Chapter-7

Advanced Microprocessors

80286 MPU

Salient features of 80286

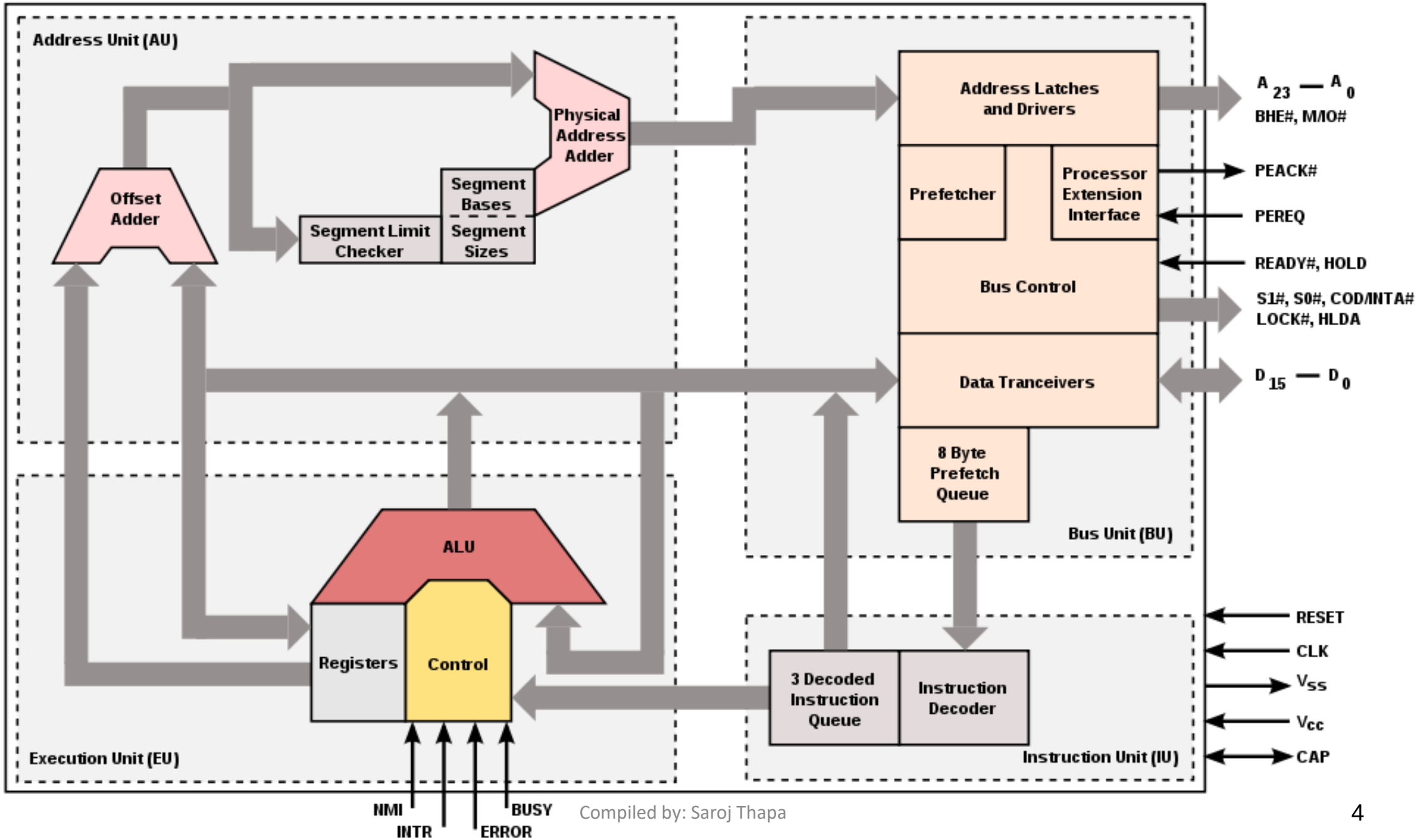
- High performance microprocessor with memory management and protection
  - 80286 is the first member of the family of advanced microprocessors with built-in/on-chip memory management and protection abilities primarily designed for multi-user/multitasking systems
- Available in 8 MHz, 10 MHz & 12.5 MHz clock frequencies

Salient features of 80286
bus and memory sizes cont…

- The 80286 CPU, with its 24-bit address bus is able to address 16MB of physical memory.
  - 1GB of virtual memory for each task

