

# Cenni su Librerie

Prof. Vittorio Ghini, Appunti delle lezioni di Sistemi Operativi,  
Corso di Laurea in Ingegneria e Scienze Informatiche, Università di Bologna

Le librerie sono dei file che contengono le implementazioni, in codice macchina, di alcune funzioni. Possono implementare funzioni di base messe a disposizione dal sistema operativo oppure funzioni definite da utenti.

Solitamente le librerie sono mantenute su disco in directory predefinite, in dei file il cui nome comincia per **lib**. L'estensione del nome del file che contiene la libreria è diverso a seconda che la libreria sia statica (.a) o condivisa (.so).

Escludendo il "lib" iniziale ed escludendo l'estensione, ciò che resta del nome del file della libreria rappresenta il **nome ufficiale** della libreria. Tale nome ufficiale è quello che si usa per indicare al linker quali librerie dobbiamo linkare, con l'opzione **-Inomelibreria**

Ad esempio, la libreria matematica che fornisce cos sin etc etc si chiama **m**, è contenuta nei file `/usr/lib/libm.a` (versione statica, se esiste) e `/lib/x86_64-linux-gnu/libm.so.6` (versione condivisa) e si passa al linker specificando il flag **-lm**

Le librerie si dividono in 2 categorie:

- librerie statiche (**static library**),
- librerie condivise o linkate dinamicamente (impropriamente, dinamiche) (**shared library** o **dynamically linked library**).

Le due categorie di librerie si distinguono in funzione di come vengono collegate all'eseguibile che le deve utilizzare. Vanno distinti due momenti:

- link-time (in cui si genera l'eseguibile, collegando le librerie ed i diversi moduli oggetto)
- run-time (il momento in cui si esegue l'eseguibile).

## Librerie Statiche

A link-time le librerie statiche sono fisicamente accorpate ai moduli e inserite assieme a queste nell'eseguibile generato. Il linker deve sapere dove cercare su disco le librerie statiche per copiarne il contenuto e inserirlo nell'eseguibile. Quindi l'eseguibile conterrà le librerie statiche. Da ciò deriva che a run-time l'eseguibile caricato in memoria avrà da subito in memoria pronto per l'esecuzione anche il codice macchina delle librerie.

Generalmente il linker cerca le librerie nella directory `/usr/lib`, ma si può ordinare al linker di cercare, a link-time, le librerie statiche anche in una o più directory diverse specificandole al linker con uno o più parametri **-Llinktimepath** (ad esempio `-L/home/studente/lib -Lnuovo/percorso/assoluto/fino/alla/directory/delle/librerie`)

## Librerie Condivise.

A link-time le librerie condivise NON sono fisicamente accorpate ai moduli e NON sono inserite nell'eseguibile generato. Invece, per ciascuna chiamata ad una funzione della libreria condivisa, il linker inserisce nell'eseguibile una porzione di codice macchina (stub) e la posizione a run-time su disco della libreria.

A run-time, al momento dell'esecuzione della chiamata a funzione, lo stub cercherà la libreria condivisa sul disco del computer in cui avviene l'esecuzione del programma, la caricherà in memoria rendendola disponibile per l'esecuzione e poi effettuerà la chiamata alla funzione saltando nel codice della libreria appena caricata in memoria.

Se le librerie non sono nelle directory predefinite del sistema, il linker deve perciò sapere due cose:  
1) dove si trova a link-time la libreria condivisa,

## 2) dove si troverà a run-time la libreria su disco,

Approfondiamo le motivazioni delle due informazioni necessarie al linker per linkare librerie caricate dinamicamente:

1) Il linker deve sapere dove si trova a link-time la libreria condivisa, poiché deve i) verificare se questa libreria fornisce veramente la funzione richiesta e ii) copiare dalla libreria il solo stub che effettua il caricamento. Con l'opzione **-Llinktimepath** diciamo al linker dove sono a link-time le librerie condivise.

2) Il linker deve sapere dove si troverà a run-time la libreria su disco, poiché deve inserire questa posizione nel codice assieme allo stub. Con l'opzione **-Wl,-rpath,runtimepath** diciamo al linker dove saranno le librerie condivise a run-time.

Ad esempio, se devo generare un eseguibile prog.exe, linkando un modulo oggetto prog.o che necessita della libreria **libmia.so** la quale si trova, a link-time in /home/studente/temp, e a run-time si troverà nella directory /home/studente/lib, allora devo linkare l'eseguibile eseguendo il comando:

```
gcc altriflag -o prog.exe prog.o -L/home/studente/temp -Wl,-rpath,/home/studente/lib -lmia
```

## Utilities per le librerie

Le librerie ed i file binari eseguibili sono dei file strutturati secondo un formato standard, in ambito Linux il più usato è il formato elf. Esistono alcune utilities che permettono di verificare il contenuto delle librerie.

Per sapere di quale librerie condivise necessita un file binario eseguibile o una libreria, lanciare:

**ldd nome\_eseguibile** (oppure **ldd percorsolibreria**)

Ad esempio, vediamo l'output ottenuto eseguendo il seguente comando:

**ldd prog.exe**

```
linux-vdso.so.1 => (0x00007ffc844d7000)
libmia.so => /home/studente/lib/libmia.so (0x00007f4504dd3000)
libc.so.6 => /lib/x86_64-linux-gnu/libc.so.6 (0x00007f45049f7000)
/lib64/ld-linux-x86-64.so.2 (0x0000558aeabc0000)
```

Per sapere quali informazioni di linking dinamico sono state inserite in una libreria condivisa oppure in un eseguibile, si può usare l'eseguibile readelf, ad esempio lanciando il comando:

**readelf -d percorsolibreria** (oppure **percorsi eseguibile**)

Ad esempio, vediamo l'output ottenuto eseguendo il seguente comando:

**readelf -d prog.exe** (analogamente **readelf -d libmia.so**)

Dynamic section at offset 0xe08 contains 26 entries:

Tag	Type	Name/Value
0x0000000000000001	(NEEDED)	Shared library: [ <b>libmia.so</b> ]
0x0000000000000001	(NEEDED)	Shared library: [libc.so.6]
0x000000000000000f	(RPATH)	Library rpath: [/home/studente/lib]
0x000000000000000c	(INIT)	0x400788

Anche readelf riconosce le dipendenze annidate, e visualizza anche le librerie utilizzate indirettamente, cioè quelle usate dalle librerie direttamente usate nell'eseguibile o libreria.

Aggiungere due parole sull'utility **file**

```
file prog.exe
prog.exe: ELF 64-bit LSB executable, x86-64, version 1 (SYSV), dynamically
linked, interpreter /lib64/ld-linux-x86-64.so.2, for GNU/Linux 2.6.32,
BuildID[sha1]=df0c3fc103bc4c91e3709c53fa35ff45cb5b8e97, not stripped

file libmia.so
libmia.so: ELF 64-bit LSB shared object, x86-64, version 1 (SYSV), dynamically
linked, BuildID[sha1]=2a187da98f0a66cb254f340c7249301bd93a7b40, not
stripped

file mia.o
mia.o: ELF 64-bit LSB relocatable, x86-64, version 1 (SYSV), not stripped

file mia.c
mia.c: C source, ASCII text

file mia.h
mia.h: C source, ASCII text
```

**AGGIUNGERE spiegazione su utility nm per visualizzare le tabelle dei simboli dei file oggetto, librerie ed eseguibili.**

Quando faccio il linking dei moduli oggetto per generare un eseguibile, il linker cerca di utilizzare PRIMA le librerie CONDIVISE, e solo se non le trova, usa le librerie statiche.

Generalmente il linker cerca le librerie nella directory `/usr/lib`, ma si puo' ordinargli di cercarle in una directory diversa specificandola al linker con il parametro `-L/nuovo/percorso`

Se voglio che il linker usi solo le librerie statiche devo specificare al gcc il flag **-static**

Domanda da approfondire: come posso dire al linker di usare solo le versioni condivise, e se non ci sono di dare un errore?

---

Come fare a sapere di quali librerie condivise un eseguibile a.out ha bisogno?

Si utilizza l'eseguibile **ldd** (List Dynamic Dependencies)

```
ldd /usr/bin/lynx
    libncurses.so.1 => /usr/lib/libncurses.so.1.9.6
    libc.so.5 => /lib/libc.so.5.2.18
```

Domanda da approfondire: ldd riconosce le dipendenze annidate? Ovvero, se a.out usa la libreria condivisa libncurses.so e la libreria libncurses utilizza a sua volta la libreria condivisa interna.so, allora ldd ci dice che a.out utilizza la libreria interna.so? SI, l'ho verificato !

---

l'eseguibile **nm** elenca tutti i simboli per i quali esistono dei riferimenti nella libreria che viene passata come argomento:

```
nm libc.so.5
00010fe8 U getname
00010fe8 W tcgetattr
00068718 T tcgetpgrp
00010fe8 T __tcgetattr
```

<b>U</b> getname	significa che il simbolo getname e' usato ma NON definito (unknown) ovvero è contenuto in una diversa libreria.
<b>T</b> tcgetpgrp	significa che il simbolo tcgetpgrp e' definito all'interno della libreria (il modo normale).
<b>W</b> tcgetattr	significa che il simbolo tcgetattr e' definito all'interno della libreria, ma in una forma detta weak (W) ovvero in modo tale da poter essere sostituito da un'altra definizione in una libreria diversa. (Domanda da approfondire: anche nella stessa libreria? Credo di sì).

A	The symbol's value is absolute, and will not be changed by further linking.
B	Un-initialized data section
D	Initialized data section
T	Normal code section
U	Undefined symbol used but not defined. Dependency on another library.
W	Doubly defined symbol. If found, allow definition in another library to resolve dependenc

l'eseguibile ***nm -D***

elenca i simboli per i quali esistono dei riferimenti nella libreria che viene passata come argomento:

---

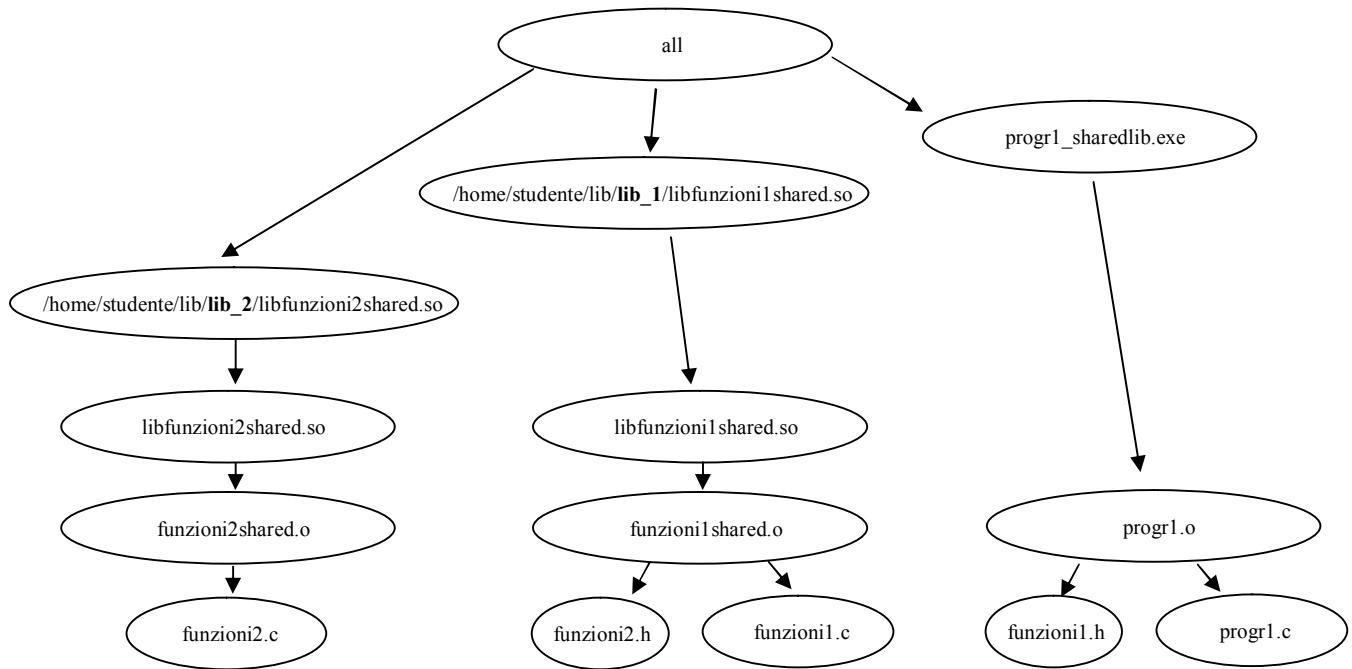
per elencare tutte le librerie dinamiche presenti in memoria, si puo' utilizzare il comando

**lsof** listing open files  
specificando alcuni parametri

```
lsof | grep mem | grep "\.so" | awk '{print $9}' | sort | uniq
```

## ESEMPIO DI LIBRERIE ANNIDATE

### albero delle dipendenze



# **Introduzione ai Sistemi Operativi**

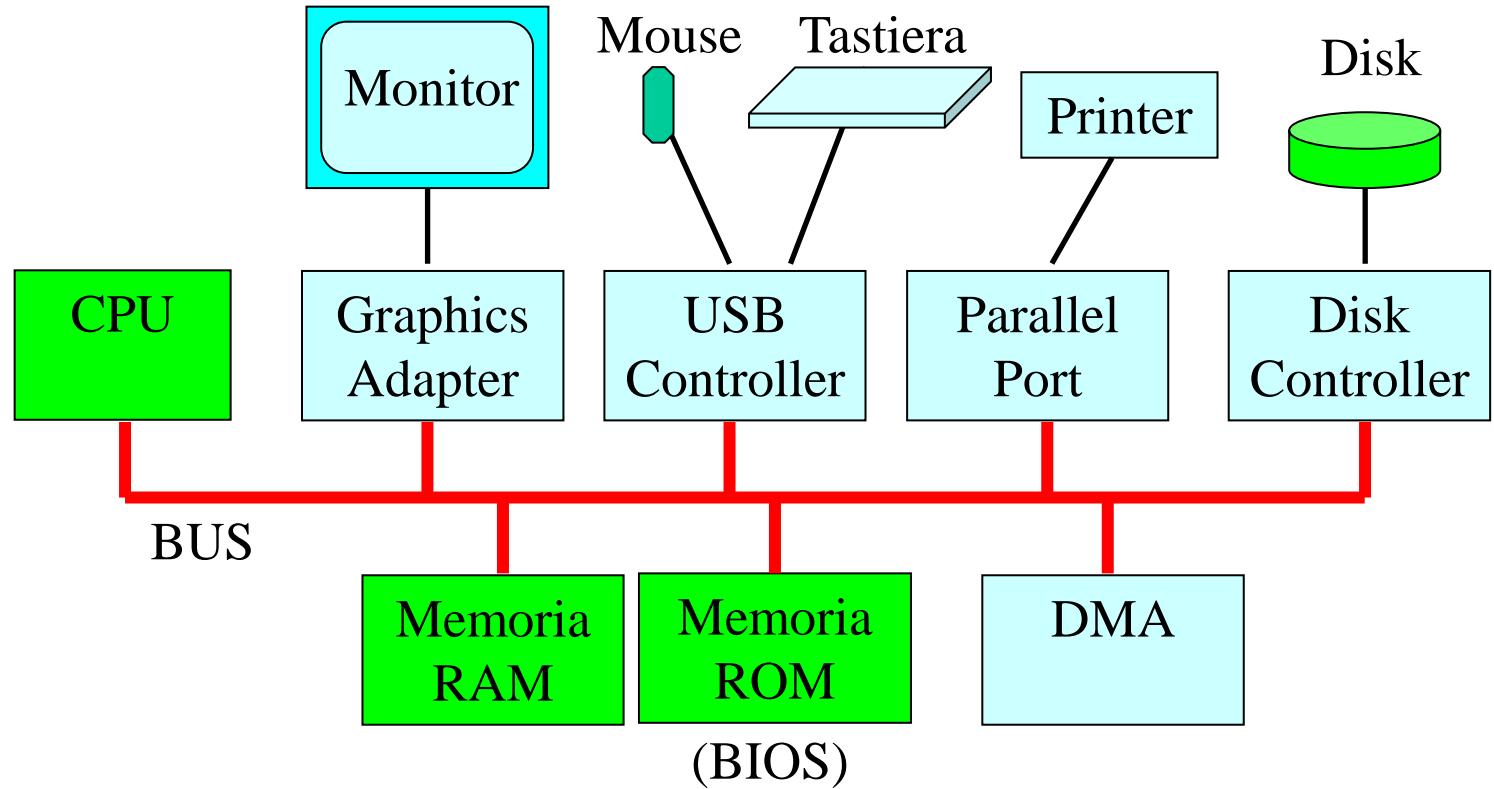
**Scopo di questa parte del corso e':**

- **introdurre i concetti principali dei sistemi operativi,**
- **identificare i requisiti hardware necessari alla gestione dei processi e del sistema operativo,**
- **individuare le interfacce software su cui i sistemi operativi si appoggiano,**
- **individuare i principali servizi forniti dal sistema operativo,**
- **individuare le interfacce software che i sistemi operativi forniscono ai livelli superiori.**

