ادامه..)

- در سال ۱۹۷۸، اینتل پردازنده‌ی **شانزده بیتی** با نام **۸۰۸۶** را روانه‌ی بازار کرد.
  - این پردازنده تنها **۲۰** خط آدرس دارد.
    - حداکثر حافظه 1MB
- سازگاری عقب‌رو (Downward camptibility): تمام پردازنده‌هایی که تولید می‌شوند باید با پردازنده‌های قدیمی سازگاری داشته باشند، برنامه‌های قدیمی را بتوان روی آن‌ها اجرا کرد.

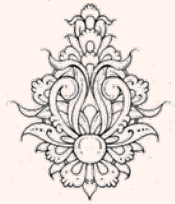
تاریخچه (ادامه..)

- ۸۰۲۸۶ با ۲۴ خط آدرس می‌توانست حداکثر حافظه‌ای 16MB را پشتیبانی کند، در این پردازنده ثبات‌ها شانزده‌بیتی بودند(هستند).
- در سال ۱۹۸۵، با عرضه‌ی ۸۰۳۸۶ پردازنده‌ی سی‌دو بیتی معرفی شدند. خطوط آدرس نیز به ۳۲ خط افزایش یافت و در نتیجه‌ی فضای آدرس‌دهی به 4GB رسید.



تاریخچه‌ی کامپیوتر (ادامه..)

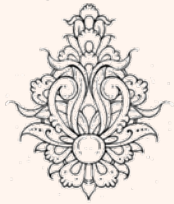
- ۸۰۴۸۶ نخستین پردازنده‌ی اینتل بود که به «خط لوله» مجهز شد.
- در Pentium از superscaler برای افزایش سرعت استفاده شد. در این پردازنده گذرگاه داده‌ی شصت و چهار بیتی مورد استفاده قرار گرفت و تکنولوژی MMX برای نخستین بار مطرح شد.
- در سال ۲۰۰۳، Opteron به عنوان نخستین پردازنده‌ی شصت و چهار بیتی مطرح شد.



x86

- اصطلاح x86 به خانواده ای از معماری مجموعه‌ی دستورالعمل‌ها که بر پایه پردازنده اینتل ۸۰۸۶ است، اشاره دارد.
- در طول سال‌ها موارد زیادی به این معماری با حفظ سازگاری عقب‌رو اضافه شده است. این معماری در پردازنده‌های Intel، Cyrix، AMD و VIA به کار گرفته شده است.




IA-32 و x86-64

- IA-32 توسعه‌یافته سی‌ودو بیتی x86 است.
- نخستین بار در ۸۰۳۸۶ به کار گرفته شد(۱۹۸۶).
- پس از Intel، AMD بزرگ‌ترین تولید کننده‌ی پردازنده با این معماری است.
- از سال ۲۰۱۱ این دو به سراغ معماری شصت‌وچهار بیتی رفته‌اند.
- این معماری مجموعه‌ی دستورالعمل گسترش یافته‌ی IA-32 می‌باشد.
- نخستین بار توسط AMD مطرح شد.

AMD64

IA-32e

Intel 64

سازگاری

- با توجه به نیاز به سازگاری مدل‌های مختلف پردازنده، اسلوب‌های کاری مختلف برای آن‌ها در نظر گرفته شده است.
- هرگاه معماری دچار تغییر شود، در عمل یک اسلوب جدید به پردازنده افزوده می‌شود.
- در صورتی که پردازنده با اسلوب قدیمی کار کند، همانند یک پردازنده‌ی قدیمی عمل خواهد کرد، در صورت نیاز به امکانات جدید باشد، باید به اسلوب جدید تغییر وضعیت دهد.

اسلوب‌های کاری پردازنده‌های خانواده‌ی X86

Mode	First supported
Real mode	Intel 8086
8080 emulation mode	NEC V20/V30 only
Protected mode	Intel 80286
Virtual 8086 mode	Intel 80386
Unreal mode	Intel 80386
System Management Mode	Intel 386SL
Long mode	AMD Opteron
Hardware virtualization	AMD Athlon 64, varie

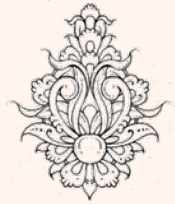
در ادامه در مورد برخی از اسلوب‌های کاری به صورت مختصر صحبت می‌شود.