Microprocessor	Data bus width	Address bus width	Memory size
8086	16	20	1M
80186	16	20	1M
80286	**16**	**24**	**16M**

Intel 80286 architecture



Functional Parts

1. Bus Interface unit
2. Instruction unit
3. Execution unit
4. Address unit

Bus Interface Unit

- Performs all memory and I/O read and write operations.
- Take care of communication between CPU and a coprocessor.
- Transmit the physical address over address bus $A_0 - A_{23.}$
- Prefetcher module in the bus unit performs this task of prefetching.
- Bus controller controls the prefetcher module.
- Fetched instructions are arranged in a 6 – byte prefetch queue.

Instruction Unit

- Receive arranged instructions from 6 byte prefetch queue.
- Instruction decoder decodes up to 3 prefetched instruction and are latched them onto a decoded instruction queue.
- Output of the decoding circuit drives a control circuit in the Execution unit.

Execution unit

- EU executes the instructions received from the decoded instruction queue sequentially.
- Contains Register Bank.
- contains one additional special register called **Machine status word (MSW)** register --- lower 4 bits are only used.
- ALU is the heart of execution unit.
- After execution ALU sends the result either over data bus or back to the register bank.

Address Unit

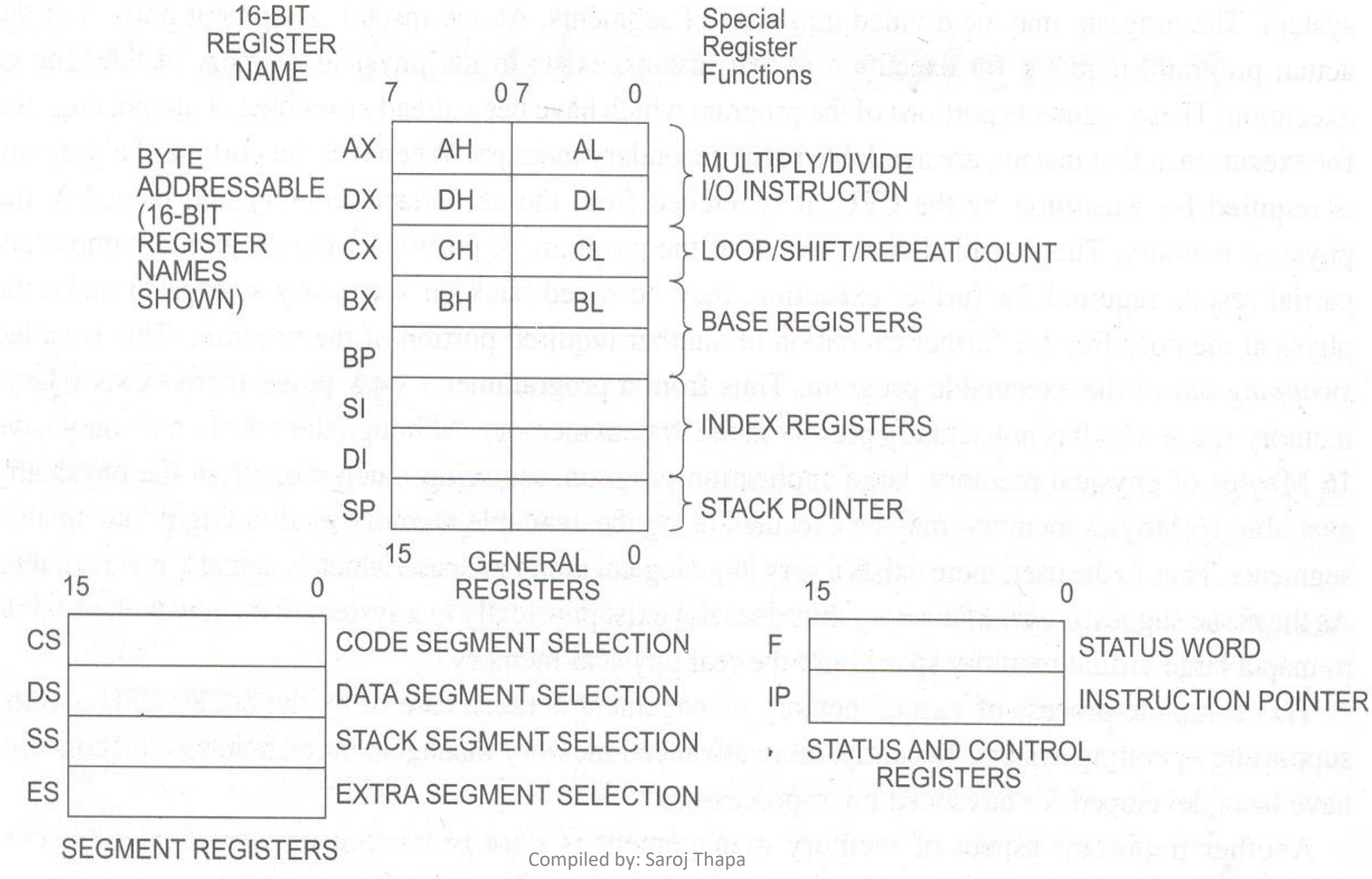
- Calculate the physical addresses of the instruction and data that the CPU want to access
- Address lines derived by this unit may be used to address different peripherals.
- Physical address computed by the address unit is handed over to the BUS unit.

