

x86 Architecture Details تفاصيل العمارة إلى **x86**

In this section, we focus on the basic architectural features of the x86 processor family, which includes both Intel IA-32 and 32-bit AMD processors .

في هذا القسم ، نركز على الميزات المعمارية الأساسية لعائلة المعالجات x86 ، والتي تتضمن كلاً من معالجات Intel IA-32 و 32 بت AMD.

Modes of Operation أساليب عملها

x86 processors have three primary modes of operation: protected mode, real-address mode, and system management mode. A sub-mode, named virtual-8086, is a special case of protected mode. Here are short descriptions of each:

تحتوي معالجات x86 على ثلاثة أوضاع أساسية للتشغيل: الوضع المحمي ووضع العنوان الحقيقي ووضع إدارة النظام. الوضع الفرعي ، المسمى Virtual-8086 ، هو حالة خاصة للوضع المحمي. فيما يلي أوصاف مختصرة لكل منها:

Protected Mode وضع حماية

Protected mode is the native state of the processor, in which all instructions and features are available. Programs are given separate memory areas named segments, and the processor prevents programs from referencing memory outside their assigned segments.

الوضع المحمي هو الحالة الأصلية للمعالج ، حيث تتوفر جميع الإرشادات والميزات. يتم إعطاء البرامج مناطق ذاكرة منفصلة تسمى المقاطع ، ويمنع المعالج البرامج من الرجوع إلى الذاكرة خارج الأجزاء المخصصة لها.

Virtual-8086 Mode While in protected mode, the processor can directly execute real-address mode software such as MS-DOS programs in a safe multitasking environment. In other words, if an MS-DOS program crashes or attempts to write data into the system memory area, it will not affect other

programs running at the same time. Windows XP can execute multiple separate virtual-8086 sessions at the same time.

وضع Virtual-8086 أثناء التواجد في الوضع المحمي ، يمكن للمعالج تنفيذ برنامج وضع العنوان الحقيقي مباشرةً مثل برامج MS-DOS في بيئة متعددة المهام آمنة. بمعنى آخر ، إذا تعطل برنامج MS-DOS أو حاول كتابة البيانات في منطقة ذاكرة النظام ، فلن يؤثر ذلك على البرامج الأخرى التي تعمل في نفس الوقت. يمكن لـ Windows XP تنفيذ عدة جلسات منفصلة لـ Virtual-8086 في نفس الوقت.

Real-Address Mode وضع العنوان الحقيقي

Real-address mode implements the programming environment of the Intel 8086 processor with a few extra features, such as the ability to switch into other modes.

This mode is available in Windows 98, and can be used to run an MS-DOS program that requires direct access to system memory and hardware devices. Programs running in real-address mode can cause the operating system to crash (stop responding to commands).

يطبق وضع العنوان الحقيقي بيئة البرمجة الخاصة بمعالج Intel 8086 مع بعض الميزات الإضافية ، مثل القدرة على التبديل إلى أوضاع أخرى.

يتوفر هذا الوضع في نظام التشغيل Windows 98 ، ويمكن استخدامه لتشغيل برنامج MS-DOS يتطلب الوصول المباشر إلى ذاكرة النظام والأجهزة. يمكن أن تتسبب البرامج التي تعمل في وضع العنوان الحقيقي في تعطل نظام التشغيل (توقف عن الاستجابة للأوامر).

System Management Mode وضع إدارة النظام

System Management mode (SMM) provides an operating system with a mechanism for implementing functions such as power management and system security. These functions are usually implemented by computer manufacturers who customize the processor for a particular system setup.

يوفر وضع إدارة النظام (SMM) لنظام التشغيل آلية لتنفيذ وظائف مثل إدارة الطاقة وأمن النظام. عادة ما يتم تنفيذ هذه الوظائف من قبل الشركات المصنعة للكمبيوتر الذين يقومون بتخصيص المعالج لإعداد نظام معين.

Address Space مساحة العنوان

In 32-bit protected mode, a task or program can address a linear address space of up to 4 GBytes. Beginning with the P6 processor, a technique called Extended Physical Addressing allows a total of 64 GBytes of physical memory to be addressed. Real-address mode programs, on the other hand, can only address a range of 1 MByte. If the processor is in protected mode and running multiple programs in virtual-8086 mode, each program has its own 1-MByte memory area.

