



## Processore Intel 80386

---



## Nuove caratteristiche

---

- Set di registri a 32 bit
- Bus dati a 32 bit
- Bus indirizzi a 32 bit
- Nuove istruzioni
- Nuovi modi di indirizzamento
- Livelli di privilegio (come il 286)
- Segmentazione e paginazione

## Modi operativi

---

- Il processore 80386 è in grado di operare in tre modalità differenti:
  - Real Address Mode (modalità reale in cui si emula un 8086)
  - Virtual 8086 mode (modalità VM86)
  - Protected Virtual Address Mode (PVAM)

## Modalità VM86

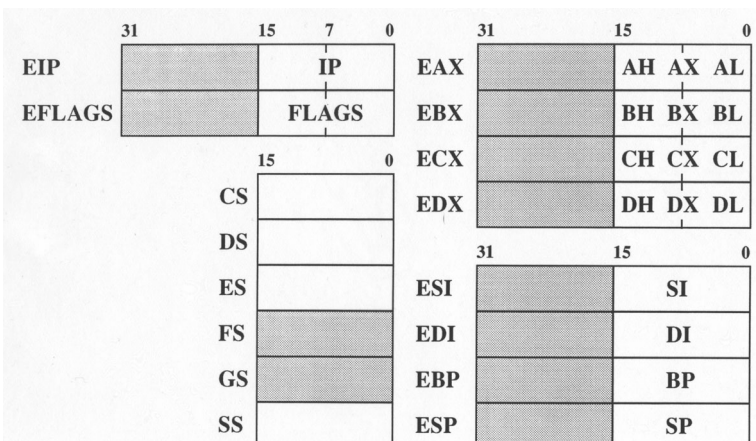
---

- È una modalità selezionabile per ogni singolo task
- Un task di tipo VM86 si, dal punto di vista dell'utente, comporta come un processore 8086:
  - Spazio di indirizzamento ridotto a 20 bit
  - Non esistono livelli di protezione
  - Meccanismo di segmentazione analogo a quello dell'8086

## Modalità VM86

- Un task VM86 si comporta come un 8086 "virtuale":
  - È ancora attiva la paginazione (e quindi la memoria virtuale)
  - Opera a livello di privilegio 3 e non può eseguire operazioni privilegiate
  - Le istruzioni di I/o e le richieste di interrupt vengono intercettate e gestite da un modulo del kernel (Virtual Machine Monitor)
- Su un processore 80386 è possibile emulare simultaneamente più processori virtuali 8086 in modo indipendente

## Registri general purpose



## Modi di indirizzamento

- Il processore 80386 fornisce un insieme di modi di indirizzamento simile, ma più sofisticato, dell'8086:
  - È possibile scalare il registro indice per un fattore pari a 2, 4 o 8 (oltre che a 1)
  - È possibile utilizzare qualsiasi registro come base
  - È possibile utilizzare qualsiasi registro (tranne ESP) come indice

## Modi di indirizzamento

<i>Modo</i>	<i>Esempio</i>
Costante immediata	<code>MOV EAX, 12345678</code>
Registro immediato	<code>MOV EAX, ECX</code>
Diretto (solo offset)	<code>MOV EAX, [12345678]</code>
Indiretto tramite registro	<code>MOV EAX, [ECX]</code>
Base/Indice + Offset	<code>MOV EAX, [ECX]+1234</code>
Base + Indice + Offset	<code>MOV EAX, [ECX][EDX]+1234</code>
Indice * Scala + Offset	<code>MOV EAX, [ESI*4]+1234</code>
Base + (Indice * Scala)	<code>MOV EAX, [EDX][ECX*8]</code>
Base + (Indice * Scala) + Offset	<code>MOV EAX, [EBX][EDI*2]+1234</code>

## Traduzione degli indirizzi

- Il processore 80386 dispone di una Memory Management Unit (MMU) integrata sul chip in grado di gestire simultaneamente 2 meccanismi di traduzione:
  - Segmentazione (traduzione da indirizzo logico a lineare; simile a quella realizzata dal processore 80286)
  - Paginazione (traduzione da indirizzo lineare a indirizzo fisico; può essere disabilitata)

## Traduzione degli indirizzi

descrittore (16 bit)  
+  
offset (16 o 32 bit)