Register organization of 80286

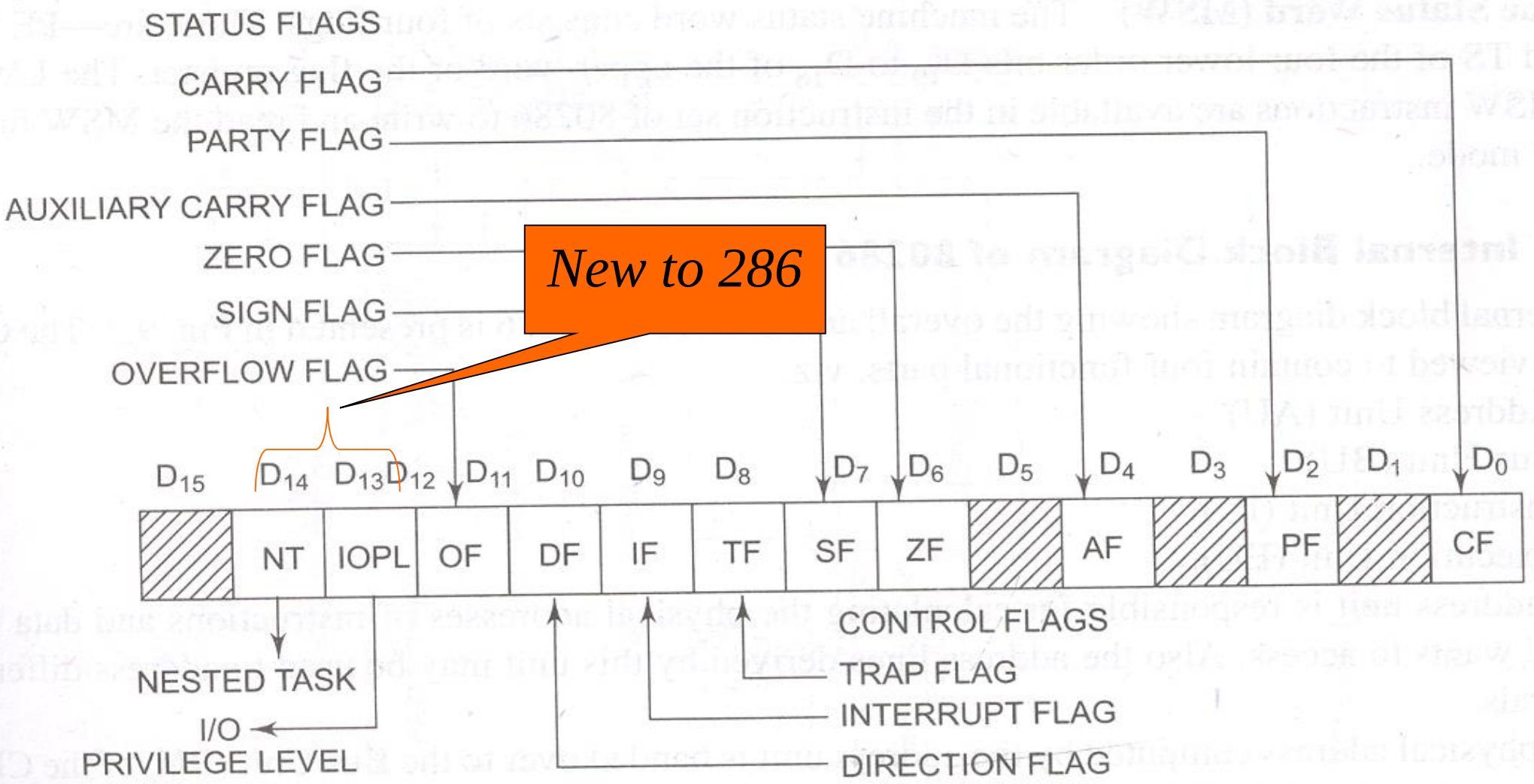
- The 80286 CPU contains the **same set of registers, as in 8086**.
  - Eight 16-bit general purpose registers.
  - Four 16 bit segment registers.
  - One Flag register.
  - One Instruction pointer.