في الوضع المحمي 32 بت ، يمكن لمهمة أو برنامج معالجة مساحة عنوان خطية تصل إلى 4 جيجابايت. بدءًا من المعالج P6 ، تتيح تقنية تسمى Extended Physical Addressing معالجة ما مجموعه 64 جيجابايت من الذاكرة الفعلية. من ناحية أخرى ، يمكن لبرامج وضع العنوان الحقيقي معالجة نطاق من 1 ميغابايت فقط. إذا كان المعالج في الوضع المحمي ويقوم بتشغيل برامج متعددة في الوضع الظاهري 8086 ، فكل برنامج منطقة ذاكرة 1 ميغابايت خاصة به.

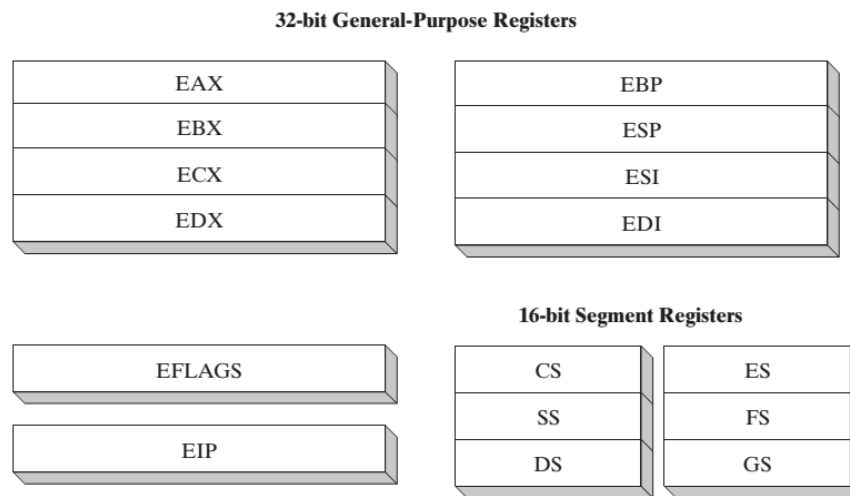
Basic Program Execution Registers سجلات تنفيذ البرنامج الأساسي

Registers are high-speed storage locations directly inside the CPU, designed to be accessed at much higher speed than conventional memory. When a processing loop is optimized for speed, for example, loop counters are held in registers rather than variables. Figure 3 shows the basic program execution registers. There are eight general-purpose registers, six segment registers, a processor status flags register (EFLAGS), and an instruction pointer (EIP).

السجلات هي مواقع تخزين عالية السرعة مباشرة داخل وحدة المعالجة المركزية ، وهي مصممة ليتم الوصول إليها بسرعة أعلى بكثير من الذاكرة التقليدية. عندما يتم تحسين حلقة المعالجة للسرعة ، على سبيل

المثال ، يتم تعليق عدادات الحلقة في سجلات بدلاً من المتغيرات. يوضح الشكل 3 سجلات تنفيذ البرنامج الأساسية. هناك ثمانية سجلات للأغراض العامة ، وستة سجلات مقاطع ، وسجل أعلام حالة المعالج (EFLAGS) ، ومؤشر تعليمات (EIP).

Figure 3 : The basic program execution registers.

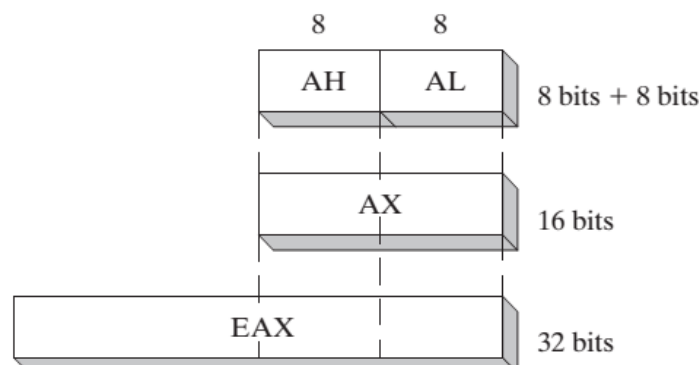


General-Purpose Registers سجلات الأغراض العامة

The general-purpose registers are primarily used for arithmetic and data movement. As shown in Figure 4, the lower 16 bits of the EAX register can be referenced by the name AX.

تستخدم سجلات الأغراض العامة بشكل أساسي في العمليات الحسابية وحركة البيانات. كما هو مبين في الشكل 4 ، يمكن الإشارة إلى أقل 16 بتًا من سجل EAX بالاسم AX.

Figure 4: general-purpose registers.