Real mode

- در این اسلوب پردازنده همانند ۸۰۸۶ و ۸۰۸۸ عمل می‌کند.
- در واقع در زمان این پردازنده‌ها این تنها مود کاری پردازنده بود.
- در این حالت تنها 1MB حافظه در دسترس خواهد بود.
- استفاده از حافظه‌ی مجازی امکان‌پذیر نخواهد بود.
- نرم‌افزار به کل فضای آدرس دسترسی دارد؛ هیچ پشتبانی سخت‌افزاری برای حفاظت از حافظه و همچنین چندوظیفگی وجود ندارد.
- در ضمن برای اجرای برنامه‌ها هیچ اولویتی وجود ندارد.

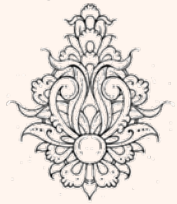
چندوظیفگی (چندکارگی)

- سیستم‌عامل می‌تواند چند فرآیند را همزمان اجرا کند.
- چند thread در یک برنامه همزمان اجرا شود.
- زمان‌بند (Scheduler) وظیفه‌ی تخصیص زمان را به عهده دارد.
- با توجه به سرعت بالای تغییر وظیفه (task switchingh)
  - در سیستم‌های تک‌پردازنده‌ای این پندار به وجود می‌آید که اجرای برنامه‌ها به صورت موازی انجام می‌شود.
- پردازنده می‌باید، چنین امکانی را پشتیبانی کند.



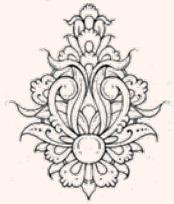
Protected mode

- این اسلوب در ۸۰۲۸۶ به بعد وجود دارد.
- در این اسلوب امکان استفاده از «حافظه‌ی مجازی» وجود دارد.
- همچنین امکان دستیابی یک فرآیند به فضای حافظه‌ی دیگر فرآیندها وجود ندارد.
- استفاده از پشتبانی سخت‌افزاری حفاظت از حافظه به سیستم‌عاملی نیاز است که برای این منظور طراحی شده باشد.



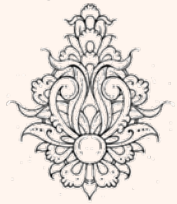
Protected mode (ادامه...)

- در ۸۰۲۸۶ برای تغییر از protected به real لازم بود سیستم reset شود.
- در ۸۰۳۸۶ بسیاری از نقیصه‌ها برطرف شد و گذرگاه آدرس به سی‌ودو بیت افزایش یافت.



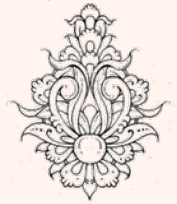
Long Mode

- اسلوبی که برنامه‌های شصت و چهار بیتی در آن کار می‌کنند.
- در این حالت برنامه‌ها به ثبات‌ها و دستوالعمل‌های سی‌ودو بیتی و نیز شانزده‌بیتی دسترسی خواهند داشت.



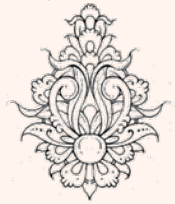
System Management Mode(SMM)

- در این اسلوب کاری، اجرای تمام فرآیندها عادی متوقف می‌شود (حتی سیستم‌عامل) و اجرای نرم‌افزارهای خاصی که توسط سازنده‌ی سخت‌افزار تعبیه شده است(firmware)، آغاز می‌شود.
- در مواردی مانند بروز خطا در حافظه، کنترل توان مصرفی، توابع امنیتی، خاموش کردن کامپیوتر در زمانی که حرارت پردازنده از حد مجاز فراتر رود و .. کاربرد دارد.