plus

  - one new 16-bit machine status word (MSW) register


16-BIT REGISTER NAME
Special Register Functions
7 0 7 0
BYTE ADDRESSABLE (16-BIT REGISTER NAMES SHOWN)
AX
AH
AL
MULTIPLY/DIVIDE I/O INSTRUCTON
DX
DH
DL
CX
CH
CL
LOOP/SHIFT/REPEAT COUNT
BX
BH
BL
BASE REGISTERS
BP
SI
INDEX REGISTERS
DI
SP
STACK POINTER
15 0
GENERAL REGISTERS
15 0
CS
CODE SEGMENT SELECTION
DS
DATA SEGMENT SELECTION
SS
STACK SEGMENT SELECTION
ES
EXTRA SEGMENT SELECTION
SEGMENT REGISTERS
15 0
F
STATUS WORD
IP
INSTRUCTION POINTER
STATUS AND CONTROL REGISTERS

Flag Register



IOPL – Input Output Privilege Level flags (bit D12 and D13) and Nested Task flag

i. IOPL – I/O Privilege Level flag: 2 –bits are used in protected mode. It holds the privilege level from 0 to 3. ‘0’ assigns to highest privilege whereas ‘3’ assigns to lower privilege level.

ii. NT: Nested Task flag: It is used in protected mode. Bit is set when one task invokes another task.

Addressing Modes

Same as 8086 MPU

Operating modes:

Intel 80286 has 2 operating modes:

Real Address Mode :

- Instruction set is upwardly compatible
- Because of extra pipelining and other circuit level improvements, in real address mode also, the 80286 operates at a much faster rate than 8086, although functionally they work in an identical fashion.
- As in 8086, the physical memory is organized in terms of segments of 64Kbyte maximum size.
- In the real mode the first 1Kbyte of memory starting from address 0000H to 003FFH is reserved for interrupt vector table.
- The addresses from FFFF0H to FFFFFH are reserved for system initialization.
- When the 80286 is reset, it always starts the execution in real address mode.
- In real address mode, it initializes the IP and other registers of 80286.