**Questa parte del corso si basa sul capitolo 1 del libro di testo “Sistemi Operativi” di A. Silberschatz, nona edizione.**

**Le presenti slide hanno il solo scopo di rendere più agevole seguire le lezioni.**

# Hardware di un Computer



**CPU** esegue istruzioni, effettua calcoli, controlla input/output, coordina spostam. dati.

**BUS** trasferisce i dati tra la memoria e gli altri dispositivi.

**Memoria RAM** (volatile) mantiene programmi (seq. di istruzioni) quando devono essere eseguiti, e i dati che i programmi usano, ma solo finché il computer è acceso.

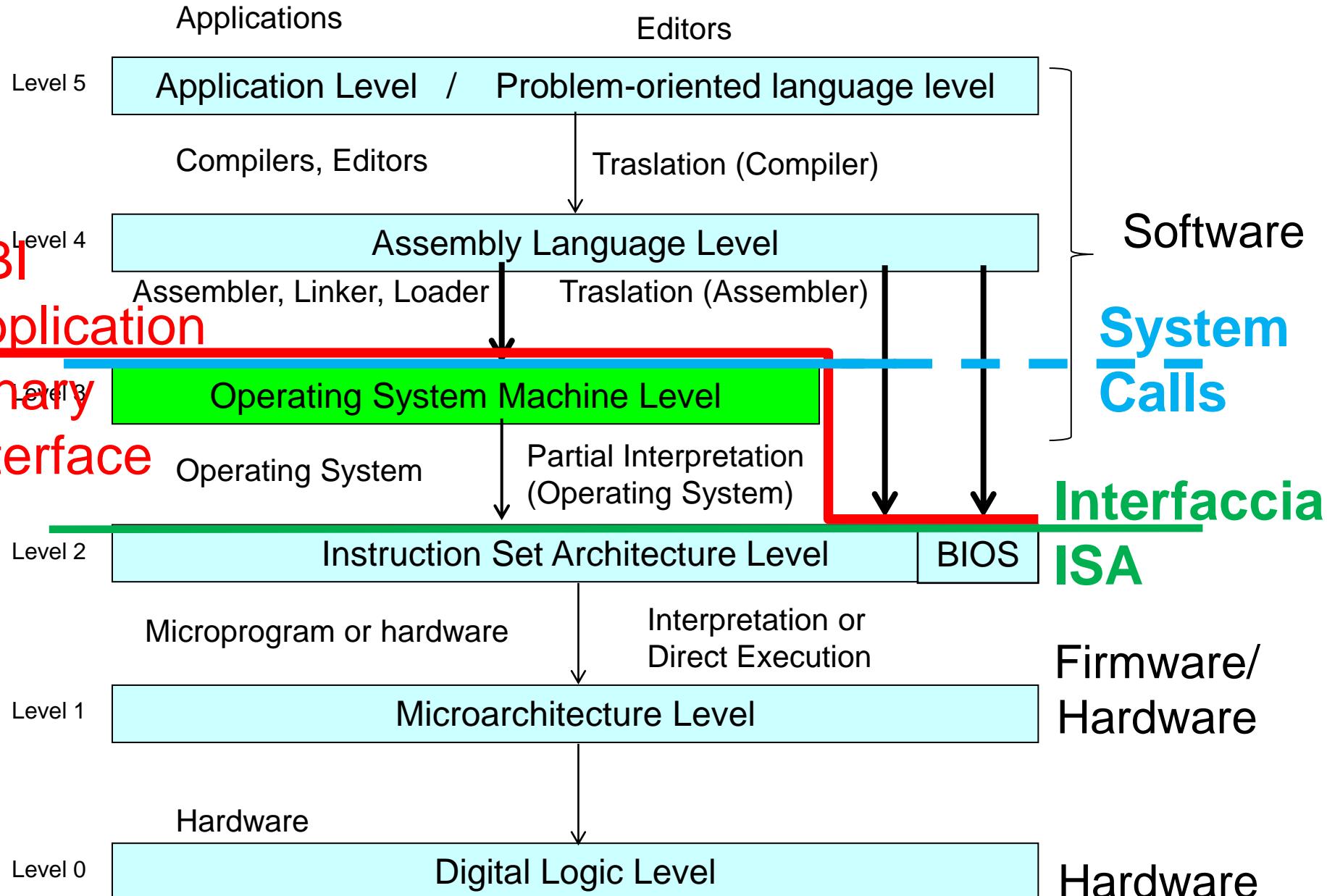
**Memoria ROM** (permanente) contiene il BIOS, le istruzioni per fornire i servizi base, usate dalla CPU anche nel momento dell'accensione del computer (il BOOT).

**Dischi** mantengono enormi quantità di programmi e dati, anche dopo lo spegnimento del computer.

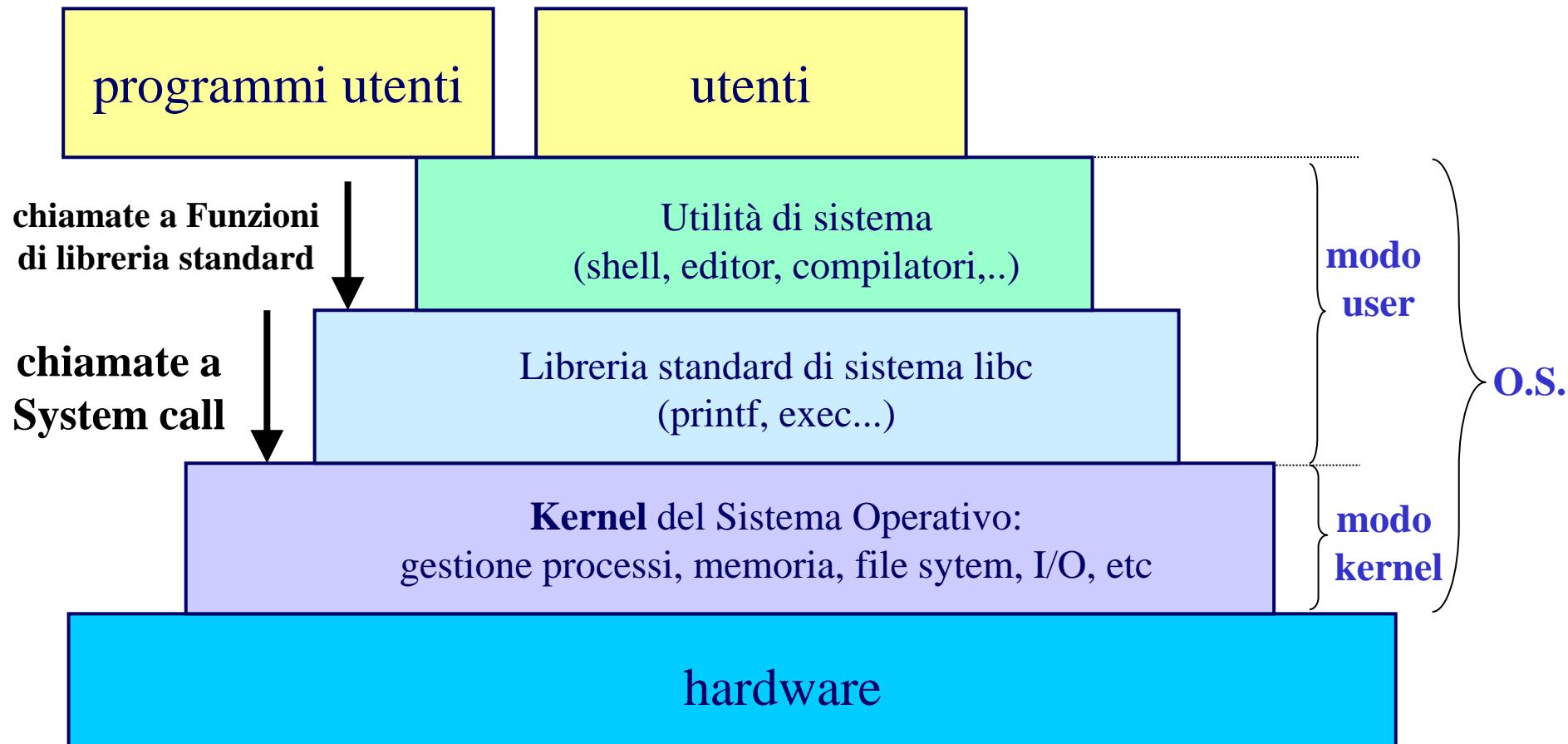
Sono inoltre presenti alcune periferiche di **I/O** (Input/Output).

# Interfacce dei servizi esposte alle applicazioni

ABI Application Binary Interface



# Interazioni con il Sistema Operativo



Il sistema operativo mette a disposizione diversi servizi:

## Gestione della Protezione:

- protezione della CPU - sfrutta la capacità della CPU di operare in due diverse modalità:
  - **modalità kernel**, che permette di utilizzare tutte le istruzioni ISA, tutti gli indirizzi di memoria, tutti i registri, tutte le periferiche.
  - **modalità utente**, che limita le istruzioni eseguibili, l'accesso alla memoria ai registri e alle periferiche.
- protezione della Memoria.

## Gestione della CPU:

- scheduling (quale processo/task deve usare la CPU e per quanto tempo?)

## Gestione della Memoria:

- Indirizzamento, Segmentazione, Protezione, Memoria Virtuale, Paging.

## Gestione dell' Input/Output:

- Periferiche I/O (tastiera, video, rete, dischi), Storage (organizzazione del filesystem).

## Chiamate di Sistema (System Calls), Librerie di sistema, programmi di utilità:

- Servizi messi a disposizione in diverse modalità. Le system call sono disponibili mediante chiamate ad interrupt effettuabili in assembly.

# Protezione hardware: Modi di esecuzione delle CPU

( es: Instruction Set Architecture of IA-32 - Privilege Levels (Rings) )

