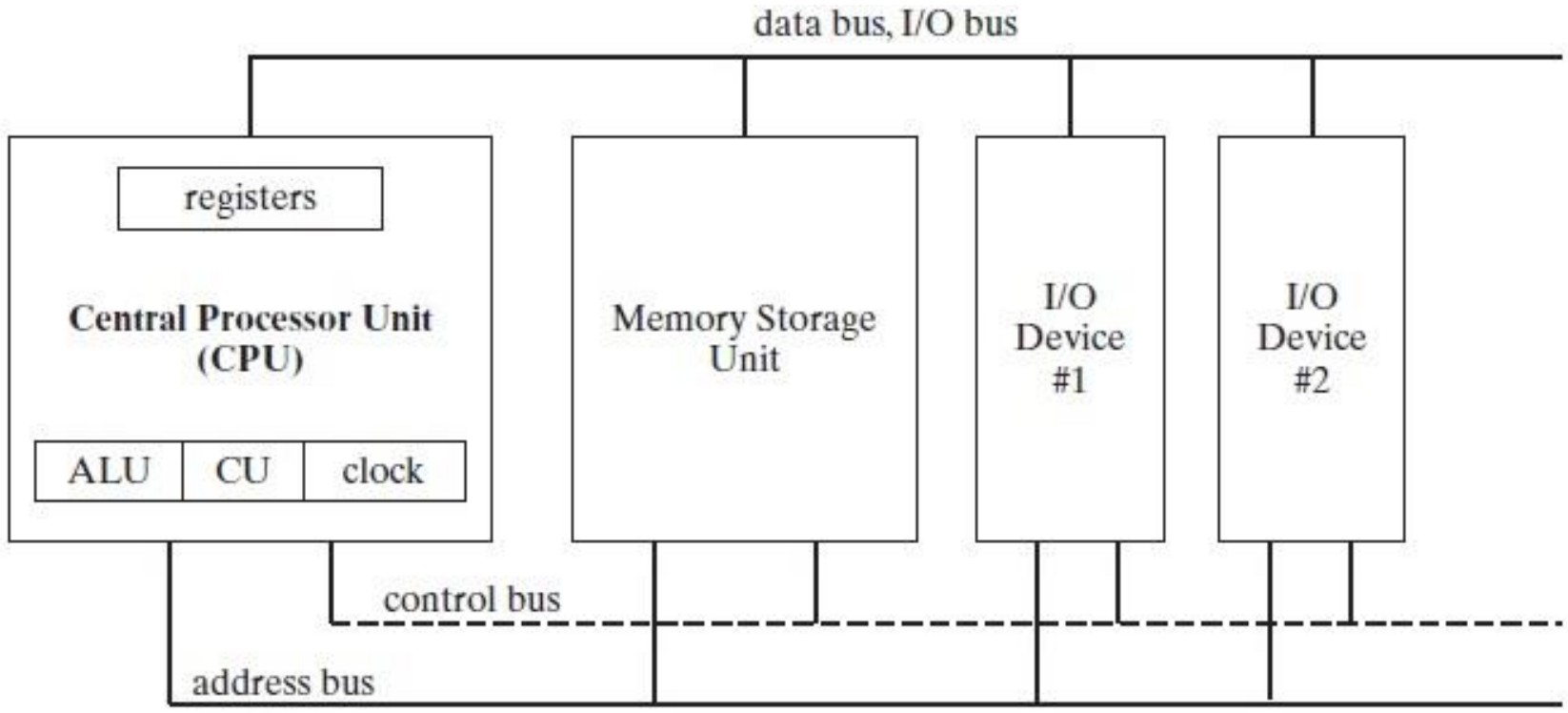
x86 Processor Architecture

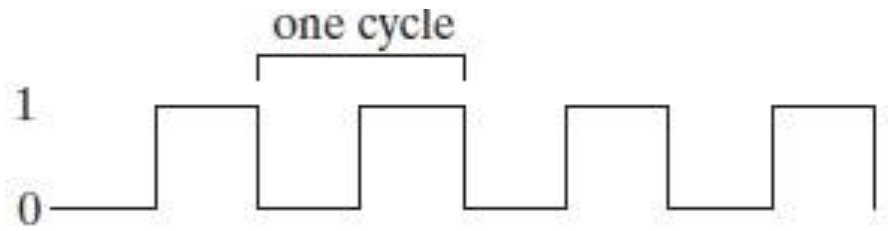
TEXT2 (2.2-2.5)

General microprocessor overview



The Clock

- Each operation involving the CPU and the system bus is synchronized by an internal clock pulsing at a constant rate.
- The basic unit of time for machine instructions is a *machine cycle* (or *clock cycle*).
- The speed of oscillation of the clock is usually quoted per processor.
- A 1GHz processor has a clock that oscillates 1 billion times per second.
- The duration of a clock cycle is calculated as the reciprocal of the clock's speed. (1ns for a 1GHz clock)



x86 Processors

- x86 processors have three primary modes of operation:
- *Protected Mode*

  Protected mode is the native state of the processor, in which all instructions and features are available.