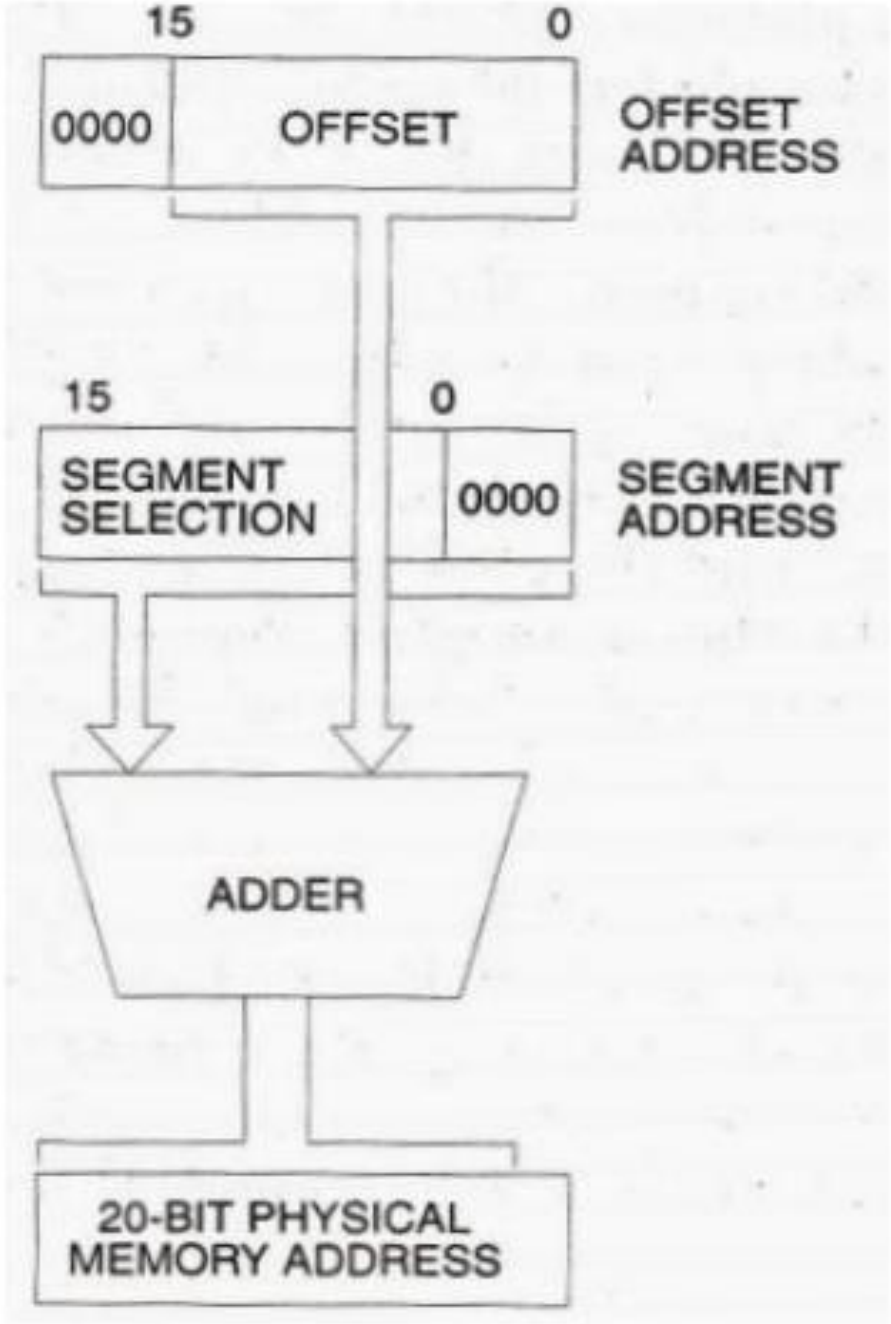


Figure: Real Address Mode Address Calculation

ii. Protected Virtual Address Mode (PVAM)

- 80286 is the first processor to support the concepts of virtual memory and memory management.
- The concept of Virtual Memory is implemented using Physical memory that the CPU can directly access and secondary memory that is used as storage for data and program, which are stored in secondary memory initially.
- The complete virtual memory is mapped on to the 16Mbyte physical memory.
- If a program larger than 16Mbyte is stored on the hard disk and is to be executed, if it is fetched in terms of data or program segments of less than 16Mbyte in size into the program memory by swapping sequentially as per sequence of execution.
- The 80286 is able to address 1 GB (230 bytes) of virtual memory.
- 80286 uses the 16-bit content of a segment register as a selector to address a descriptor stored in the physical memory.
- The descriptor is a block of contiguous memory locations containing information of a segment, like segment base address, segment limit, segment type, privilege level, segment availability in physical memory descriptor type and segment.
- Hardware reset is the only way to come out of protected mode