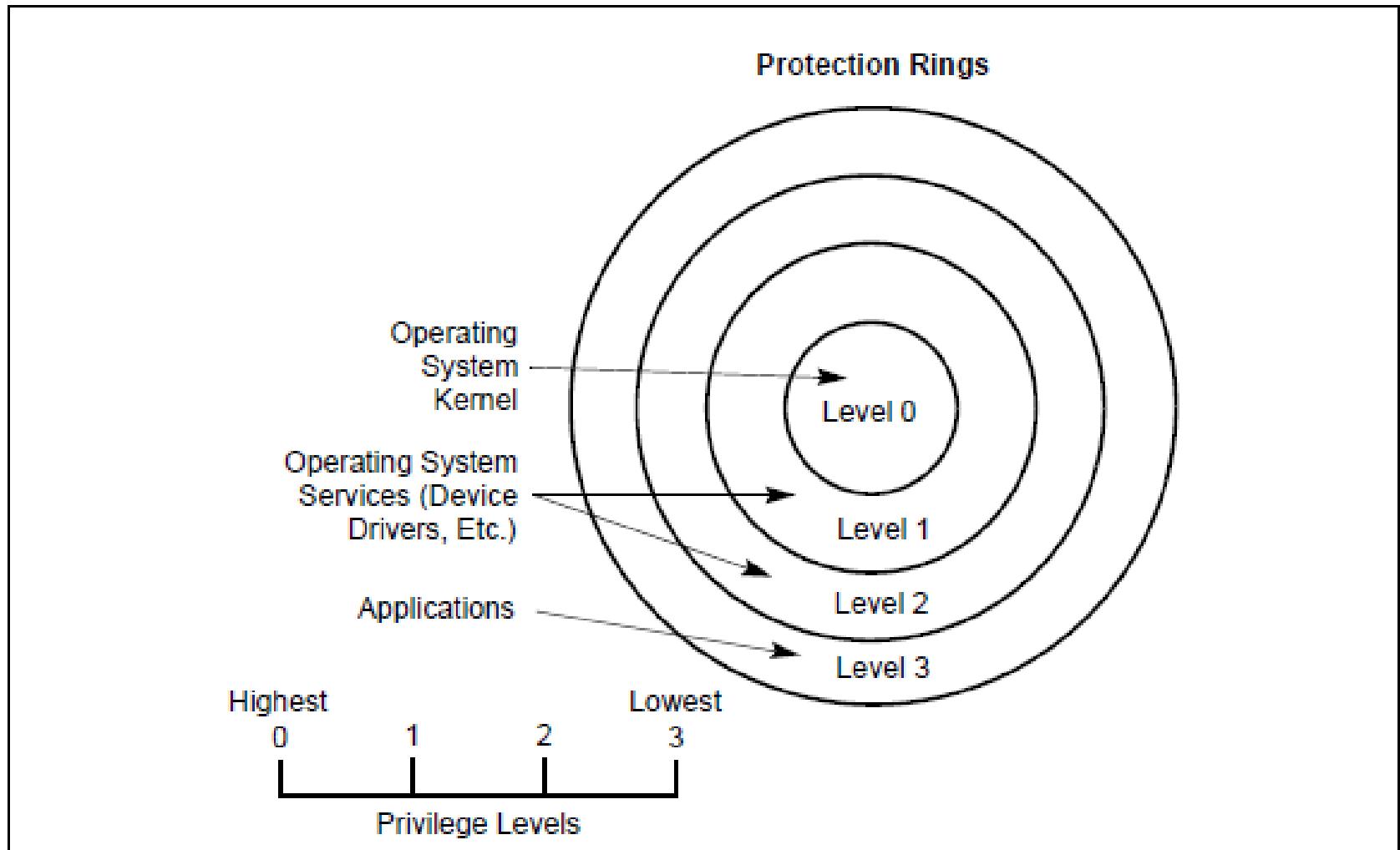
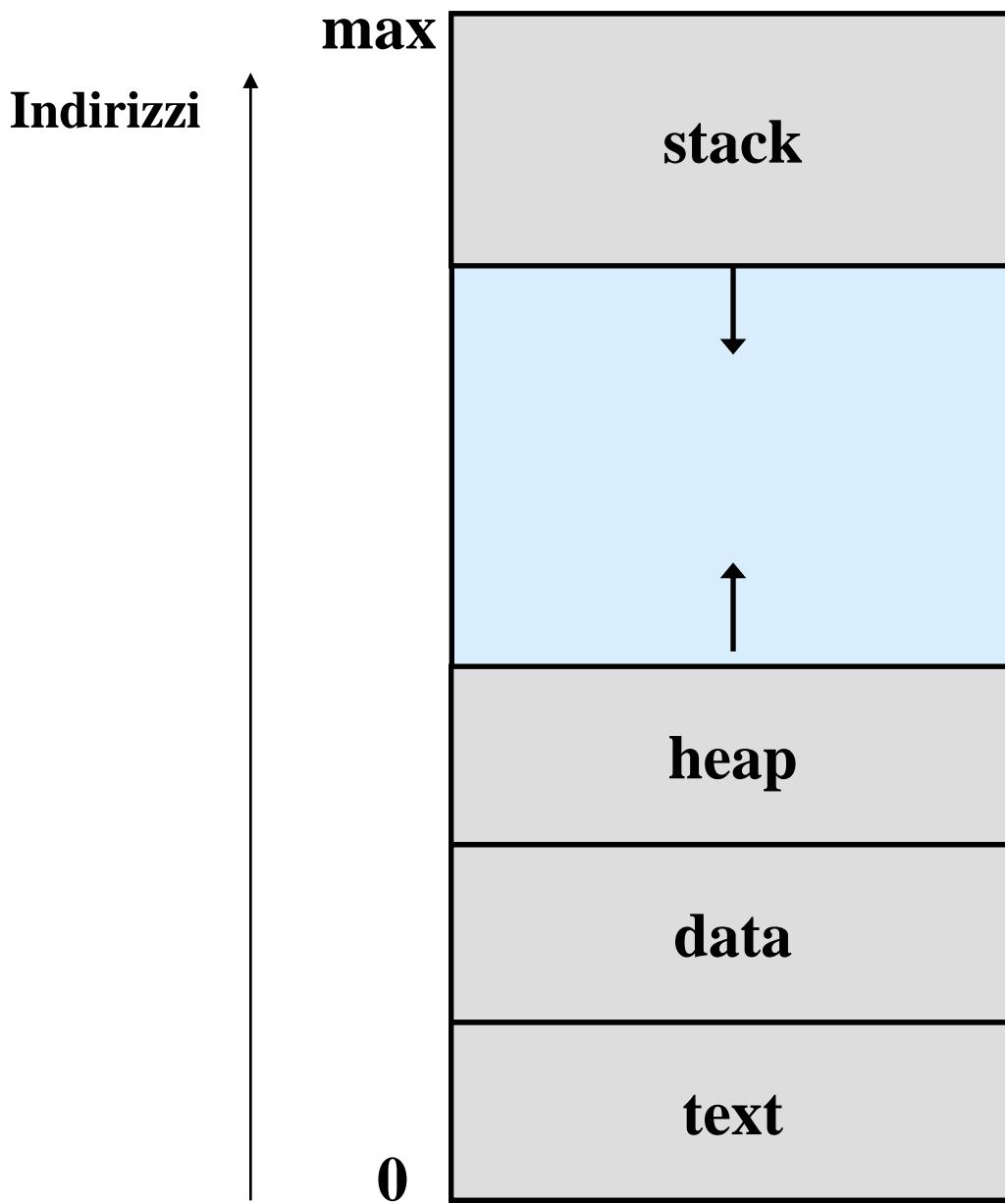


Figure 6-3. Protection Rings

# Organizzazione della Memoria usata dalla parte utente dei Processi



Contiene i Record di attivazione  
delle chiamate a funzione

Contiene le zone di Memoria  
allocata dinamicamente

Contiene le  
Variabili globali

Contiene il Codice eseguibile  
(istruzioni macchina)

# Supporto ai Processi da parte del livello ISA

I processori moderni hanno caratteristiche comuni che permettono di fornire ai livelli superiori una interfaccia di programmazione denominata livello ISA (Instruction Level Architecture) variabile da processore a processore ma avente alcune analogie:

**Modalità di protezione (modo kernel, modo utente) e istruzioni per switch tra i modi.**

**ALU, unità aritmetico-logica e istruzioni per comandarla.**

**Registri general purpose (di uso generale) e istruzioni per scambio dati tra registri della CPU e memoria , periferiche .**

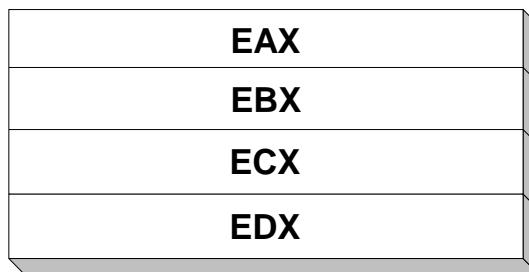
**Registri Specializzati (nome differente a seconda del processore):**

- **Extended Instruction Pointer (EIP)** serve a formare l'indirizzo in memoria (detto **Program Counter (PC)**) della prossima istruzione da eseguire. Contiene l'offset della prossima istruzione da eseguire, rispetto all'inizio del segmento di codice.
- **Program Status (PS)** detto anche **Registro di Stato (Status Register)**.
- **Stack Segment Register (SS)**. Punta all'inizio dello stack.
- **Code Segment Register (CS)**. Punta all'inizio della sezione text, il codice eseguibile.
- **Data Segment Register (DS)**. Punta all'inizio della sezione data, con le var globali.

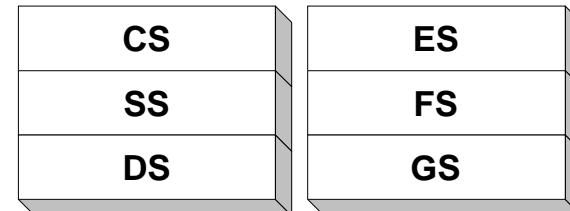
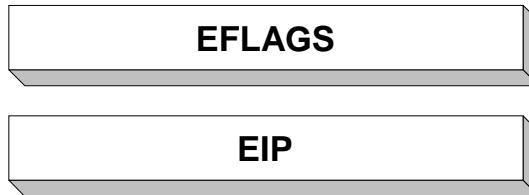
# Registri disponibili ai Programmi nei processori Intel "a 32 bit" cioe' di tipo IA-32 (i386, Pentium, ...)

- Registers are high speed memory inside the CPU
  - Eight 32-bit general-purpose registers
  - Six 16-bit segment registers
  - Processor Status Flags (EFLAGS) and Instruction Pointer (EIP)

## 32-bit General-Purpose Registers

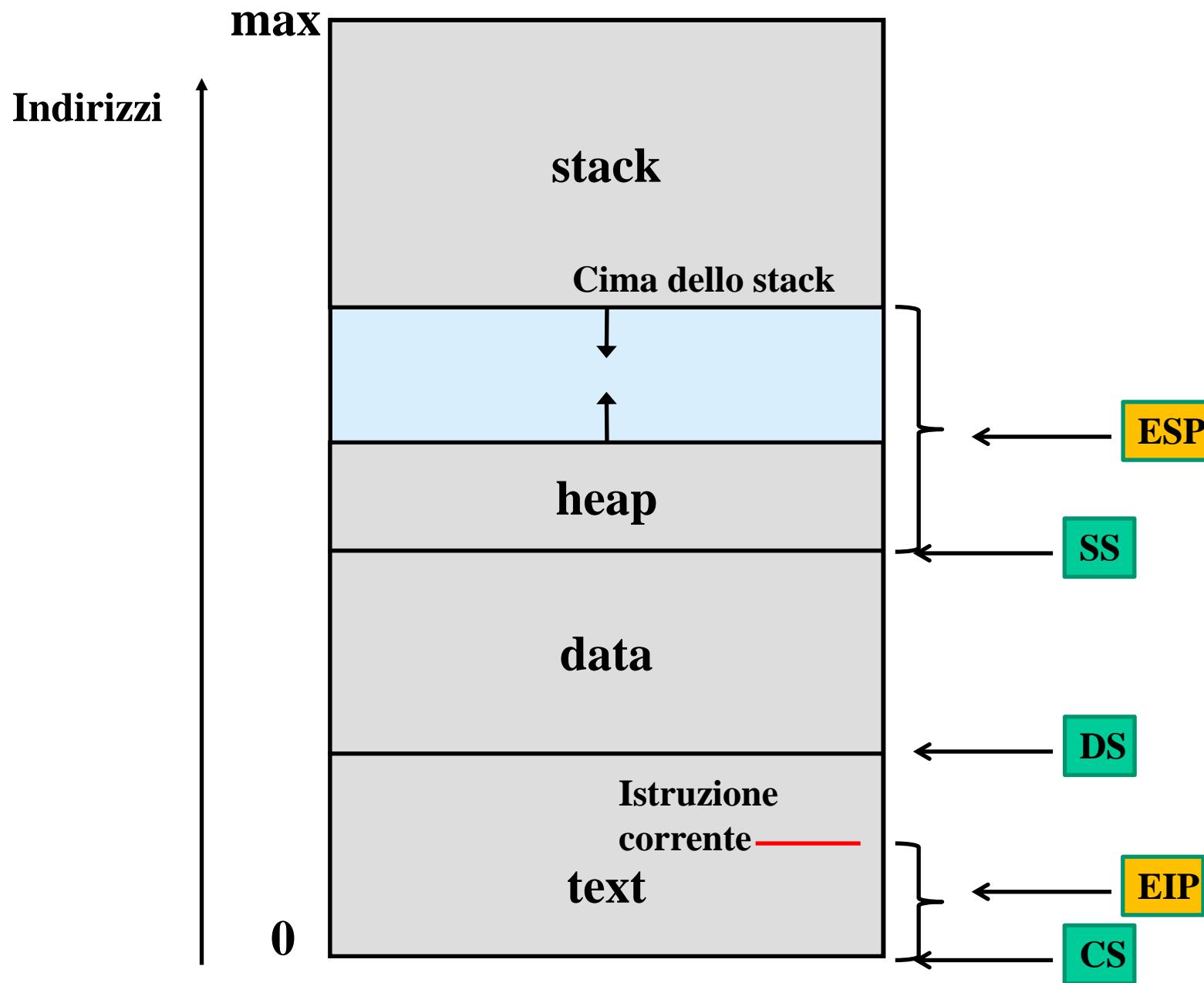


## 16-bit Segment Registers



- Inoltre, Registro di Stato (Status Register), non disponibile ai programmi, definisce modalità di funzionamento, utente o kernel

# Uso dei registri di segmento e di offset nella parte utente dei Processi



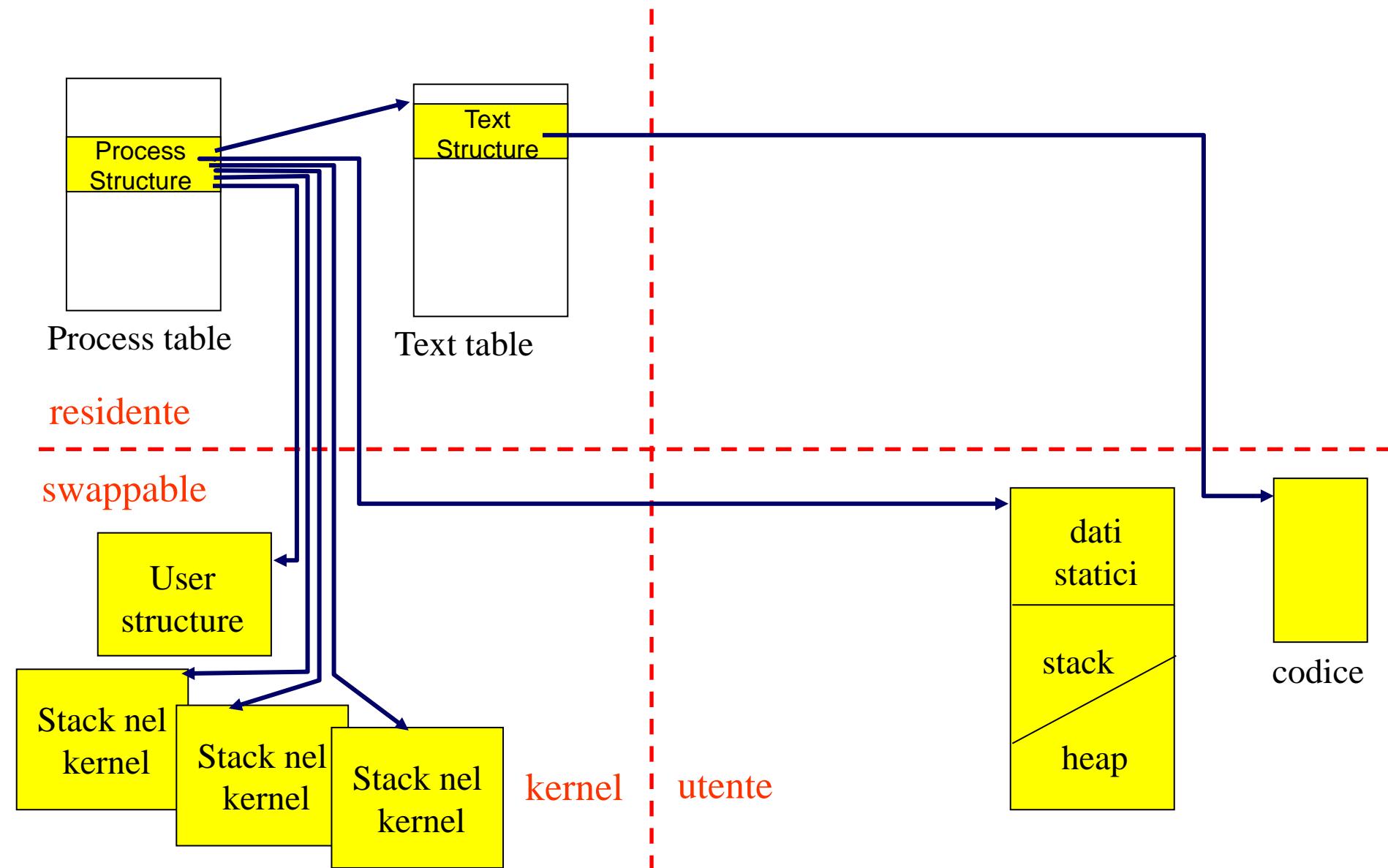
## **Supporto ai "modi di esecuzione della CPU" per i processi**

Quando un processo esegue una chiamata ad interrupt, la CPU entra nella modalità di esecuzione kernel e deve utilizzare uno (o più) stack "di sistema" separato rispetto allo stack utilizzato per le normali chiamate a funzione.