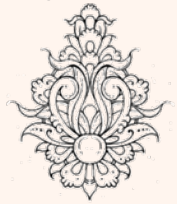
اسلوب‌های کاری پردازنده‌های خانواده‌ی X86

- تمامی پردازنده‌ها از ۸۰۲۸۶ به بعد، حتی پردازنده‌های شصت و چهار بیتی ابتدا در real mode آغاز به کار می‌کنند.
- windows 3.1 از real mode پشتیبانی نمی‌کرد و از این رو به پردازنده‌های ۸۰۲۸۶ به بعد احتیاج داشت.
- تقریبا تمام سیستم‌عامل‌های کنونی پس از start-up به protected mode سوییچ می‌کنند. سیستم‌عامل‌های شصت‌و چهاربیتی به long_mode تغییر وضعیت می‌دهند.

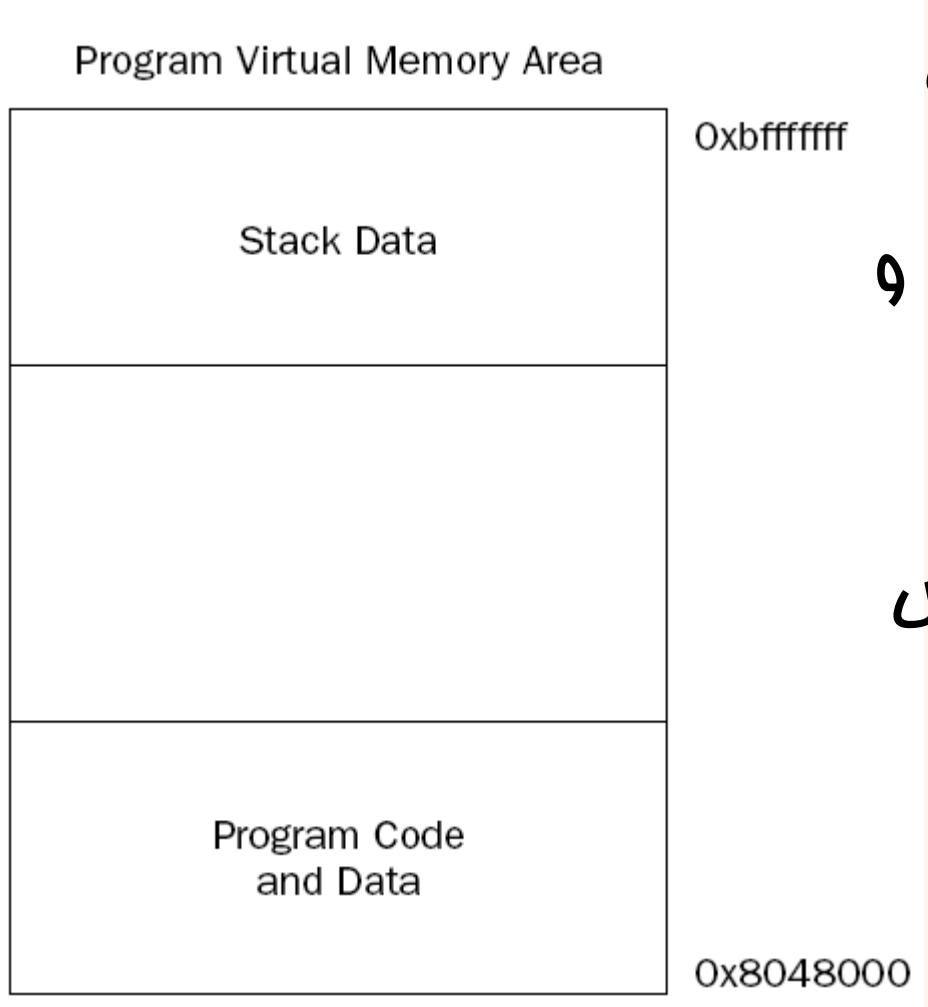


آدرس منطقی در برابر آدرس فیزیکی

- آدرس منطقی یا «logical address» آدرسی است که توسط برنامه‌نویس مشاهده می‌شود.
- در مقابل آن آدرس فیزیکی «physical address» وجود دارد که آدرس واقعی سلول‌های حافظه است.
- هنگامی که در سیستم‌عامل لینوکس یک برنامه فراخوانی شود، این برنامه در هر جایی از حافظه‌ی فیزیکی می‌تواند قرار گیرد.
- برای سادگی به هر برنامه یک حافظه‌ی مجازی اختصاص داده می‌شود.