**Indirizzo logico**

**Segmentazione**

32 bit

**Indirizzo lineare**

**Paginazione**  
(opzionale)

32 bit

**Indirizzo fisico**

## Multitasking

---

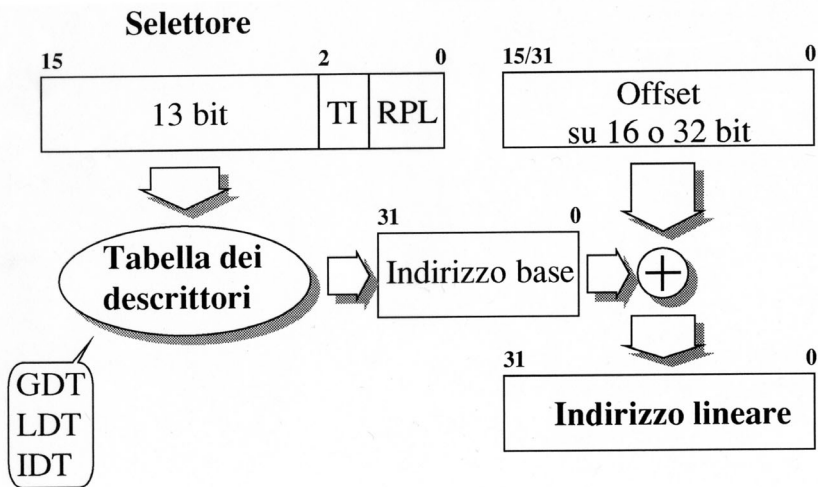
- Il processore 80386 fornisce un supporto alla multiprogrammazione:
  - È in grado di supportare il context-switching
  - Riconosce diversi livelli di privilegio
  - Ogni task ha il suo spazio di indirizzamento protetto

## Segmentazione

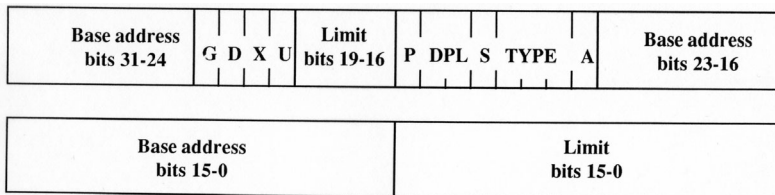
---

- Il meccanismo di segmentazione del 386 è un sovrainsieme di quello del 286:
  - Permette di definire segmenti di lunghezza variabile (da 1 byte a 4 GB) e con indirizzo base allineato arbitrariamente
  - Forza i controlli di accesso relativi a modo e privilegio sui segmenti

# Segmentazione: meccanismo di traduzione



# Segmentazione: formato dei descrittori



Tipi di segmento (campo TYPE):

- 000 Data, read only
- 001 Data, read/write
- 010 Stack, read only
- 011 Stack, read/write
- 100 Code, execute only
- 101 Code, execute/read
- 110 Code, execute only, conforming
- 111 Code, execute/read, conforming

## Descrittori: significato dei bit

- A: accessed. Settato dal 386 quanto fa accesso ai dati contenuti nel segmento
- Type: identifica il tipo di segmento
- S: System. Se uguale a 0 identifica un descrittore di segmento uguale a 0, altrimenti come non di sistema (codice, dati o stack)
- DPL livello di privilegio del segmento definito dal descrittore
- P: present. Se a 0 il segmento corrispondente non è presente in memoria fisica

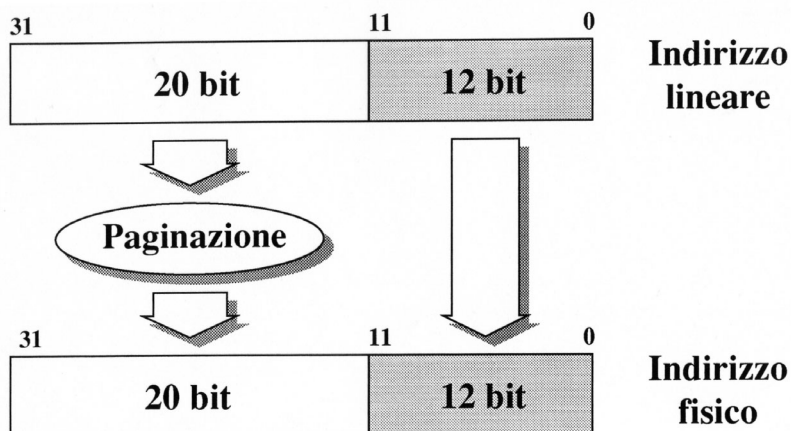
## Descrittori: significato dei bit

- U: user. Ignorato dal 386 e può essere usato dai programmatori
- X: reserved. Riservato
- D: default size. Se zero indica una dimensione degli operandi pari a 16 bit, altrimenti la dimensione di default è di 32 bit
- G: granularity. Se uguale a 0 indica che la lunghezza del segmento specificato dal descrittore è espressa in byte, altrimenti in unità da 4KB

# Paginazione

- È un processo di traduzione degli indirizzi
- Può essere usata in concomitanza con la segmentazione (segmentazione paginata)
- Può essere disabilitata
- Permette di minimizzare la frammentazione della memoria
- Permette di realizzare la paginazione "on demand"