Ciò permette al kernel di separare e proteggere i record di attivazione utilizzati nelle chiamate ad interrupt.

Ciascun processo, perciò, mantiene uno stack per ciascun livello di privilegio della CPU.

# Immagine in Memoria dei Processi (spazi utente & kernel)



- Notare la presenza di uno stack per le funzioni utente nello spazio utente e di più stack per l'esecuzione delle system calls in spazio kernel.

# Cosa c'e' in esecuzione? Task

In un computer sono in esecuzione:

- alcuni processi (i programmi lanciati dagli utenti)
- alcuni gestori degli interrupt
  - per eventi asincroni originati dalle periferiche (scadenza timer, arrivo caratteri da tastiera, arrivo msg da DMA, da usb, da rete)
  - per eventi sincroni generati dai processi (invocazioni di system call mediante chiamate esplicite alla istruzione che esegue interrupt software).
- alcuni gestori delle eccezioni
  - per eventi sincroni generati dalla istruzioni eseguite dai processi

I processi, gli interrupt e le eccezioni eseguono ciascuno in un proprio contesto denominato Task. I Task mantengono le informazioni sui segmenti di memoria utilizzati e sul valore corrente dei registri principali.

Lo scheduler del sistema operativo decide per quanto tempo eseguire ciascun task.

Salvare e ripristinare lo stato di un task consente di intervallare l'esecuzione di più task che potranno così utilizzare a turno la CPU (**interleaving**) dando un'impressione di un'esecuzione contemporanea.

## **Supporto al Sistema da parte del livello ISA**

I processori moderni offrono una interfaccia di programmazione (livello ISA, Instruction Level Architecture) che fornisce supporto non solo ai processi ma anche all'implementazione del sistema operativo.

Il livello ISA offre infatti anche diversi registri dedicati al sistema operativo e numerose istruzioni macchina che consentono al sistema operativo:

- di effettuare l'interleaving concedendo l'uso della CPU per piccoli intervalli di tempo ad un processo e poi ad un altro, salvando e cambiando il contesto di esecuzione ogni volta che cambia il processo in esecuzione.
- di eseguire in un contesto separato e protetto le system calls chiamate dal processo.

# Instruction Set Architecture of IA-32

## Task

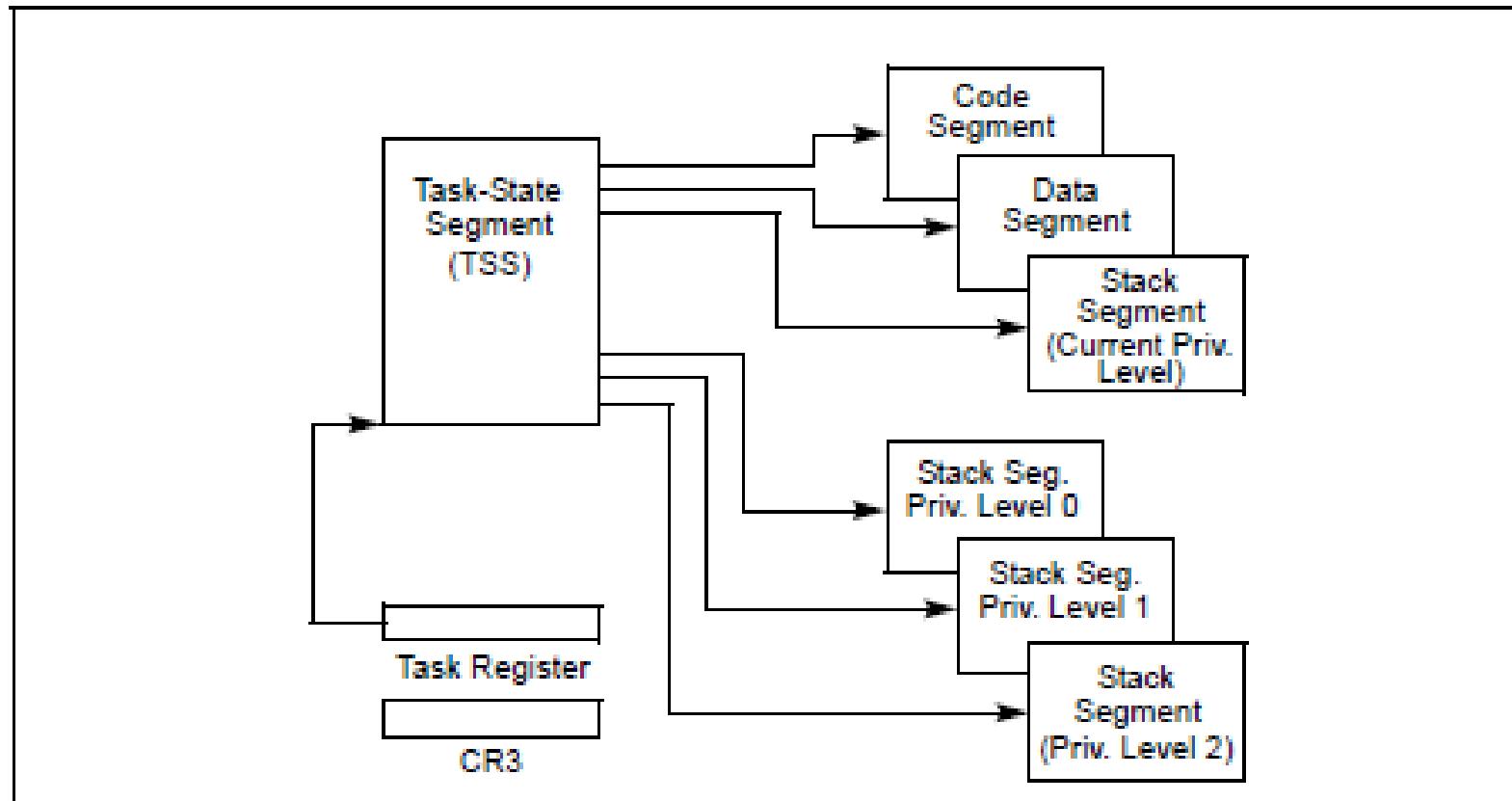


Figure 7-1. Structure of a Task

# ISA of IA-32

## Task- State Segment

31	15	0
I/O Map Base Address	Reserved	T 100
Reserved	LDT Segment Selector	96
Reserved	GS	92
Reserved	FS	88
Reserved	DS	84
Reserved	SS	80
Reserved	CS	76
Reserved	ES	72
	EDI	68
	ESI	64
	EBP	60
	ESP	56
	EBX	52
	EDX	48
	ECX	44
	EAX	40
	EFLAGS	36
	EIP	32
	CR3 (PDBR)	28
Reserved	SS2	24
	ESP2	20
Reserved	SS1	16
	ESP1	12
Reserved	SS0	8
	ESP0	4
Reserved	Previous Task Link	0

 Reserved bits. Set to 0.

Figure 7-2. 32-Bit Task-State Segment (TSS)

# ISA of IA-32

\*\*\*\*\*

## System-Level Registers and Data Structures used for Task Management

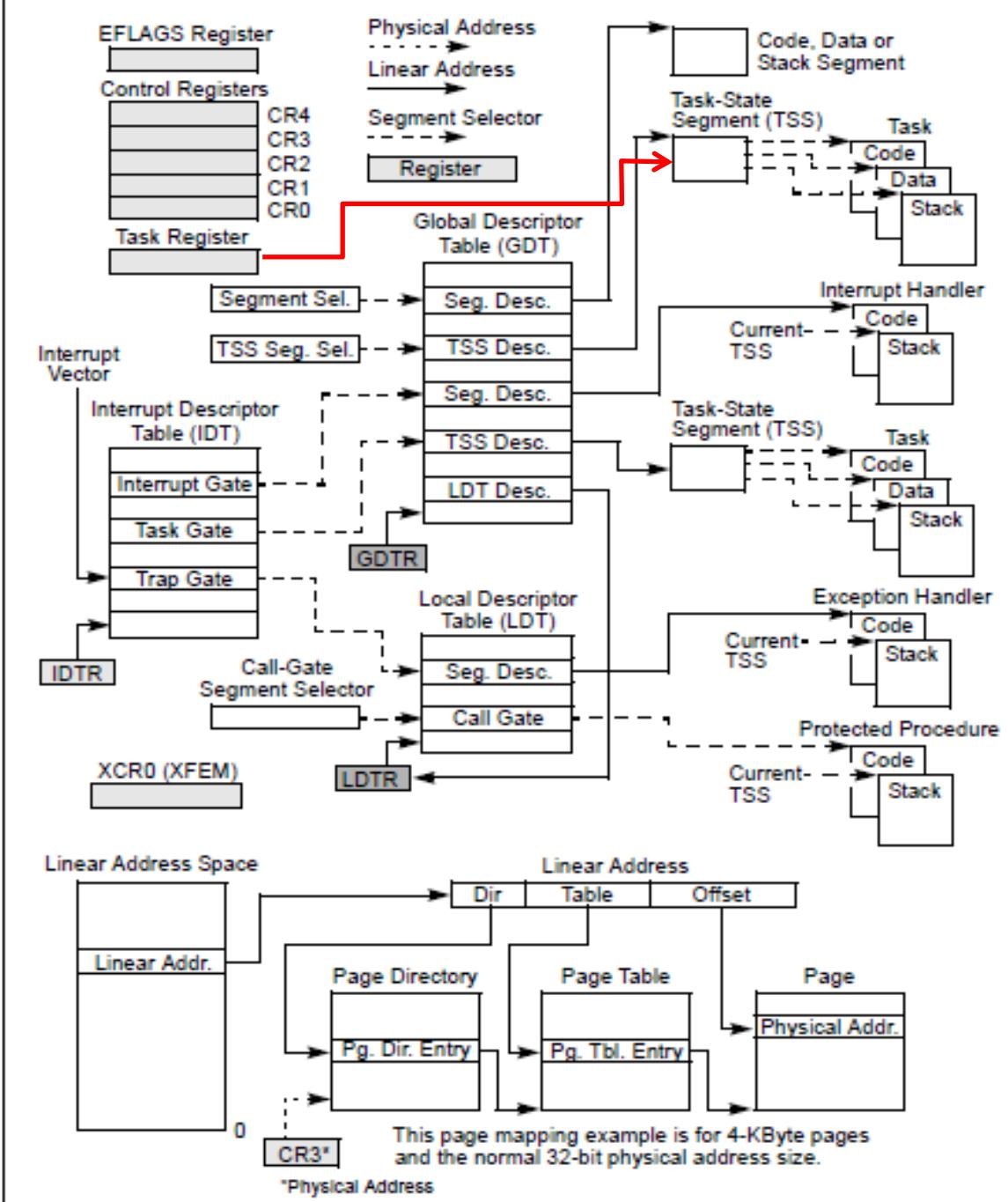


Figure 2-1. IA-32 System-Level Registers and Data Structures

# ISA of IA-32

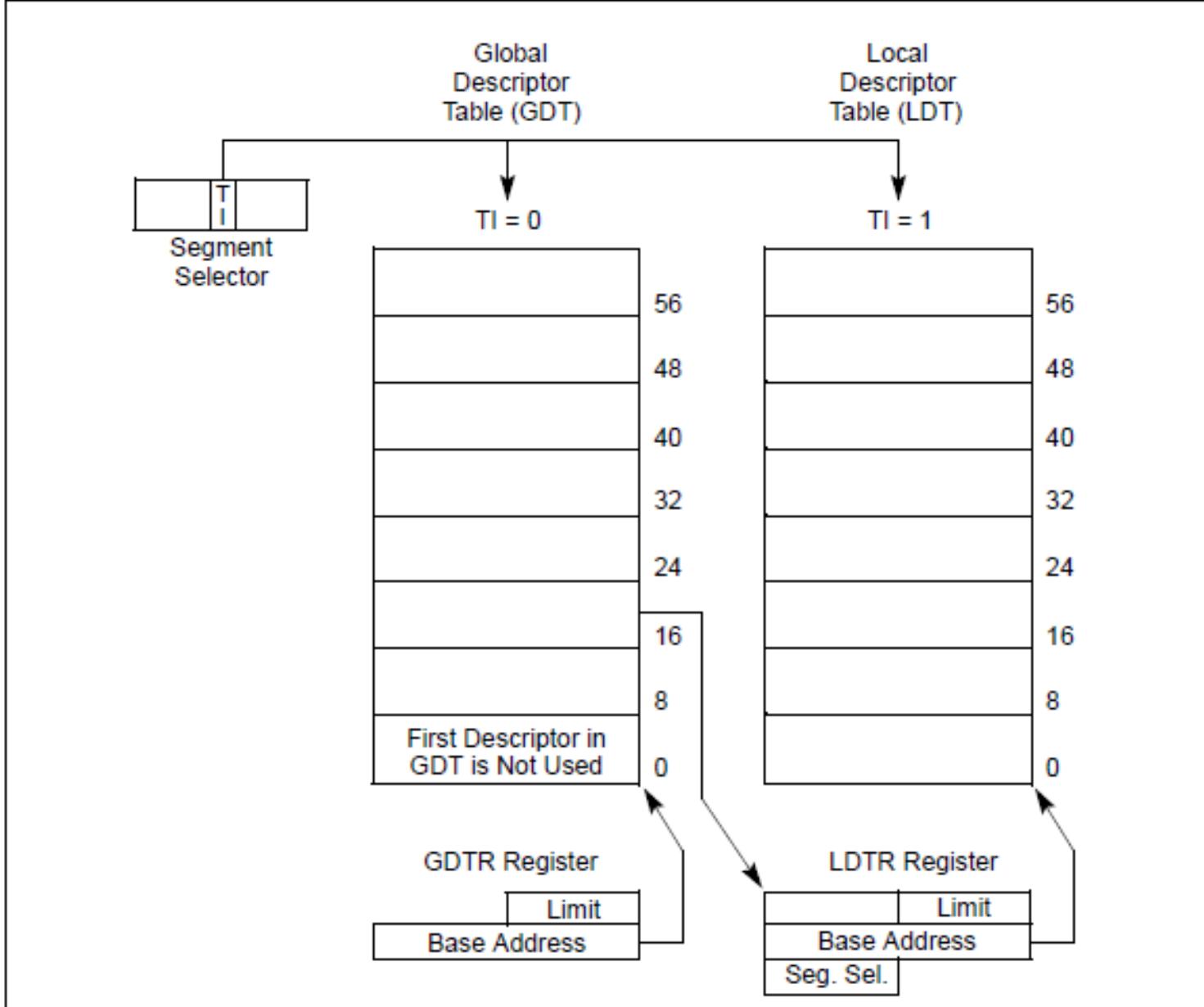
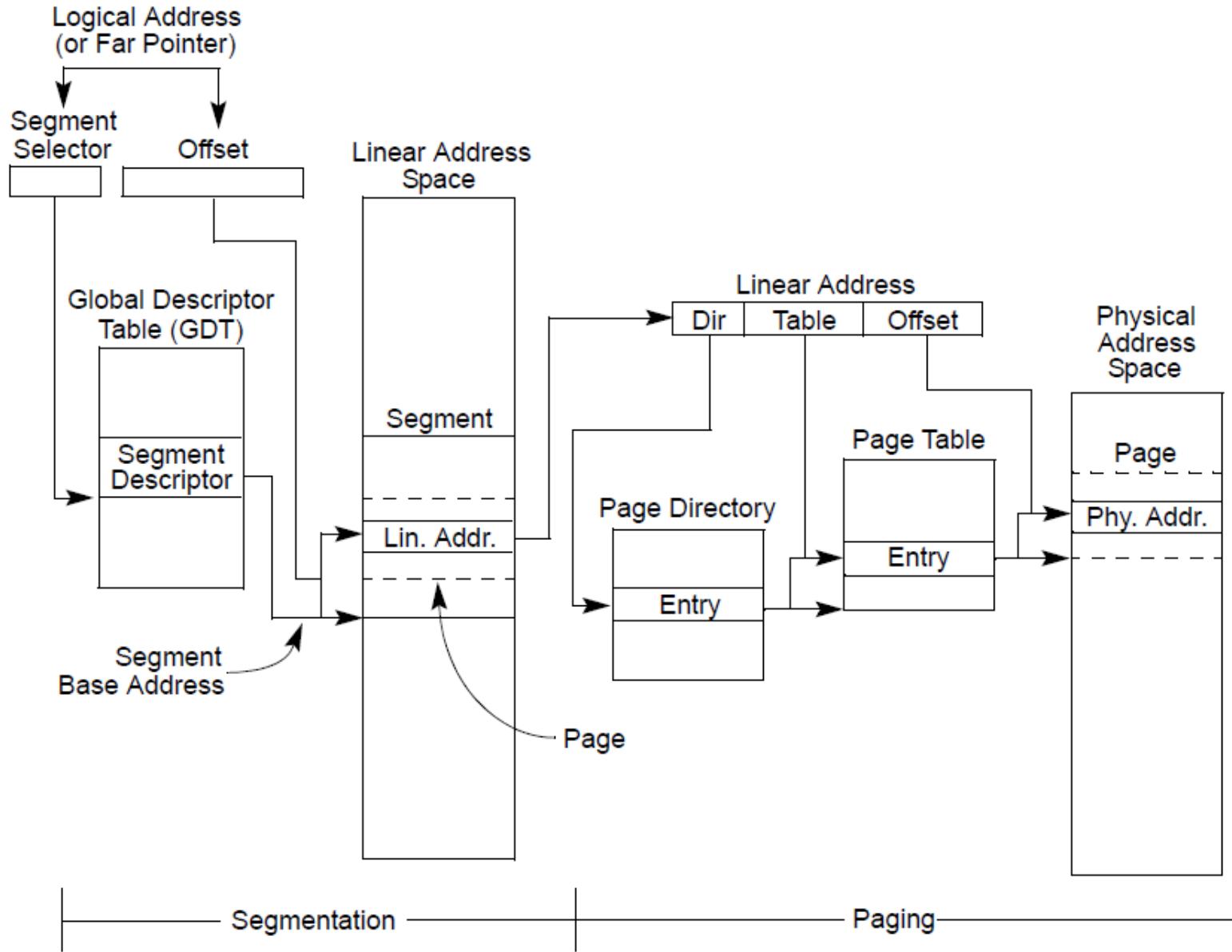