آدرس منطقی دربرابر آدرس فیزیکی(ادامه...)

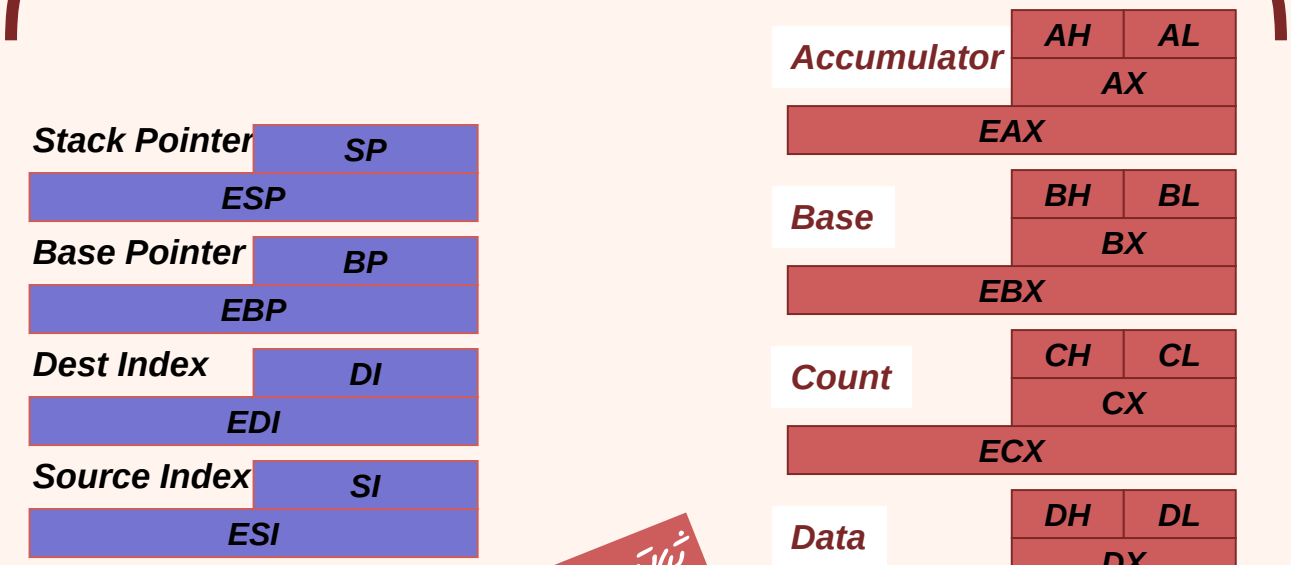


- این فضا برای همه‌ی برنامه‌ها از آدرس 0x8048000 شروع و تا آدرس 0xbfffffff ادامه دارد.
- وظیفه‌ی تبدیل آدرس بر عهده‌ی سیستم‌عامل است.