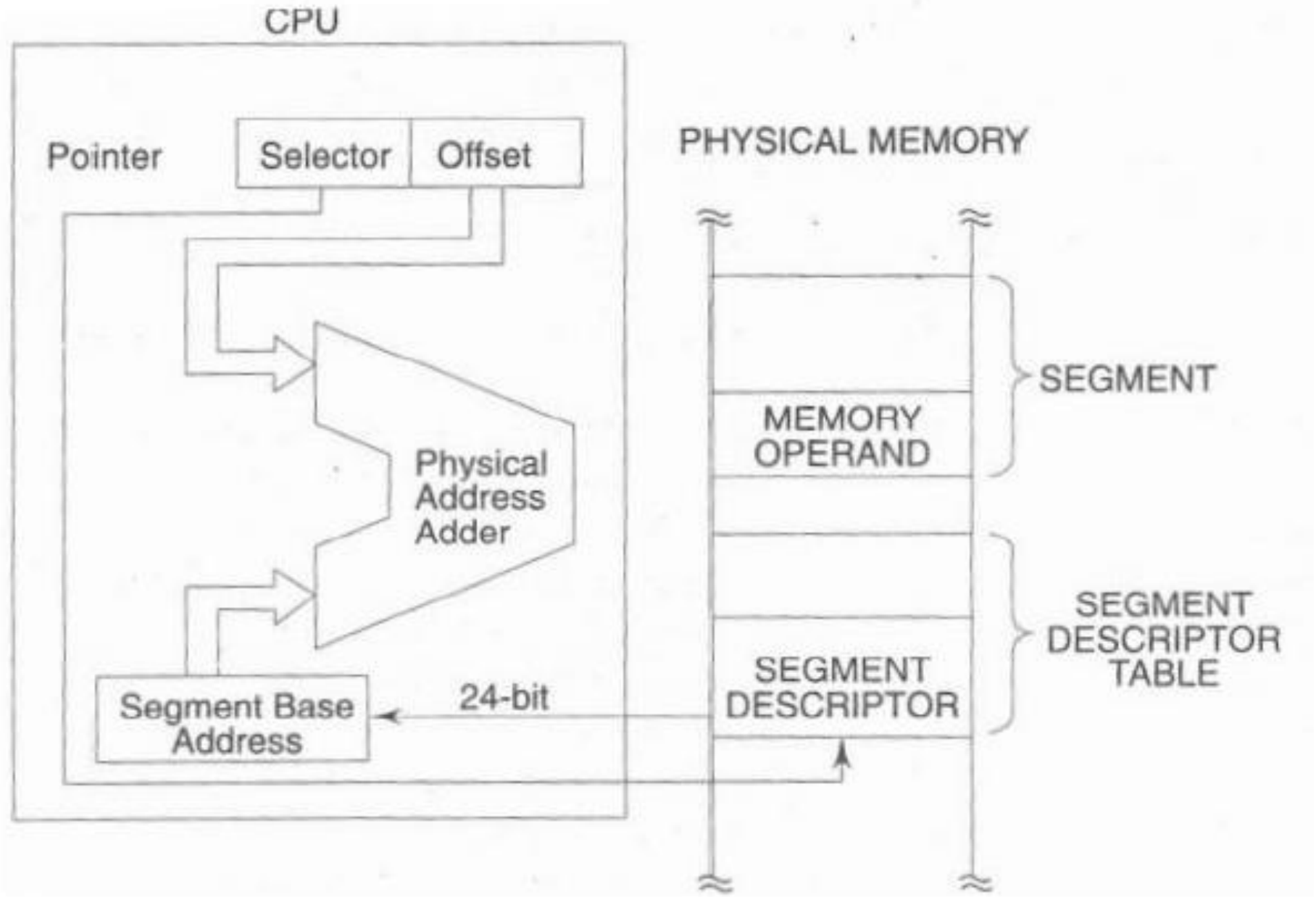


Figure: Physical Address Calculation in PVAM

Cont..

- The segment register now contains a selector
- Selector selects a descriptor from a descriptor table
- The descriptor describes the memory segment's location
- Two descriptor table
  - Global Descriptor Table (GDT)
  - Local Descriptor Table (LDT

PRIVILEGE Levels

- The 80286 supports a four level hierarchical privilege mechanism to control the access to descriptors(??) and hence to the corresponding segments.
- Each task assigned a privilege level, which indicates the priority or privilege of that task.
- It can only changed by transferring the control, using gate descriptors, to a new segment.
- A task executing at level 0, the most privileged level, can access all the data segment defined in GDT and LDT of the task.
- A task executing at level 3, the least privileged level, will have the most limited access to data and other descriptors.
- The use of rings allows for system software to restrict tasks from accessing data.
- In most environments, the operating system and some device drivers run in ring 0 and applications run in ring 3.

Privilege Level cont..