Portions of some registers can be addressed as 8-bit values. For example, the AX register, has an 8-bit upper half named AH and an 8-bit lower half named AL. The same overlapping relationship exists for the EAX, EBX, ECX, and EDX registers:

يمكن معالجة أجزاء من بعض السجلات كقيم 8 بت. على سبيل المثال ، يحتوي سجل AX على نصف علوي من 8 بت يسمى AH ونصفه سفلي 8 بت يسمى AL. توجد نفس العلاقة المتداخلة لسجلات EAX و EBX و ECX و EDX:

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

The remaining general-purpose registers can only be accessed using 32-bit or 16-bit names, as shown in the following table:

لا يمكن الوصول إلى سجلات الأغراض العامة المتبقية إلا باستخدام أسماء 32 بت أو 16 بت ، كما هو موضح في الجدول التالي:

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

Specialized Uses Some general-purpose registers have specialized uses:

- EAX is automatically used by multiplication and division instructions. It is often called the extended accumulator register.
- The CPU automatically uses ECX as a loop counter.
- ESP addresses data on the stack (a system memory structure). It is rarely used for ordinary arithmetic or data transfer. It is often called the extended stack pointer register.

- ESI and EDI are used by high-speed memory transfer instructions. They are sometimes called the extended source index and extended destination index registers.
- EBP is used by high-level languages to reference function parameters and local variables on the stack. It should not be used for ordinary arithmetic or data transfer except at an advanced level of programming. It is often called the extended frame pointer register.

الاستخدامات المتخصصة: لبعض سجلات الأغراض العامة استخدامات متخصصة:

- يتم استخدام EAX تلقائيًا عن طريق تعليمات الضرب والقسمة. غالبًا ما يطلق عليه سجل المجمع الممتد.
- تستخدم وحدة المعالجة المركزية (CPU) تلقائيًا ECX كمقياس حلقي.
- يعالج ESP البيانات الموجودة على المكس (بنية ذاكرة النظام). نادرًا ما يستخدم في العمليات الحسابية العادية أو لنقل البيانات. غالبًا ما يطلق عليه سجل مؤشر المكس الممتد.
- يتم استخدام ESI و EDI بواسطة تعليمات نقل الذاكرة عالية السرعة. يطلق عليهم أحيانًا اسم فهرس المصدر الموسع وسجلات فهرس الوجهة الموسعة.
- يتم استخدام EBP من قبل اللغات عالية المستوى للإشارة إلى معلمات الوظيفة والمتغيرات المحلية على المكس. لا ينبغي استخدامه للحساب العادي أو نقل البيانات إلا في مستوى متقدم من البرمجة. غالبًا ما يطلق عليه سجل مؤشر الإطار الموسع.

تسجيلات القطاع Segment Registers

In real-address mode, 16-bit segment registers indicate base addresses of preassigned memory areas named segments. In protected mode, segment registers hold pointers to **segment descriptor tables**. Some segments hold program instructions (code), others hold variables (data), and another segment named the stack segment holds local function variables and function parameters.

في وضع العنوان الحقيقي ، تشير سجلات مقطع 16 بت إلى العناوين الأساسية لمناطق الذاكرة المعينة مسبقًا المسماة بالمقاطع. في الوضع المحمي ، تحتفظ تسجيلات المقطع بالمؤشرات إلى جداول واصف

المقطع. تحتوي بعض المقاطع على تعليمات البرنامج (رمز) ، بينما يحتفظ البعض الآخر بالمتغيرات (البيانات) ، بينما يحتوي جزء آخر يسمى مقطع المكس على متغيرات الوظيفة المحلية ومعلومات الوظيفة.

Instruction Pointer مؤشر التعليمات

The EIP, or instruction pointer, register contains the address of the next instruction to be executed. Certain machine instructions manipulate EIP, causing the program to branch to a new location.

يحتوي مؤشر EIP ، أو مؤشر التعليمات ، على عنوان التعليمات التالية التي سيتم تنفيذها. تعالج تعليمات معينة للجهاز EIP ، مما يتسبب في تفرع البرنامج إلى موقع جديد.

EFLAGS Register سجل EFLAGS

The EFLAGS (or just Flags) register consists of individual binary bits that control the operation of the CPU or reflect the outcome of some CPU operation. Some instructions test and manipulate individual processor flags.

يتكون سجل EFLAGS (أو الأعلام فقط) من وحدات ثنائية فردية تتحكم في تشغيل وحدة المعالجة المركزية أو تعكس نتيجة بعض عمليات وحدة المعالجة المركزية. تختبر بعض التعليمات أعلام المعالج الفردية وتتلاعب بها.

Control Flags أعلام التحكم

Control flags control the CPU's operation. For example, they can cause the CPU to break after every instruction executes, interrupt when arithmetic overflow is detected, enter virtual-8086 mode, and enter protected mode.