- *Real-Address Mode*

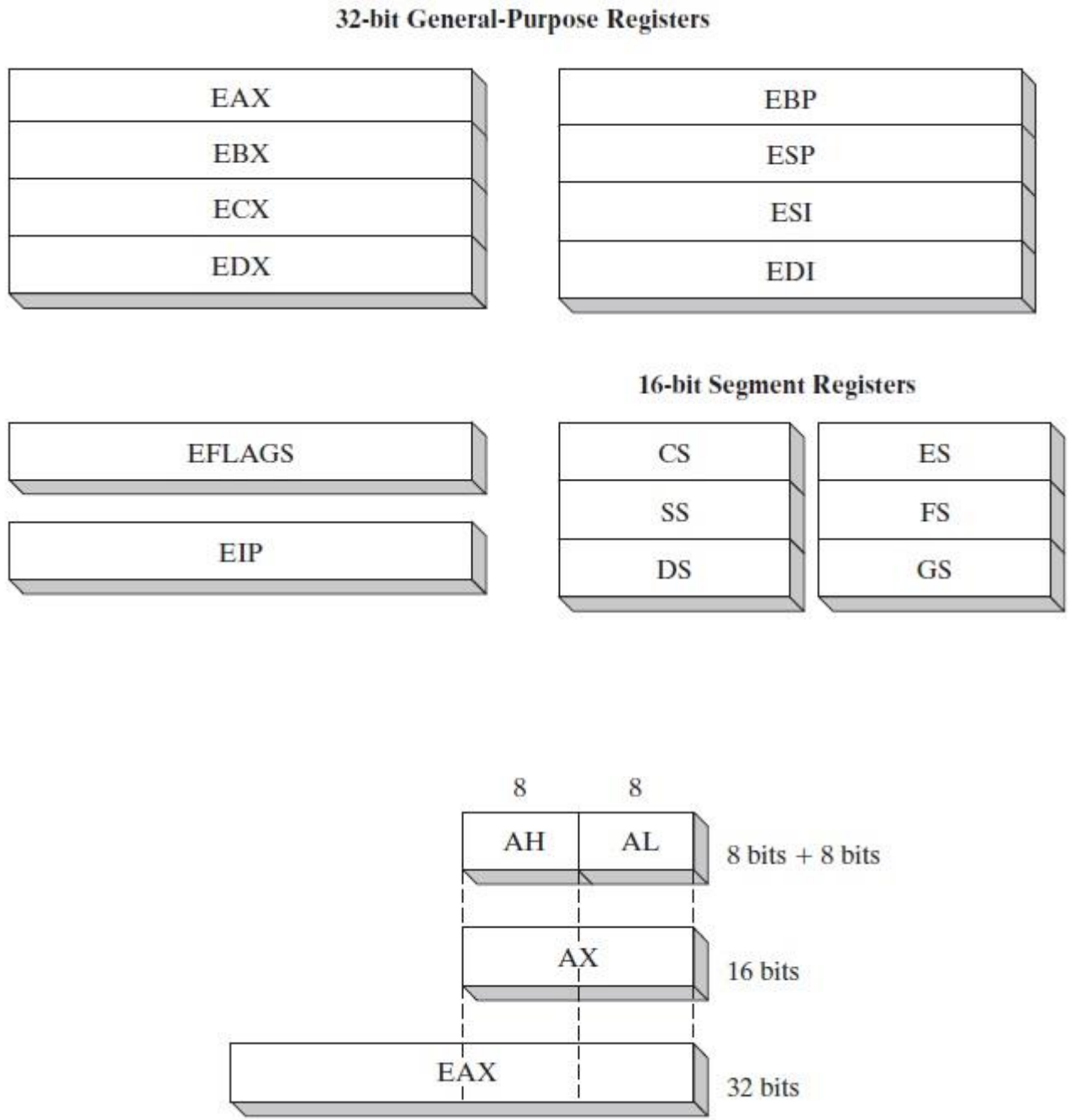
  Real-address mode implements the programming environment of the Intel 8086 processor with a few extra features.