Figure 3-10. Global and Local Descriptor Tables

# ISA – Segmentazione e Paginazione in IA-32



# Processi

Un processo è l'istanziazione in memoria di un programma eseguibile.

Quando un programma viene lanciato, il **loader** (che fa parte del sistema operativo) :

- **crea i segmenti di memoria** per il processo popolando la tabella con le informazioni sui diversi segmenti,
- carica in memoria il codice eseguibile (sezione text) del programma,
- carica in memoria la sezione Data,
- **crea lo stack utente** per l'esecuzione delle funzioni del programma,
- **crea gli stack di sistema per l'esecuzione delle system calls** che verranno invocate dal programma utente,
- copia eventuali argomenti passati a riga di comando mettendoli a disposizione del main
- infine ordina alla CPU di eseguire la prima istruzione eseguibile corrispondente al main del programma.

# Chiamata ad Interrupt da Programma

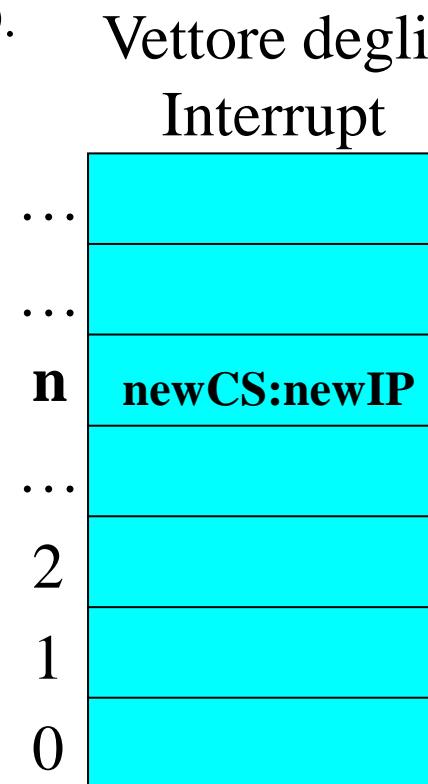
- I programmi chiamano Interrupt per ottenere servizi da sistema operativo o BIOS.
- Per chiamare un interrupt da programma, si usa l'istruzione assembly: **INT n**
- n è un numero intero maggiore o uguale a zero che viene usato come indice per accedere alla n-esima posizione del Vettore degli Interrupt.
- Il Vettore degli Interrupt è posizionato a partire dall'indirizzo 0 in memoria.
- L' n-esimo elemento del Vettore di Interrupt contiene diverse informazioni, tra cui l'indirizzo (CS:IP) della prima istruzione eseguibile (codice macchina) della routine di gestione dell'interrupt di indice n.
- Routine sono fornite da BIOS e S.O.

Codice del Processo  
in esecuzione

IP  
oldIP

```
push BX  
mov EAX, 13  
INT n  
pop BX  
inc AX
```

CS  
oldCS



routine di gestione  
dell'Interrupt n

```
push EAX  
mov BX, 4  
.....  
IRET
```

newIP  
newCS

# Chiamata ad Interrupt da Programma – Cambio di Contesto

E' in esecuzione (1) il codice di un processo che sta utilizza lo stack utente.

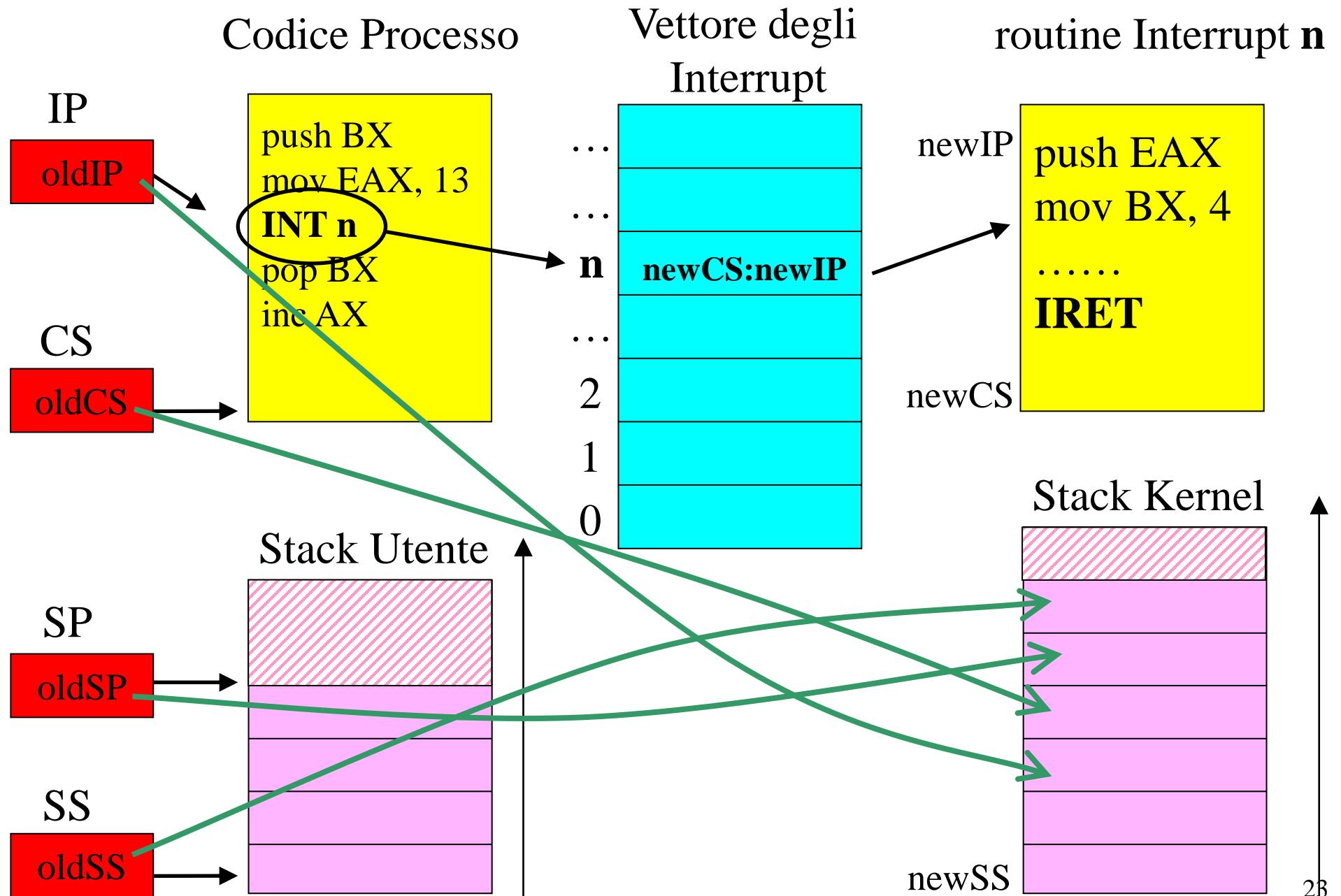
Quando la CPU esegue l'istruzione INT n :

- l' Instruction Pointer viene fatto puntare all'istruzione successiva ad INT.
- il processore passa in modalità kernel con il livello di privilegio da usare.
- il processore salva i valori attuali dei registri SS, SP, CS, IP nello stack di sistema del processo che ha chiamato l'interrupt, cioè lo stack dedicato all'esecuzione in modalità kernel per quel processo.
- il processore carica i registri SS e SP con i valori dello **stack di** sistema per quel livello di privilegio.
- il processore carica i registri CS e IP con l'indirizzo della routine di gestione dell'interrupt trovato nell'n-esima posizione del vettore di interrupt.
- A questo punto (2) viene eseguita la routine dell'Interrupt, nello stack di sistema.

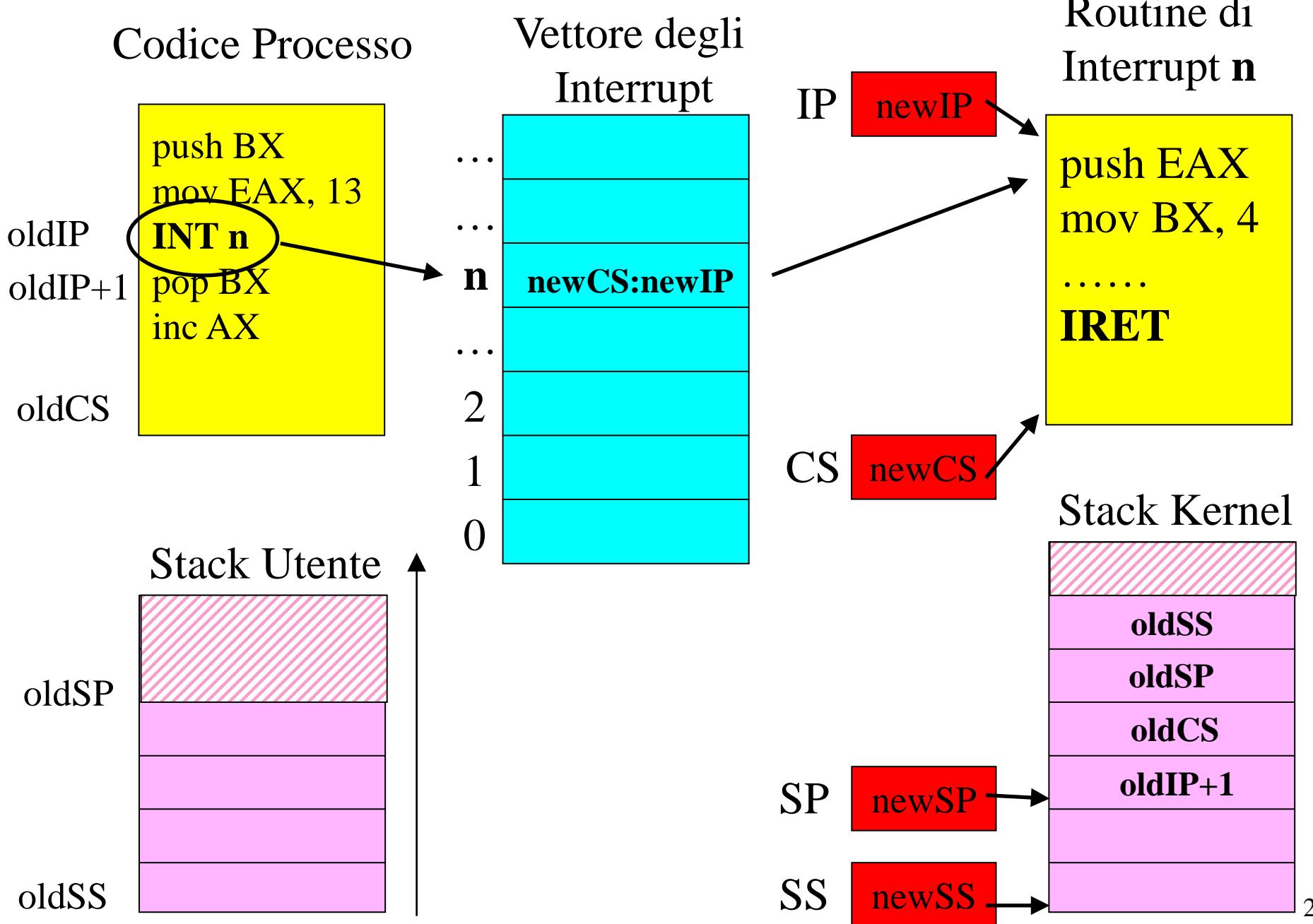
La routine dell'Interrupt termina (3) con l' istruzione IRET (Interrupt Return) che :

- carica i registri IP, CS, SP e SS con i valori salvati sullo stack di sistema.
- fa tornare il processore in modalità utente.
- così l'esecuzione ricomincia (4) dall'istruzione del programma successiva all'istruzione INT n utilizzando lo stack utente del processo.