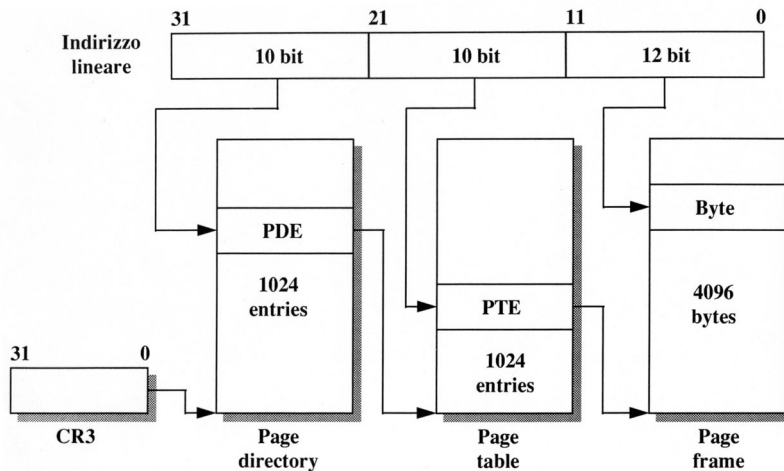
## Paginazione: meccanismo di traduzione



# Paginazione: meccanismo di traduzione

- I 32 bit dell'indirizzo lineare sono divisi in tre parti:
  - I 12 bit meno significativi costituiscono l'offset all'interno della pagina selezionata (che è lunga 4 KB)
  - I 10 bit servono per trovare la pagina voluta all'interno della tabella delle pagine del task (page table)
  - I 10 bit più significativi servono a trovare la tabella delle pagine del task all'interno di una tabella denominata page directory
- Le due tabelle contengono ciascuna 1024 descrittori di 32 bit
- Una tabella unica sarebbe troppo grande!
- L'indirizzo di partenza della page directory è contenuto nel registro special purpose CR3

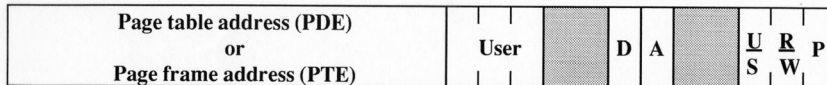
# Paginazione: meccanismo di traduzione



# Paginazione: formato dei descrittori

**La Page Directory e le Page Table hanno descrittori il cui formato è simile:**

- PDE: Page Directory Entry;
- PTE: Page Table Entry;



# Descrittori: significato dei bit

- Page Table Address: indirizzo fisico base della page table relativa
- Page Frame Address: indirizzo fisico dalla pagina relativa
- User: bit riservati al programmatore
- P: present. Indica se la PTE o la PDE relativa sono presenti in memoria
- D: dirty. Presente solo nella PTE e settato quando viene fatta una scrittura nella pagina associata
- A: accessed. Settata quando il descrittore viene utilizzato nella traduzione di un indirizzo
- U/S: user/supervisor. Se uguale a 0 i task a livello di privilegio 3 non possono fare accesso alla pagina, altrimenti tutti possono accedervi
- R/W: read/write. Se uguale a 0 i task a livello di privilegio 3 non possono fare scritture nella pagina associata

## Translation Lookaside buffer: TLB

- Per velocizzare le operazioni di traduzione da indirizzo lineare a indirizzo fisico il 386 mantiene una memoria cache (TLB) che memorizza le traduzioni più recenti
- Prima di effettuare un'operazione di traduzione viene cercata una corrispondenza nel TLB
- Questo meccanismo permette di ridurre notevolmente gli accessi alla memoria
- Il TLB può memorizzare 32 descrittori di pagina (significa che  $32 * 4KB = 128 KB$  non necessitano traduzione)
- Le simulazioni mostrano che il TLB "copre" circa il 98% delle traduzioni

## Translation Lookaside buffer: TLB

- Il TLB è costituito da una memoria set-associativa a 4 vie con 32 entry
- Ogni entry contiene l'indirizzo lineare su 20 bit, l'indirizzo fisico su 20 bit e 4 bit di tag:
  - V: valid. Dice se la linea di cache è valida
  - D: dirty. Dice se la pagina relativa è stata scritta
  - U: user. Dice se la pagina è accessibile a codice che gira a livello di privilegio 3
  - W: writeable. Dice se la pagina relativa può essere scritta



## Paginazione on demand

---

- I bit P, D e A sono usati per realizzare un meccanismo di paginazione su domanda.
- Quando il processore genera un indirizzo relativo ad una pagina non presente in memoria viene generata una trap di page fault:
  - Viene invocata una procedura per caricare la pagina in memoria
- Se la memoria fisica è completamente occupata un meccanismo di page swap libera "un posto":
  - I bit D e A permettono di realizzare meccanismi di scelta della pagina da rimpiazzare e di capire se la pagina rimpiazzata deve essere riscritta su disco