Programs can set individual bits in the EFLAGS register to control the CPU's operation. *Examples are the Direction and Interrupt flags.*

تتحكم أعلام التحكم في تشغيل وحدة المعالجة المركزية. على سبيل المثال ، يمكن أن تتسبب في تعطيل وحدة المعالجة المركزية بعد تنفيذ كل تعليمات ، والمقاطعة عند اكتشاف تجاوز حسابي ، وإدخال الوضع الظاهري 8086 ، والدخول إلى الوضع المحمي. يمكن للبرامج تعيين وحدات البت الفردية في سجل EFLAGS للتحكم في تشغيل وحدة المعالجة المركزية. الأمثلة هي إشارات الاتجاه والمقاطعة.

Status Flags أعلام الحالة

The Status flags reflect the outcomes of arithmetic and logical operations performed by the CPU. They are the Overflow, Sign, Zero, Auxiliary Carry, Parity, and Carry flags.

تعكس إشارات الحالة نتائج العمليات الحسابية والمنطقية التي تقوم بها وحدة المعالجة المركزية. وهي أعلام Overflow و Sign و Zero و Auxiliary Carry و Parity و Carry.

Their abbreviations are shown immediately after their names:

- The *Carry flag* (CF) is set when the result of an unsigned arithmetic operation is too large to fit into the destination.
- The *Overflow flag* (OF) is set when the result of a signed arithmetic operation is too large or too small to fit into the destination.
- The *Sign flag* (SF) is set when the result of an arithmetic or logical operation generates a negative result.
- The *Zero flag* (ZF) is set when the result of an arithmetic or logical operation generates a result of zero.
- The *Auxiliary Carry flag* (AC) is set when an arithmetic operation causes a carry from bit 3 to bit 4 in an 8-bit operand.
- The *Parity flag* (PF) is set if the least-significant byte in the result contains an even number of 1 bits. Otherwise, PF is clear. In general, it is used for error checking when there is a possibility that data might be altered or corrupted.

تظهر اختصاراتهم مباشرة بعد أسمائهم:

- يتم تعيين علامة الحمل (CF) عندما تكون نتيجة عملية حسابية غير موقعة كبيرة جدًا بحيث لا تتناسب مع الوجهة.

- يتم تعيين علامة Overflow (OF) عندما تكون نتيجة العملية الحسابية الموقعة كبيرة جدًا أو صغيرة جدًا بحيث لا تتناسب مع الوجهة.
- يتم تعيين علامة الإشارة (SF) عندما تولد نتيجة عملية حسابية أو منطقية نتيجة سلبية.
- يتم تعيين علامة الصفر (ZF) عندما تنتج نتيجة عملية حسابية أو منطقية نتيجة الصفر.
- يتم ضبط علم الحمل المساعد (AC) عندما تتسبب عملية حسابية في نقل من بت 3 إلى بت 4 في معامل 8 بتات.
- يتم تعيين علامة التكافؤ (PF) إذا كانت البايته الأقل دلالة في النتيجة تحتوي على عدد زوجي من 1 بت. خلاف ذلك ، PF واضح. بشكل عام ، يتم استخدامه للتحقق من الأخطاء عندما يكون هناك احتمال أن يتم تغيير البيانات أو تلفها.

MMX Registers تسجيلات MMX

MMX technology was added onto the Pentium processor by Intel to improve the performance of advanced multimedia and communications applications. The eight 64-bit MMX registers support special instructions called SIMD (Single-Instruction, Multiple-Data). As the name implies, MMX instructions operate in parallel on the data values contained in MMX registers. Although they appear to be separate registers, the MMX register names are in fact aliases to the same registers used by the floating-point unit.

تمت إضافة تقنية MMX إلى معالج Pentium بواسطة Intel لتحسين أداء الوسائط المتعددة وتطبيقات الاتصالات المتقدمة. تدعم سجلات MMX الثمانية ذات 64 بت تعليمات خاصة تسمى SIMD (تعليمات فردية ، بيانات متعددة). كما يوحي الاسم ، تعمل تعليمات MMX بالتوازي مع قيم البيانات الموجودة في سجلات MMX. على الرغم من أنها تبدو سجلات منفصلة ، إلا أن أسماء سجلات MMX هي في الواقع أسماء مستعارة لنفس السجلات التي تستخدمها وحدة الفاصلة العائمة.

XMM Registers

The x86 architecture also contains eight 128-bit registers called XMM registers. They are used by streaming SIMD extensions to the instruction set.

تحتوي بنية x86 أيضًا على ثمانية سجلات 128 بت تسمى سجلات XMM. يتم استخدامها عن طريق دفع ملحقات SIMD إلى مجموعة التعليمات.