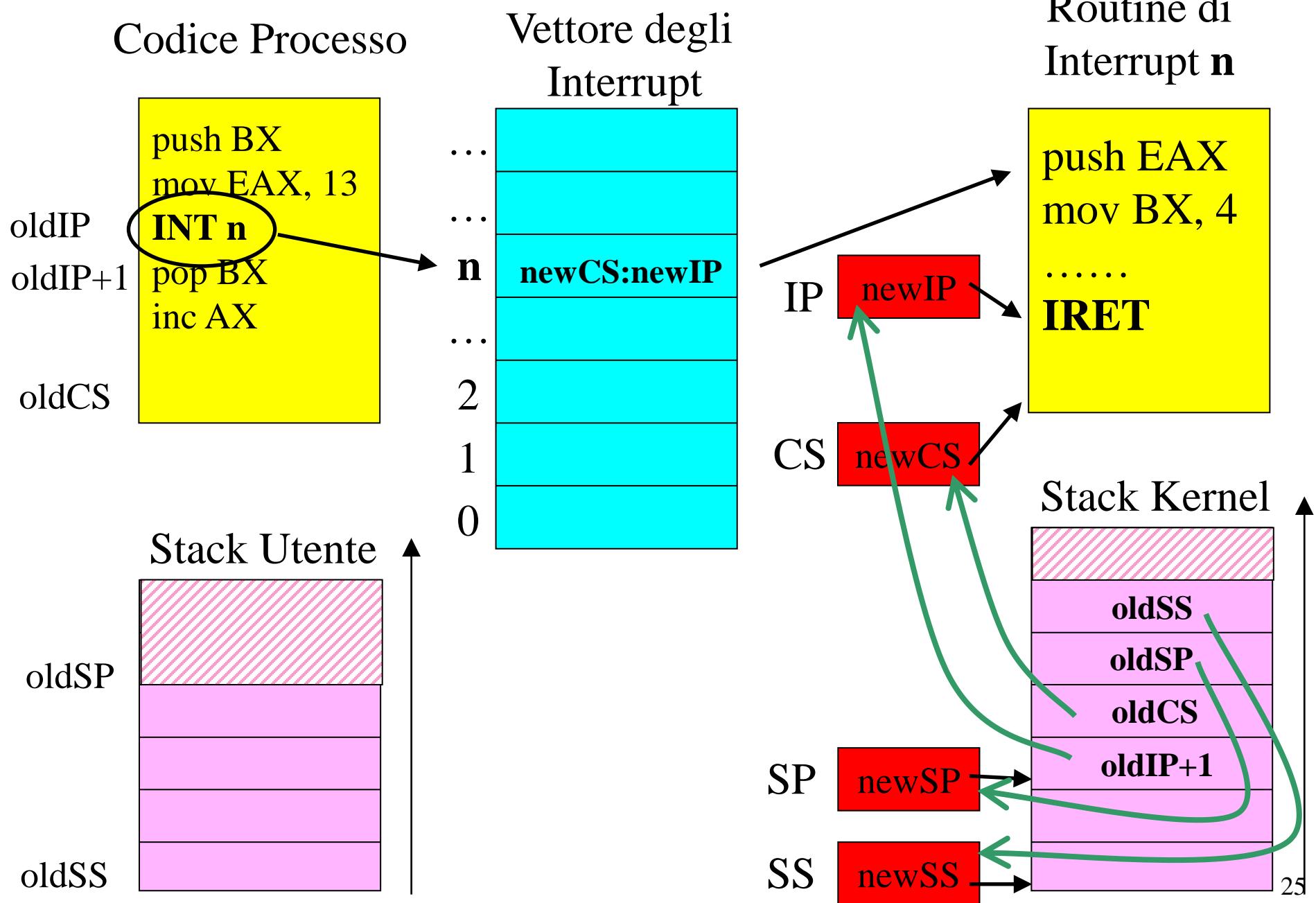
# (1) Prima di Chiamata ad Interrupt da Programma



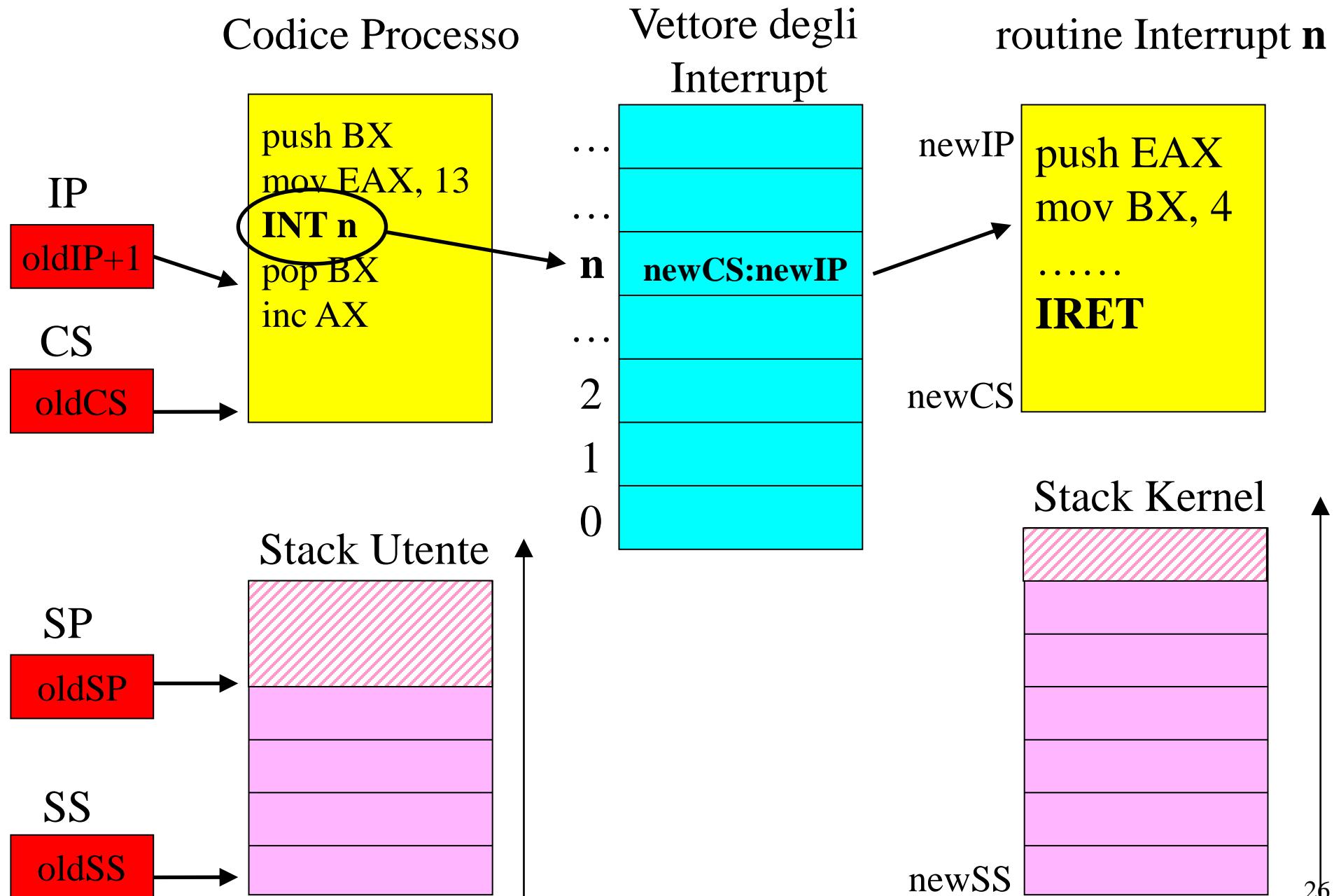
## (2) Dopo esecuzione istr. INT n -



### (3) Prima di esecuzione istr. IRET



## (4) Dopo Esecuzione istr. IRET



# Il meccanismo delle System Calls

- un programma utente, durante l'esecuzione può invocare una system call.
- la system call è implementata nella routine di gestione di un certo interrupt n.
- la system call viene invocata eseguendo una istruzione INT n, con un certo n intero
- il programma passa i parametri all' interrupt mettendoli in registri (EAX e altri)
- chiamata ad interrupt
- switching di contesto – da modo utente a modo kernel
  - salvataggio del contesto
- le routine di gestione degli interrupt.
  - puntatori a funzione nel vettore degli interrupt.
- esecuzione su stack del kernel (per separare contesto di esecuzione)
- ritorno a modo utente
  - ripristino del contesto

# Instruction Set Architecture (ISA) & Sistema Operativo

## Interrupt e Eccezioni

- Eccezioni (Exceptions) e Interruzioni (Interrupts)
  - entrambe gestite mediante routine rintracciabili a partire dal Vettore degli Interrupt
- Eccezioni (Exceptions)
  - sono sincrone rispetto alle istruzioni eseguite dalla CPU, ovvero
  - sono provocate (**involontariamente**) da una istruzione macchina eseguita dalla CPU che provoca un errore o un caso particolare da gestire
- **TRAP**
  - l'istruzione che ha causato il trap viene momentaneamente sospesa, ma alla fine della gestione del trap viene portata a buon fine.
  - Es: trap per debugging
- **FAULT**
  - l'istruzione che ha causato il fault viene interrotta, e viene eseguita la routine di gestione. In un successivo momento l'istruzione verrà rieseguita da principio.
  - Es: Page Fault, la pagina di memoria che contiene l'indirizzo a cui stiamo cercando di accedere è swappata su disco. La pagina viene caricata in memoria. Prima o poi l'istruzione verrà nuovamente eseguita.
- **ABORT**
  - Causata da errore irrimediabile, l'istruzione viene abortita e il processo killato.
  - Es: divisione di un numero per zero.
  - Es: **segmentation fault** (nonostante il nome è una eccezione di tipo Abort)

# Instruction Set Architecture (ISA) & Sistema Operativo

## Interrupt e Eccezioni

- Interrupt

Considerando il momento in cui vengono eseguiti, gli Interrupt possono essere

- **SINCRONI (interrupt software)**

- esplicitamente chiamati dalla CPU mediante l'istruzione INT n.
- Es: la CPU ordina di fare output su video di un carattere chiamando una syscall.

- **ASINCRONI (interrupt hardware)**

- scatenati da una periferica che, mediante il BUS, avvisa la CPU che è accaduto un evento che deve essere gestito.
- Ad esempio, la tastiera avvisa che l'utente ha premuto un tasto.
- La periferica invia un segnale che codifica un numero intero, tale numero è l'indice dell'Interrupt da chiamare.
- La CPU interrompe quello che sta facendo e gestisce l'Interrupt.

Considerando la priorità e la possibilità di essere ritardati, gli Interrupt possono essere

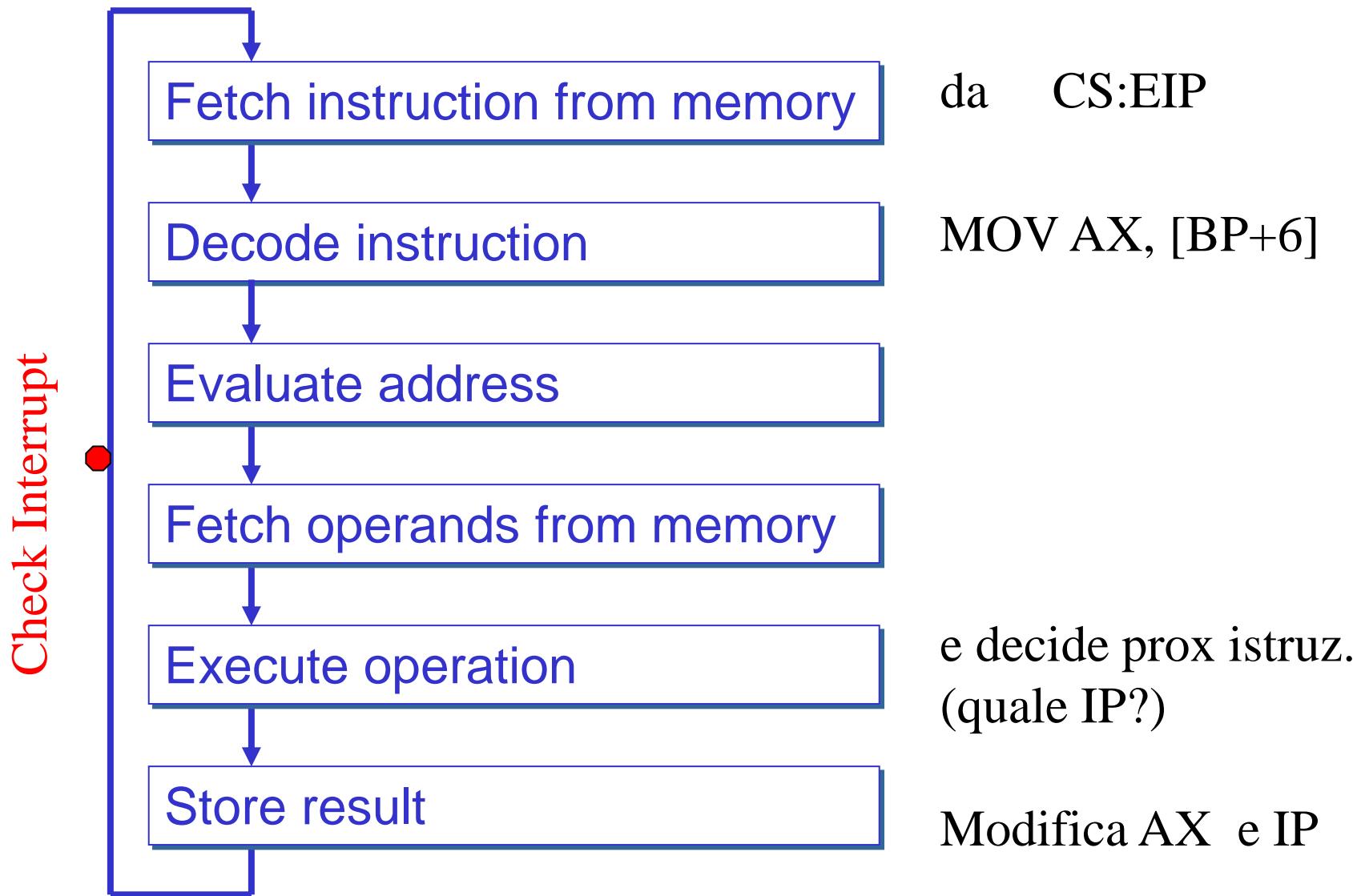
- **MASCHERABILI**

- Es: E' arrivato un carattere da tastiera, ma se c'è qualcosa più urgente da fare è meglio svolgere i compiti più urgenti.

- **NON MASCHERABILI**

- Es: Avviso di errore sul Bus, bisogna gestirlo immediatamente.
- Durante l'esecuzione di una routine di gestione degli Interrupt, la CPU setta un bit (un piedino) che disabilita la gestione degli Interrupt Mascherabili.