ثبات‌های پردازنده‌ی خانواده‌ی X86

General Purpose

ثبات‌های همه‌منظوره

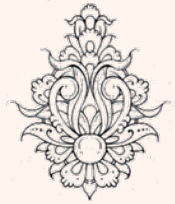


Index Registers

ثبات‌های شاخص

Special Registers

ثبات‌های خاص‌منظوره



کاربردهای خاص ثبات‌ها

- General-Purpose
  - EAX – accumulator

«انباره»: نتایج محاسبات ریاضی در این ثبات قرار می‌گیرد

  - EBX- base index

آدرس پایه‌ی خانه‌های حافظه را در این ثبات قرار می‌گیرد

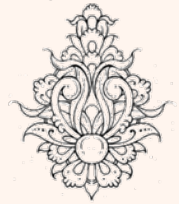
  - ECX – loop counter

به عنوان شمارنده‌ی حلقه استفاده می‌شود

قابلیت کاهش/افزایش به صورت خودکار را دارد

  - EDX – Data Register

حاصل برخی دستورالعمل‌ها مانند قسمت پرارزش ضرب در این ثبات قرار می‌گیرد



ثبات‌های شاخص

- ESP – stack pointer

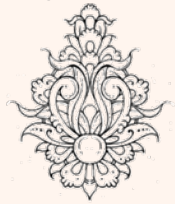
اشاره‌گر پشته

- EBP – extended frame pointer (stack)

با استفاده از این اشاره‌گر می‌توان بدون نیاز اشاره‌گر پشته به محتوای آن دست یافت، بر ای دسترسی به آرگومان‌های تابع مورد استفاده قرار می‌گیرد

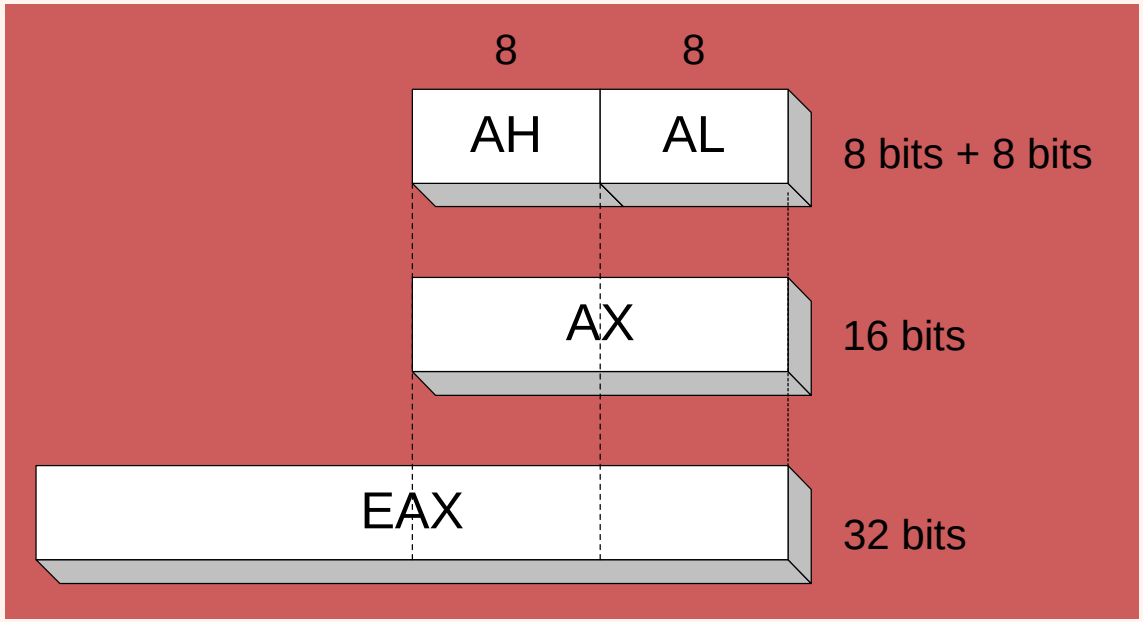
- ESI, EDI – index registers

ثبات‌های منبع و مقصد:
آدرس شروع رشته/آرایه را در خود نگه می‌دارند
برای کار با رشته‌ها و ساختارهای مشابه به کار می‌روند



دسترسی به بخش‌های مختلف ثبات‌های همه‌منظوره

- با استفاده از نام مناسب می‌توان به بخش‌های مختلف یک ثبات دسترسی پیدا کرد.

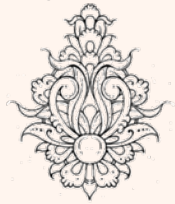


32-bit	16-bit	8-bit (high)	8-bit (low)
EAX	AX	AH	AL
EBX	BX	BH	BL
ECX	CX	CH	CL
EDX	DX	DH	DL

دسترسی به بخش‌های مختلف ثبات‌های پایه و شاخص

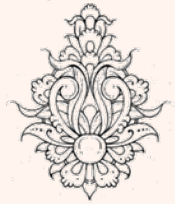
- تنها می‌توان به شانزده بیت کم‌ارزش این ثبات‌ها به صورت مستقل دسترسی پیدا کرد.