- *System Management Mode*

  provides an operating system with a mechanism for implementing functions such as power management and system security.

Basic x86 Program Registers

- *Registers* are high-speed storage locations directly inside the CPU, designed to be accessed at much higher speed than conventional memory.
- The *general-purpose registers* are primarily used for arithmetic and data movement.
- Portions of some registers can be addressed as lower 16-bit or 8-bit values.
- For example, the EAX register has a lower 16-bit AX part, while the AX register, has an 8-bit upper half named AH and an 8-bit lower half named AL.


32-bit General-Purpose Registers
EAX
EBX
ECX
EDX
EBP
ESP
ESI
EDI
16-bit Segment Registers
EFLAGS
EIP
CS
SS
DS
ES
FS
GS
8
8
AH
AL
8 bits + 8 bits
AX
16 bits
EAX
32 bits

- All ..X general purpose registers can be expressed in the same formats shown for EAX previously.

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

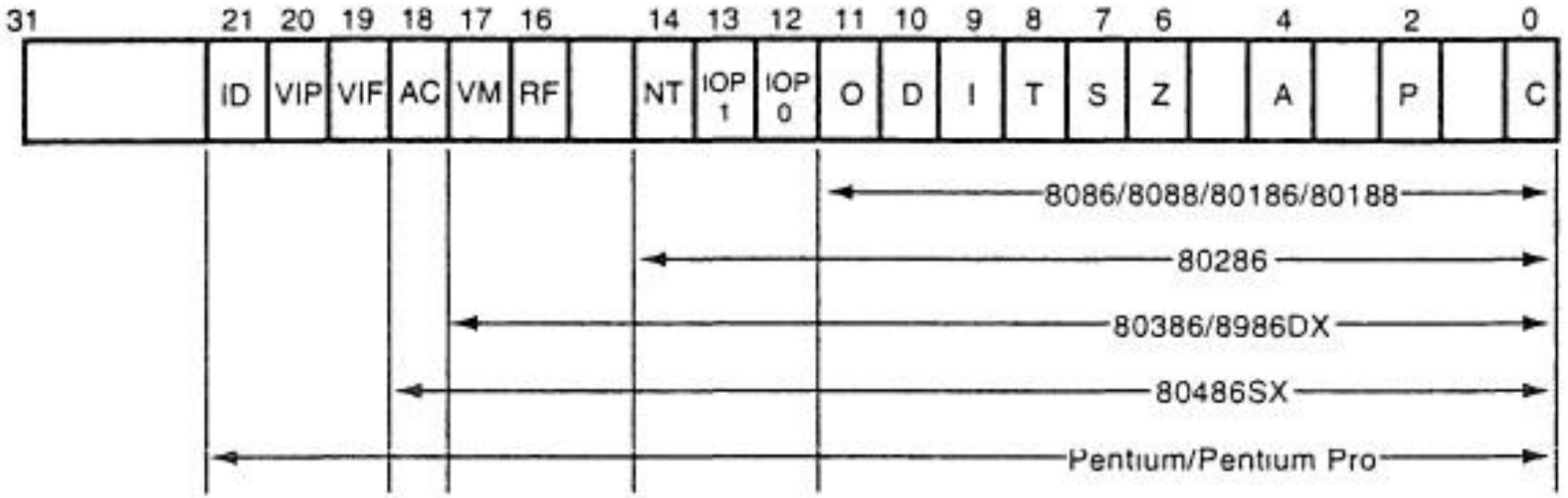
32-Bit	16-Bit
ESI	SI
EDI	DI
EBP	BP
ESP	SP

Special-purpose general-purpose registers

- EAX: Used for multiplication and division instructions.
- ECX: Used by the CPU as a counter in loop instructions (automatic)
- ESP: Used to point to the stack
- ESI and EDI: Used for high speed memory transfer instructions.
- EBP: Points to a memory location on the stack. Usually used by high level languages.
- The EIP: stores the address of the next instruction to be executed.

- EFLAGS: They indicate the condition of the microprocessor and control its operation.
- Status flags: reflect the outcomes of arithmetic and logical operations performed by the CPU.
  - **Carry** flag (CF): result is too large to fit into the destination (*unsigned*).
  - **Overflow** flag (OF): result is too large or too small to fit into the destination (*signed*).
  - **Sign** flag (SF): result is negative.
  - **Zero** flag (ZF): result is zero.
  - **Auxiliary Carry** flag (AC): a carry from bit 3 to bit 4 in an 8-bit operand.
  - The **Parity** flag (PF): the least-significant byte in the result contains an even number of 1 bits.