# ISA - Instruction Processing - Ciclo di Neumann



# Sistemi operativi MultiTasking: sfruttare il Time Sharing

Nei moderni sistemi operativi, più processi, più thread, più gestori di interrupt ed gestori di eccezioni, sono presenti in memoria contemporaneamente (**MultiTasking**), e cercano di eseguire concorrentemente contendosi l'uso della CPU (**Time Sharing**).

- Lo scheduler è la componente del S.O. che si occupa di alternarli nell'uso della CPU.
- L'esecuzione della CPU viene suddivisa in un certo numero di quanti temporali (detti **time slice**).
- Allo scadere di un quanto di tempo, il processo (o thread) corrente viene interrotto e l'esecuzione passa ad un altro processo (o thread).
- Quando un processo (o thread) richiede un'operazione di I/O, la CPU viene assegnata ad un altro processo, mentre le periferiche attendono il completamento delle operazioni di I/O.
- Quando l'operazione di I/O è stata effettuata dalle periferiche, il processo che la richiedeva si rimette a disposizione dello scheduler e attende il suo turno per l'utilizzo della CPU.

I passaggi (context switch ) avvengono così frequentemente che i programmi sembrano essere eseguiti contemporaneamente.

# Sistemi operativi "Interrupt Driven"

I moderni S.O. sono detti "Interrupt Driven" poichè gran parte delle funzionalità del kernel del S.O. viene eseguito all'interno di una qualche routine di gestione di un interrupt, cioè viene eseguito come reazione al verificarsi di un evento che ha sollevato un interrupt o una eccezione.

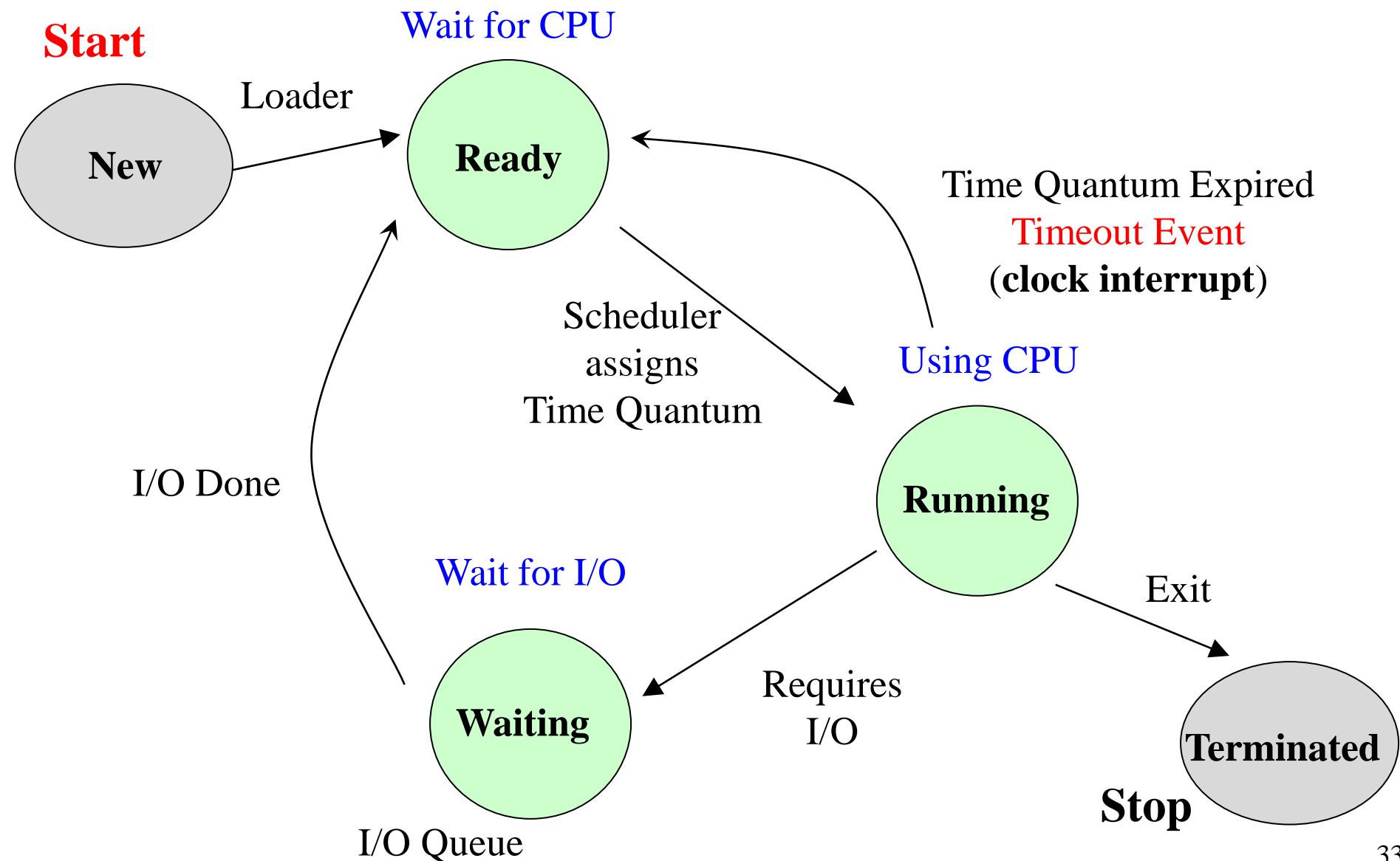
Uno dei più importanti eventi che sollevano un interrupt è lo scadere del "quanto" di tempo di esecuzione che lo scheduler ha concesso ad un processo (o ad un thread all'interno di un processo).

Allo scadere del quanto di tempo, il timer di sistema genera un interrupt che risveglia lo scheduler.

Lo scheduler decide quale altro processo (o thread) dovrà essere eseguito e passa il controllo a tale processo (thread).

# Sistema Operativo - Scheduler

## Ciclo di Vita dei Processi (passaggio di stato dei processi)



# **Passaggio di stato dei processi, sintesi**

Ammissione (new → ready):

una volta creato e collocato in memoria dal loader, il processo è inserito nella coda dei processi ready.

Dispatch (ready → running):

il processo è scelto dallo scheduler come il prossimo ad eseguire ed è messo in esecuzione.

Interrupt di tempo (running → ready):

il processo termina il suo quanto di tempo e torna in coda nella coda dei ready

Richiesta (running → waiting):

il processo effettua una chiamata a sistema bloccante e viene inserito nell'opportuna coda di attesa

Evento (waiting → ready):

l'attesa termina quando si verifica un evento e il processo torna nella coda dei ready

Conclusione (running → terminated):

il processo esegue l'ultima istruzione e termina

# Interfaccia Utente a caratteri (testuale)

## Interprete dei comandi

### Shell scripting

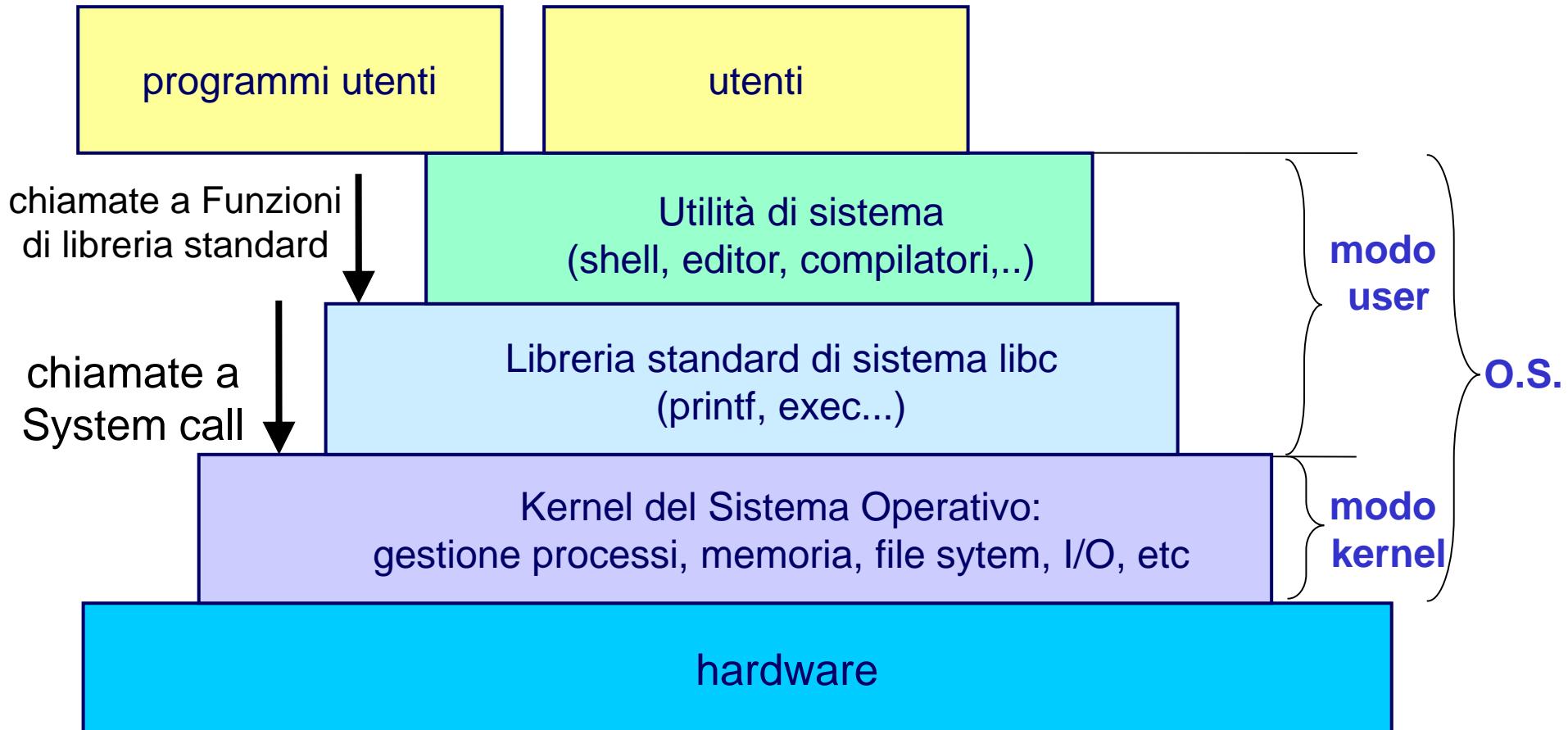
#### NOTA BENE:

Questa guida contiene solo una introduzione minimale all'utilizzo dell'interprete di comandi bash, e serve per fornire agli studenti del corso di Sistemi Operativi le informazioni iniziali per utilizzare una semplice interfaccia a riga di comando con cui compilare programmi in linguaggio ANSI C mediante il compilatore gcc, eseguire e debuggare tali programmi, scrivere ed eseguire semplici script, capire le interazioni tra i programmi e l'utente e, in sostanza, identificare le funzionalità messe a disposizione dell'utente dal sistema operativo.

Per tale motivo, alcuni concetti sono stati volutamente semplificati, allo scopo di rendere più semplice la comprensione, anche a discapito della realtà.

Vittorio Ghini

# Struttura del Sistema Operativo



# Requisito Hardware per il Sistema Operativo

## Modi di esecuzione della CPU

Instruction Set Architecture of IA-32

Privilege Levels (Rings)

Protection Rings

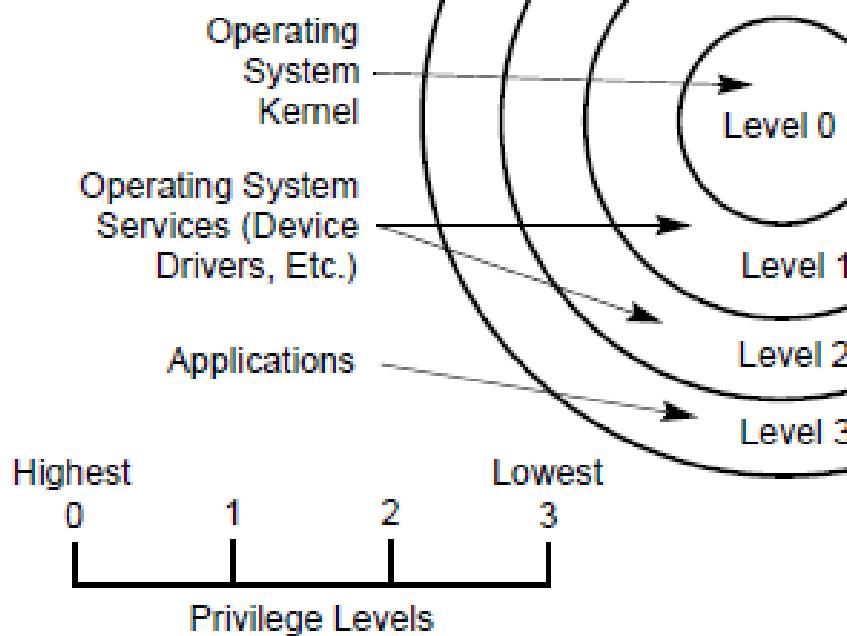


Figure 6-3. Protection Rings

# chiamata a system call mediante interrupt

```
/* file print.s Descr.: stampa a video di stringa Architettura: x86      Dialetto assembly AT&T  (-masm=att)
Assemblaggio e Linking    Modo 0, non usare gcc:
Assemblare con: as -o print.o --gstabs print.s (eventuale opzione --gstabs per poter usare gdb o ddd)
Linkare con:   ld -o print.exe print.o
Eseguire con ./print.exe o (per il debug) con gdb print.exe o ddd print.exe */
```

## .data

```
miastringa: .string "MANNAG\n" # stringa da stampare compresa di a capo
```

## .text

```
.globl _start
```

### \_start:

```
nop
```

/\* qui attivo due volte, mediante l'istruzione **int**, l'interruzione software identificata dal valore **0x80=8016** con la quale, in generale, si richiamano routine o servizi del sistema operativo (nel nostro caso Linux). Il servizio richiamato e' identificato dal valore inserito nel registro eax prima di attivare la interruzione.