32-bit	16-bit
ESI	SI
EDI	DI
EBP	BP
ESP	SP



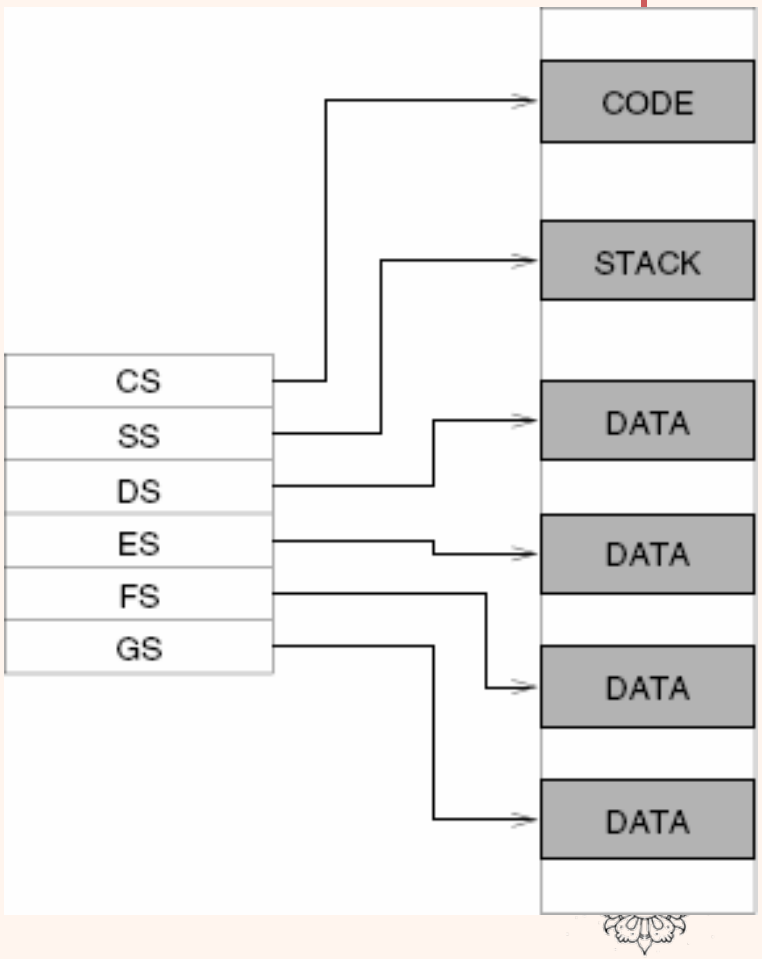
segmented memory

- در پردازنده‌ی ۸۰۲۸۶، ثبات‌ها ۱۶ بیتی است، در حالی که گذرگاه آدرس بیست و چهار بیتی است. بدین ترتیب کل آدرس در یک ثبات نمی‌گنجد.
- برای رفع این مشکل آدرس هر خانه‌ی حافظه با کمک دو ثبات نشان داده می‌شود.
- در واقع حافظه به قسمت‌هایی تقسیم می‌شود، آدرس هر بخش در یک سری ثبات به نام ثبات segment نگهداری می‌شود.