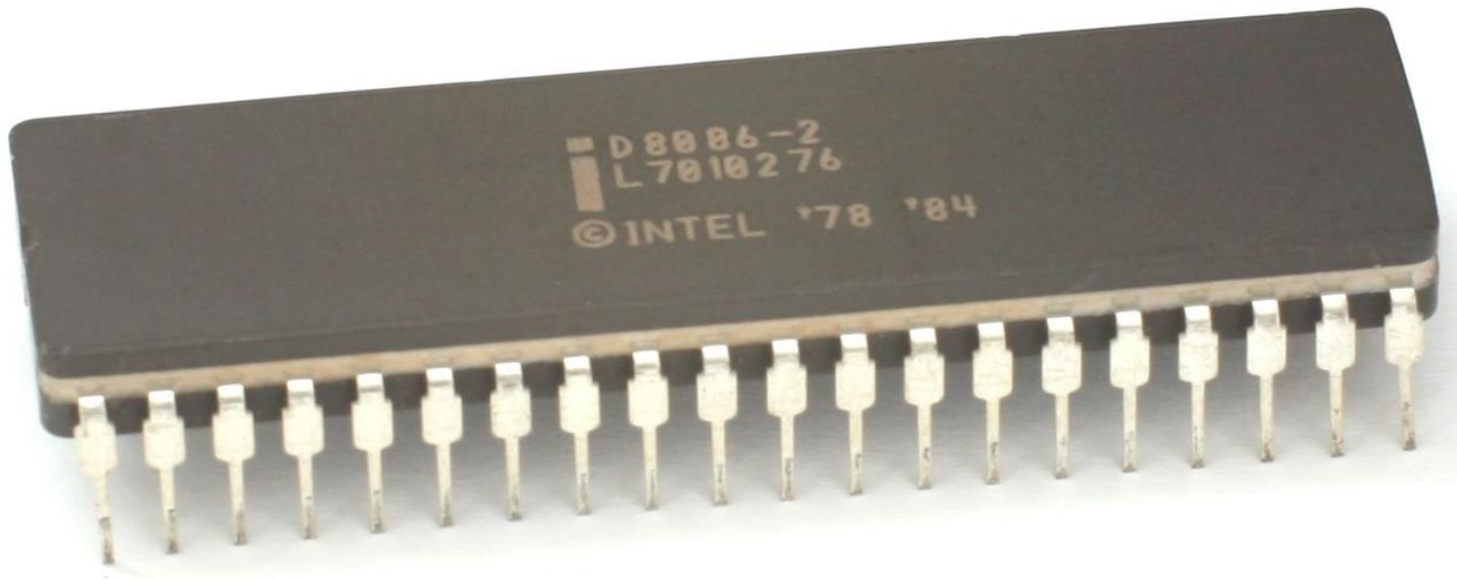
EFLAG register for x86 processors (up to Pentium)



Control Flags

- I (Interrupt): controls interrupt request pin (INTR). If I=1 pin is enabled. If I=0, the pin is enabled. (Assembly: **STI** and **CLI**)
- D (direction): Sets increment or decrement mode for DI and/or SI registers. D=1:automatic increment, D=2:automatic decrement. (Ass. **STD** and **CLD**)