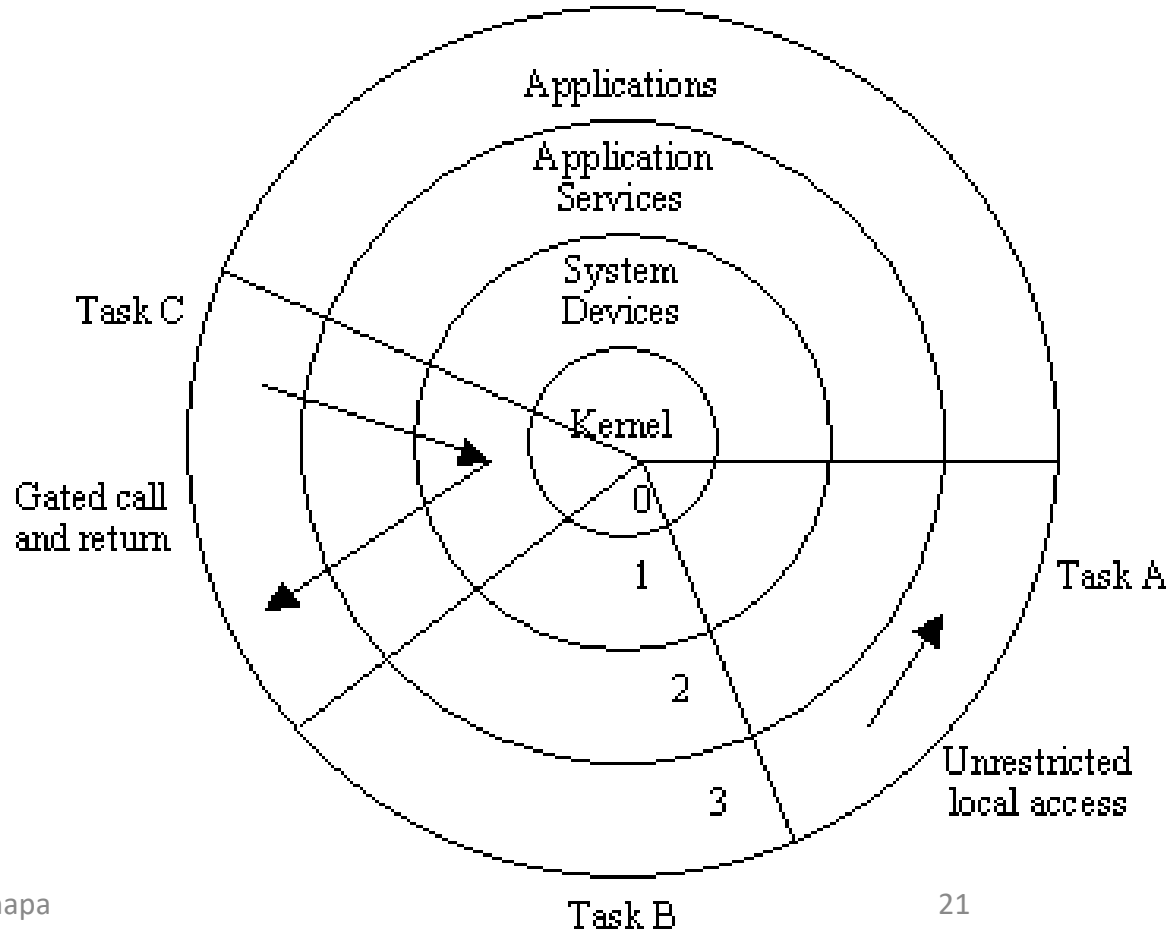
There are four types of privilege levels

00 - kernel level (highest privilege level)

01 - OS services

10 - OS extensions

11 - Applications (lowest privilege level)



A glimpse on Descriptor

- Descriptor is a identifier of a program segment or page.
- A segment cannot be accessed, if its descriptor does not exist in either LDT or GDT(????).
- Set of descriptor (descriptor table) arranged in a proper sequence describes the complete program.
- The descriptor is a block of contiguous memory location containing information of a segment, like