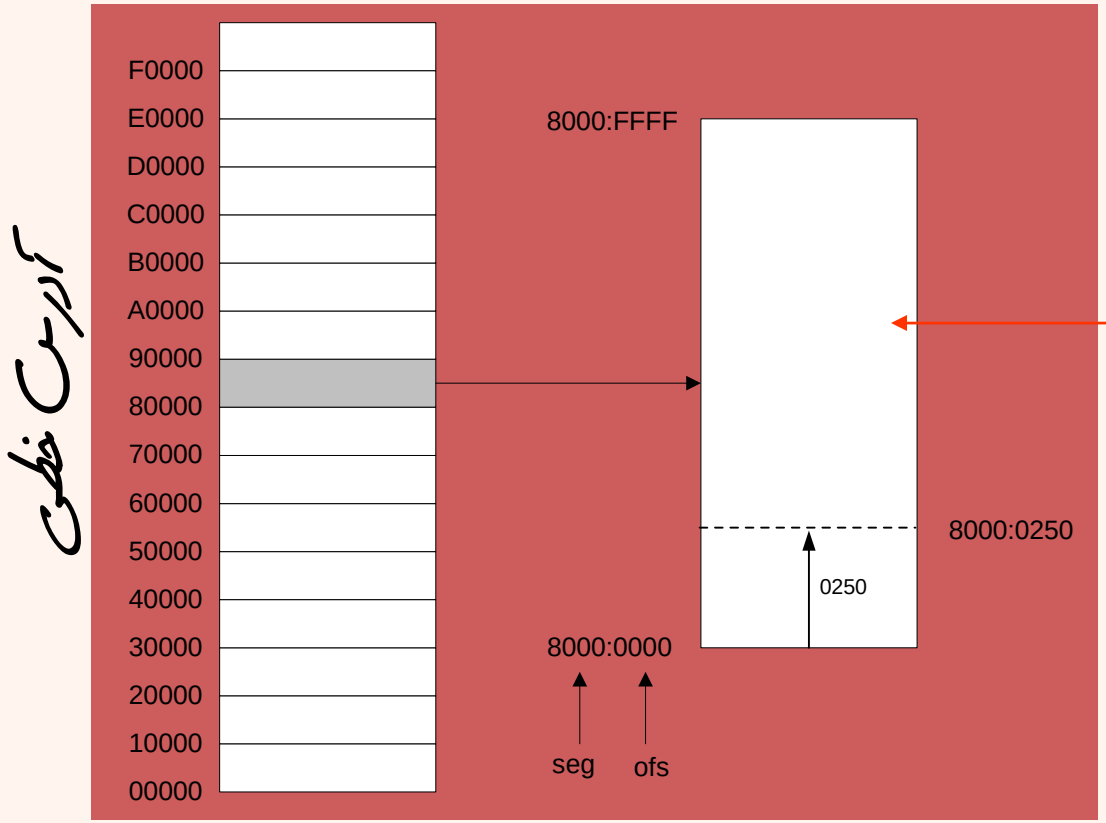
نگاهی گذرا به ثبات‌های سگمنت

CS	Code Segment
DS	Data Segment
ES	Extra Segment
SS	Stack Segment
FS	
GS	



segmented memory

Segmented Memory



یک سگمنت از حافظه

Irvine, Kip R. Assembly Language for Intel-Based Computers, 2003.

segmented memory

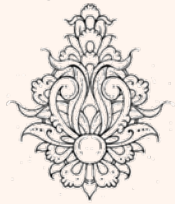
- در این حالت حافظه به بخش‌هایی (segment) تقسیم می‌شود.
- در این حالت آدرس به صورت «Segment:Offset» نمایش داده می‌شود.
- به عنوان مثال در ۸۰۸۶ که خطوط آدرس بیست بیتی است، برای محاسبه‌ی آدرس خطی (linear address) بخش سگمنت چهار بیت به سمت چپ شیفت داده شده و با بخش آفست جمع می‌شود.
- مثال:

2222:3333 → 22220+3333 → 25553

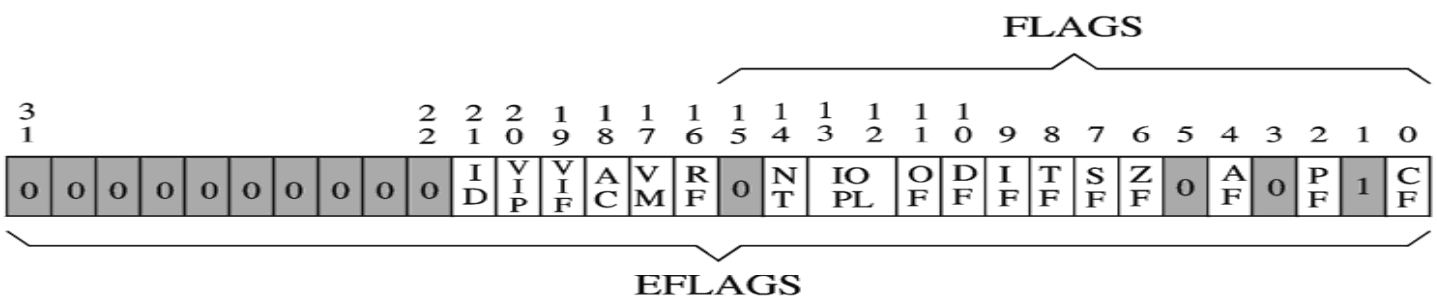
2000:5553 → 20000+5553 → 25553

flat memory model

- در سیستم‌های سی‌ودو بیتی، می‌توان کل فضای حافظه را به صورت پیوسته مورد استفاده قرار داد، از این‌رو ثبات‌های segment مورد استفاده قرار نمی‌گیرند.



نگاهی کلی به ثبات پرچم‌ها



Status flags

CF = Carry flag
PF = Parity flag
AF = Auxiliary carry flag
ZF = Zero flag
SF = Sign flag
OF = Overflow flag

Control flags

DF = Direction flag

System flags

TF = Trap flag
IF = Interrupt flag
IOPL = I/O privilege level
NT = Nested task
RF = Resume flag
VM = Virtual 8086 mode
AC = Alignment check
VIF = Virtual interrupt flag
VIP = Virtual interrupt pending
ID = ID flag

پرچم‌های وضعیت

- EFLAGS
  - status flags
  - control flags
  - system flags

هر پرچم (flag) یک بیت است که به طور گسترده در دستورات پرش شرطی مورد استفاده قرار می‌گیرد

- Carry
  - unsigned arithmetic out of range
- Parity
  - sum of 1 bits is an even number
- Adjust Flag (Auxiliary Carry)
  - used for BCD numbers
- Zero
  - result is zero
- Sign
  - result is negative
- Overflow
  - signed arithmetic out of range

Status flags

۱۵	۱۴	۱۳	۱۲	۱۱	۱۰	۹	۸	۷	۶	۵	۴	۳	۲	۱	۰
				OF				SF	ZF		AF		PF		CF

پرچم‌های کنترلی و سیستمی

Direction Flag

- «پرچم‌های کنترلی» برای تعیین نحوه‌ی عملکرد سیستم به کار می‌روند. برای Pentium 4 تنها یک بیت کنترلی با نام DF تعریف شده است.
- این بیت به پردازنده اعلام می‌کند در مواجهه با رشته‌ها چگونه عمل کند. در صورتی که مقدار این بیت صفر باشد، دستورات رشته پس اجرا آدرس را کم می‌کنند.
- «پرچم‌های سیستمی»، برای کنترل عملیات در سطح سیستم‌عامل به کار می‌رود.

System Flags

ثبات‌های کنترلی

- ثبات‌های کنترلی، اسلوب کاری پردازنده را مشخص می‌کند.

Control registers

Control Register	Description
CR0	System flags that control the operating mode and states of the processor
CR1	Not currently used
CR2	Memory page fault information
CR3	Memory page directory information
CR4	Flags that enable processor features and indicate feature capabilities of the processor

مقدار این ثبات‌ها به صورت مستقیم قابل دسترسی نیستند، برای دسترسی به آنها و تغییر احتمالی ابتدا محتوای آن به ثبات‌های عمومی منتقل می‌شود، پس از اعمال تغییرات مورد نیاز، مقدار ثبات عمومی دوباره به ثبات کنترلی بازگردانده می‌شود.

در خانواده‌ی X86-64 ثبات دیگری با نام Extended Feature Enable Register اضافه شده است، برای رفتن به long mode از این ثبات استفاده می‌شود.

(EFER)