The Intel 8086

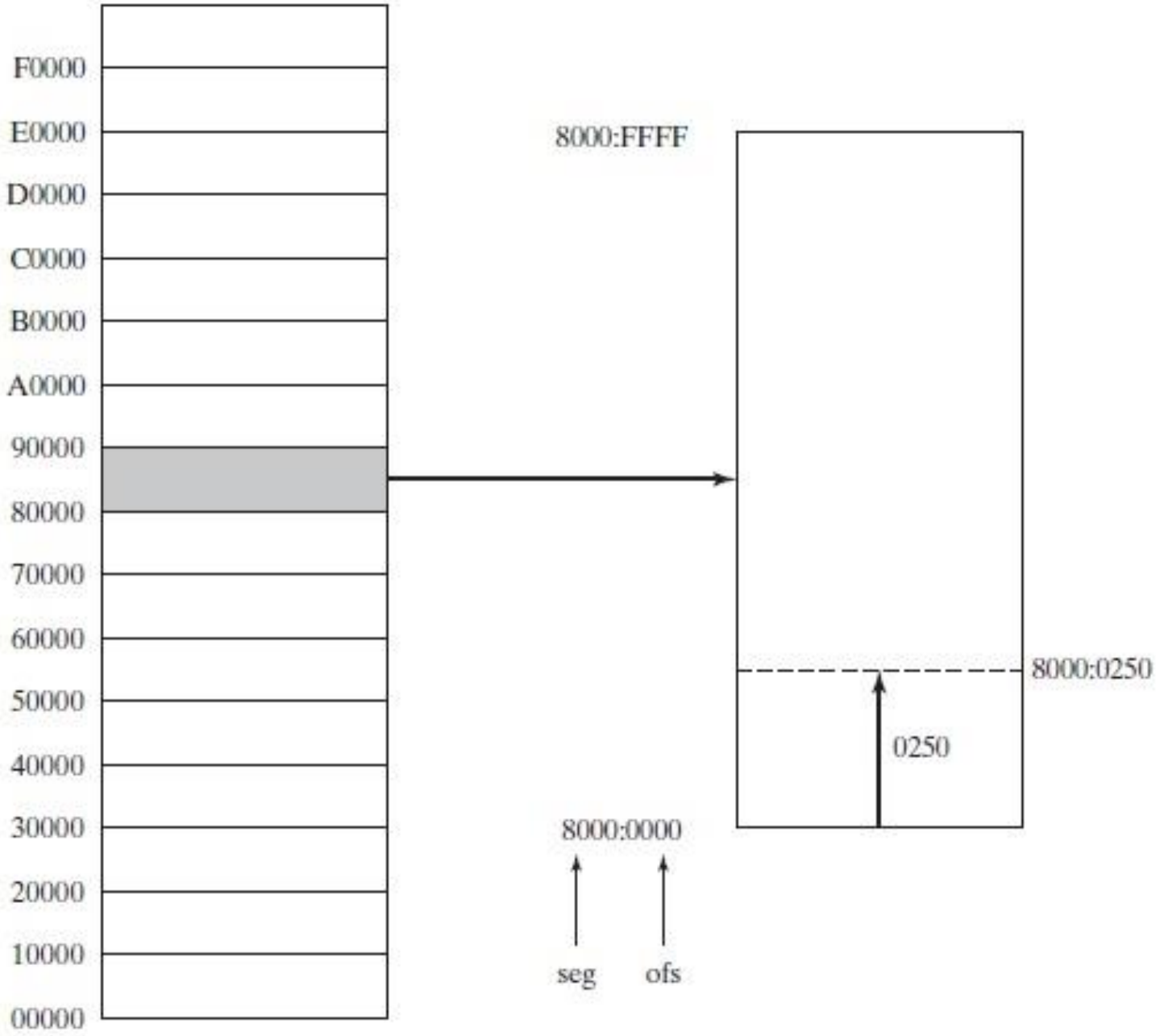


- The Intel 8086 processor (1978) marked the beginning of the modern Intel architecture family.
- Primary innovations: 16-bit registers, a 16-bit data bus and a segmented memory model permitting programs to address up to 1 MByte of RAM.
- The original IBM PC contained the 8088, a slightly modified version of the 8086.

Backward Compatibility
Each processor introduced into the Intel family since the 8086 has been backward-compatible with earlier processors.

Real Address Mode

- In real-address mode, an x86 processor can access 1,048,576 bytes of memory (1 MByte) using 20-bit addresses in the range 00000H to FFFFFH.
- Intel engineers had to solve a basic problem: the 8086 had 16 bit registers.
- They came up with a scheme known as *segmented memory*. All of memory is divided into 64-kilobyte (64-KByte) units called *segments*.



- Each segment begins at an address having a zero for its last hexadecimal digit.
- To specify a particular byte address, the ***base*** address of its segment, as well as an ***offset*** is needed.
- Hence addresses are in the form- segment:offset
- The actual address is referred to as the physical, linear or effective address.

- The segment registers CS, DS, SS, ES, FS and GS are used for storing the base addresses of segments.
- A typical program has three segments: code, data, and stack.
- CS, DS and SS are used with these respectively.
- ES, FS and GS may be used for ‘extra’ purposes.

Protected Mode

- Protected mode is the more powerful “native” processor mode.
- When running in protected mode, a program’s linear address space is 4 GBytes, using addresses 0 to FFFFFFFF hexadecimal.
- The **flat** segmentation model is appropriate for protected mode programming in MASM.
- In the flat segmentation model, all segments are mapped to the entire 32-bit physical address space of the computer.
- Segment registers point to *segment descriptor tables,* which the operating system uses to keep track of locations of individual program segments.

Reminder

- Download Visual Studio Express Edition for Assembly language programming.