i. Segment base address

ii. Segment limit

iii. Segment type

iv. Privilege level – prevents unauthorized access

v. Segment availability in physical memory

vi. Descriptor type

vii. Segment use by another task

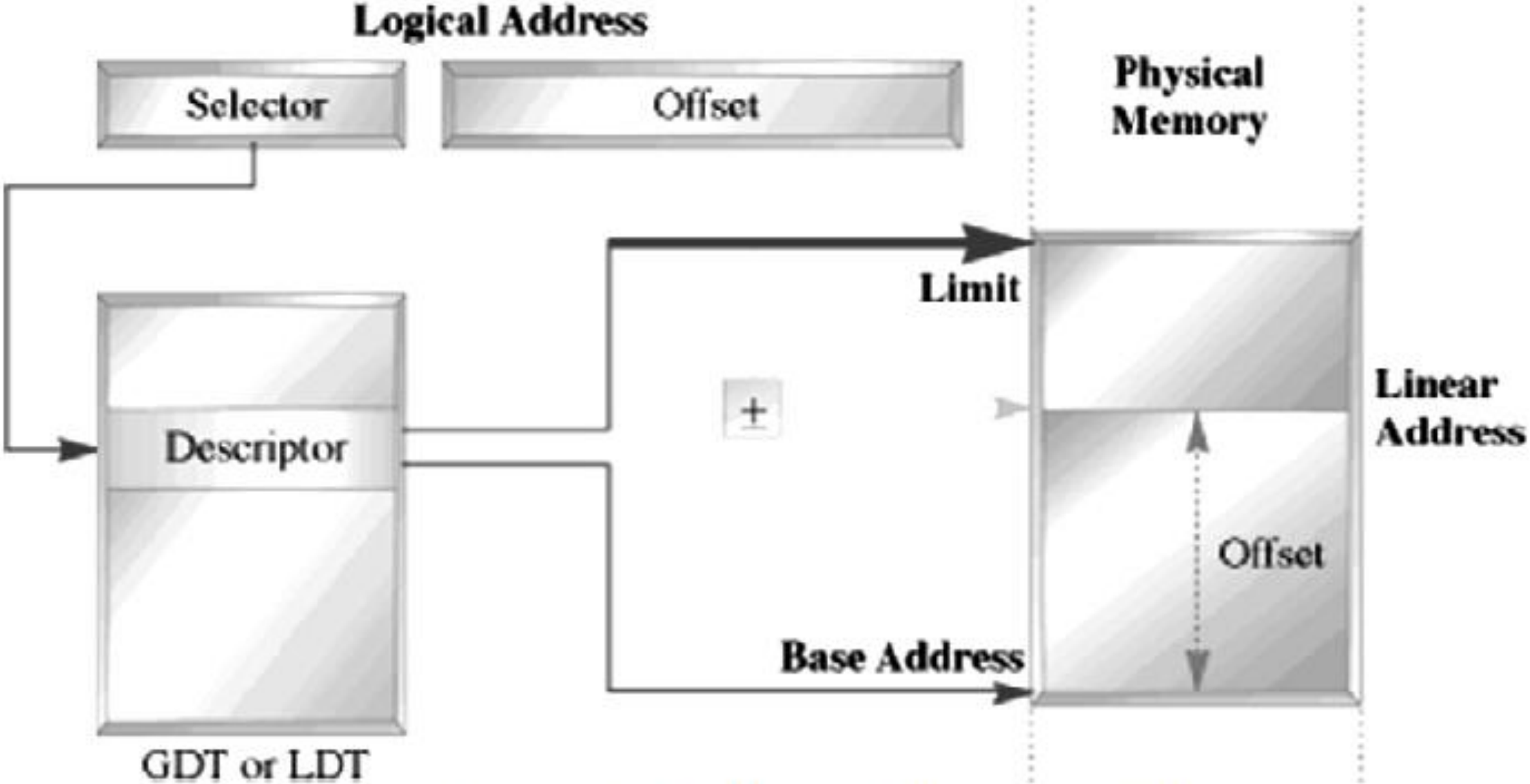


Figure: Protected Mode Addressing with Descriptor Table

Global Descriptor Table (GDT):

- The 80286 has a single Global Descriptor Table (GDT) which is shared between all tasks and addresses up to 512MB of the virtual address space.
- The Global Descriptor Table or GDT is a data structure used by Intel x86-family processors starting with the 80286 in order to define the characteristics of the various memory areas used during program execution, including the base address, the size and access privileges like execute- ability and write-ability.

Local Descriptor Table (LDT):

- Each task will have its own Local Descriptor Table (LDT) which is a private 512MB of address space.
- LDT is essential to implement separate address spaces for multiple processes.
- The operating system will switch the current LDT when scheduling a new process, using the LDT machine instruction.

End of 80286