- Il valore 4 chiede il servizio di stampa di una stringa.
- Il valore 1 invece corrisponde alla routine di terminazione del programma e ritorno al sistema operativo.

```
*/
```

```
/* stampo stringa e vado a capo */
```

```
movl $4, %eax
```

```
/* servizio da ottenere: stampa */
```

```
movl $1, %ebx
```

```
/* sottoservizio da ottenere */
```

```
movl $miastringa, %ecx
```

```
/* indirizzo di inizio stringa in registro ecx */
```

```
movl $7, %edx
```

```
/* lunghezza della stringa da stampare in registro edx */
```

```
int $0x80
```

```
/* ordine di eseguire interrupt */
```

```
/* termino */
```

```
fine:
```

```
movl $1, %eax
```

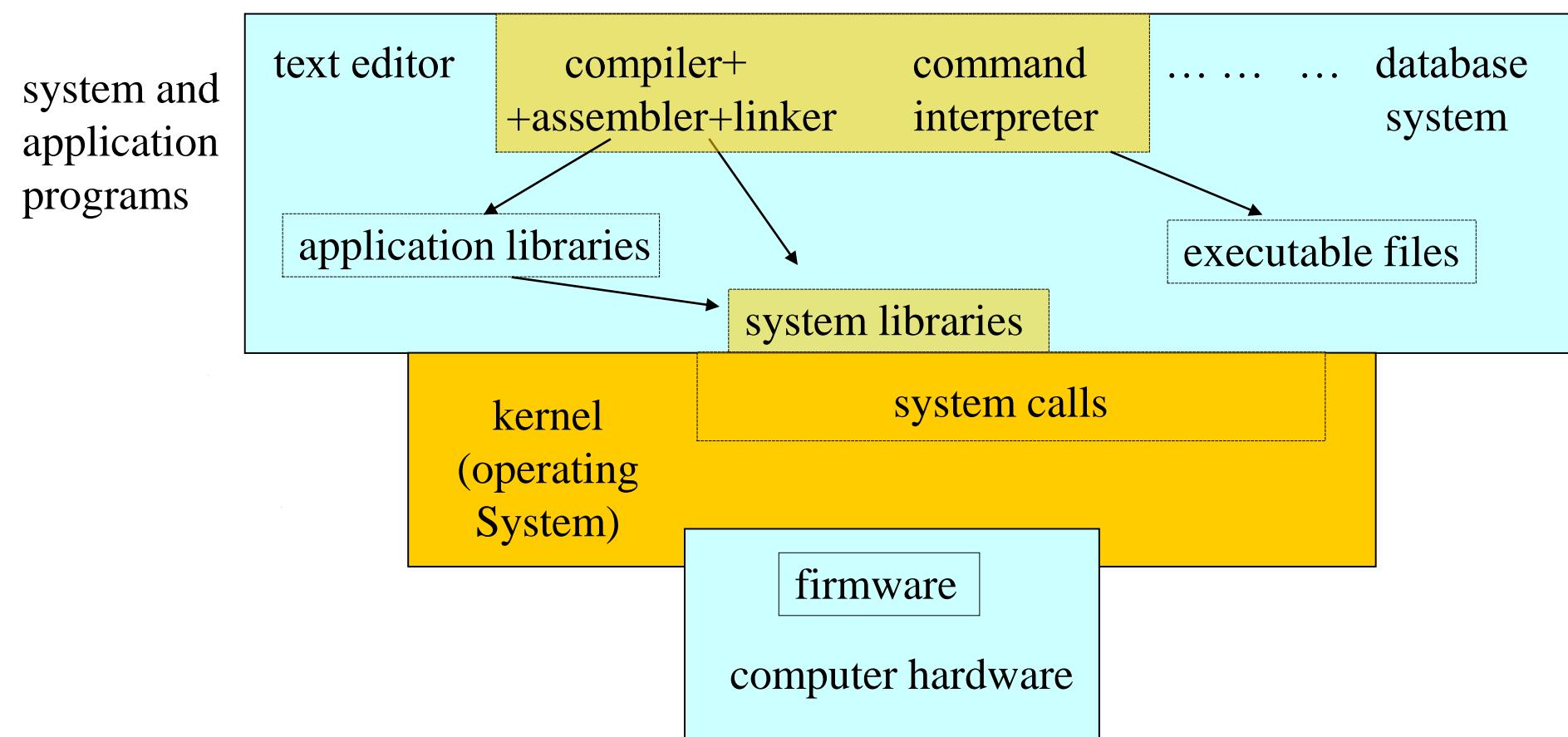
```
/* servizio da ottenere: terminazione processo */
```

```
int $0x80
```

```
/* ordine di eseguire interrupt */
```

# Librerie e Chiamate di sistema (1)

Ricordiamo l'organizzazione del computer, in particolare la relazione tra le system calls e le librerie di sistema.



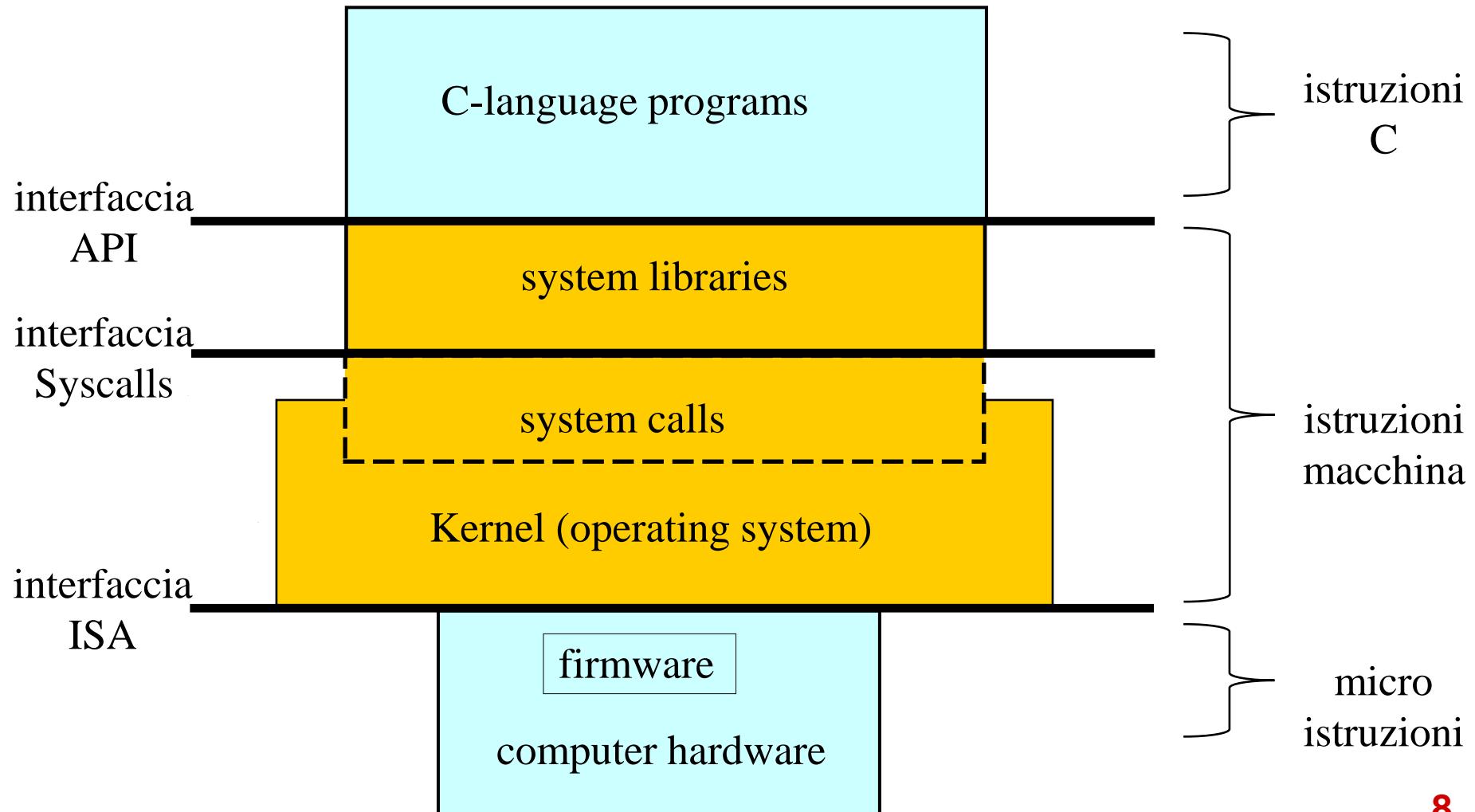
# Librerie e Chiamate di sistema (2)

- Le chiamate di sistema forniscono ai processi i servizi offerti dal SO:  
Controllo dei processi, Gestione dei file e dei permessi, Gestione dei dispositivi di I/O, Comunicazioni.
- Il modo in cui sono realizzate cambia al variare della CPU e del sistema operativo.
- Il modo di utilizzarle (chiamarle) cambia al variare della CPU e del sistema operativo.
- Sono utilizzate (invocate) direttamente utilizzando linguaggi di basso livello (assembly).
- Possono essere chiamate (invocate) indirettamente utilizzando linguaggi di alto livello (C o C++)
- Infatti, normalmente i programmi applicativi non invocano direttamente le system call, bensì invocano funzioni contenute in librerie messe a disposizione dal sistema operativo ed utilizzate dai compilatori per generare gli eseguibili. L'insieme di tali funzioni di libreria rappresentano le **API (Application Programming Interface)** cioè l'interfaccia che il sistema operativo offre ai programmi di alto livello.
- Le librerie messe a disposizione dal sistema operativo sono dette **librerie di sistema**.

# Librerie e Chiamate di sistema (3)

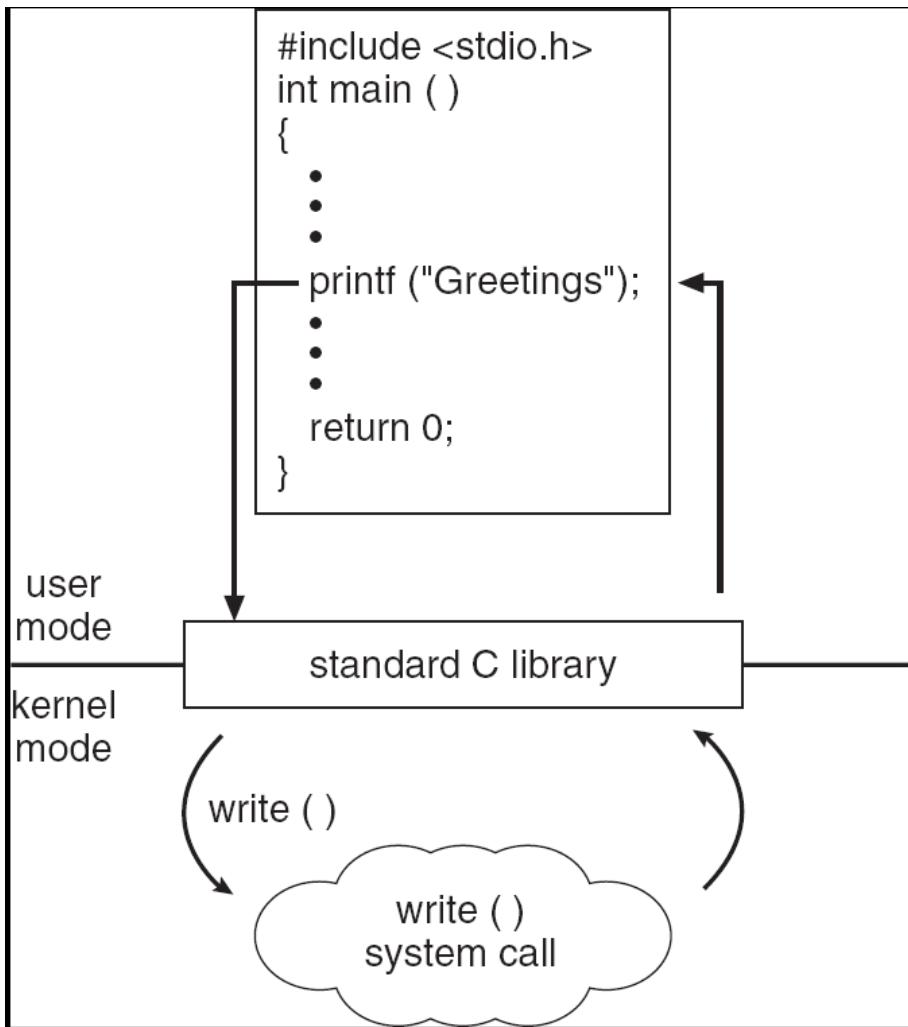
- Per ciascun linguaggio importante, il s.o. fornisce API di sistema da usare.
  - Cambiando il sistema operativo oppure cambiando il processore (CPU) su cui il sistema operativo si appoggia, i nomi delle funzioni delle API rimangono gli stessi ma cambia il modo di invocare le system call, quindi cambia l'implementazione delle funzioni delle API per adattarle alle system call e all'hardware.
  - Perché è importante programmare usando linguaggi di alto livello (es C)  
**Un programma sorgente in linguaggio C che usa le API non deve essere modificato se cambio il sistema operativo o l'hardware (e questi mantengono le stesse API), poiché sul nuovo s.o. cambia l'implementazione delle API e quindi cambia l'eseguibile che viene generato su diversi s.o ed hardware.**
- Alcune API molto diffuse sono:
  - Win32 API per Windows
  - **POSIX API per sistemi POSIX-based (tutte le versioni di UNIX, Linux, Mac OS X)**
  - Java API per la Java Virtual Machine (JVM).
- Possono esistere anche librerie messe a disposizione non dal sistema operativo bensì realizzate, ad esempio, da un utente.
- Solitamente tali librerie applicative sono implementate utilizzando le librerie di sistema.

# Linguaggi utilizzati e interfacce di servizio



# Esempio con la libreria standard C

- Per Linux, la libreria standard del linguaggio C (il *run-time support system*) fornisce una parte dell'API



- Programma C che invoca la funzione di libreria per la stampa *printf()*
- La libreria C implementa la funzione e invoca la system call *write()* nel modo richiesto dallo specifico s.o. e dalla specifica CPU.
- La libreria riceve il valore restituito dalla chiamata al sistema e lo passa al programma utente

# Quali system call utilizza un eseguibile?

## strace

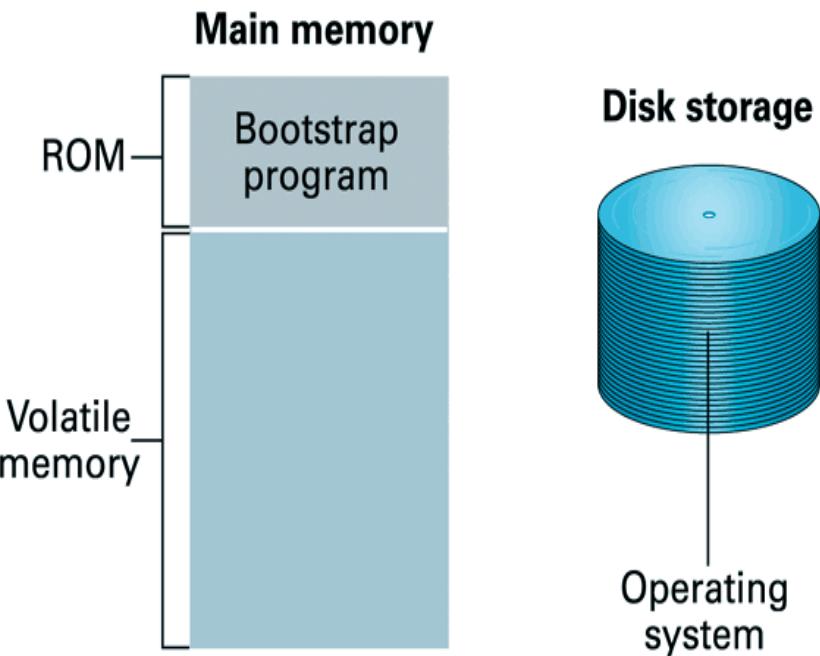
- In Linux esiste un comando che permette di vedere quali system call sono usate da un programma in esecuzione.
- **strace** esegue il comando specificato come argomento fino a che questo termina. Intercetta e visualizza le system calls che sono chiamate dal processo e i segnali che sono ricevuti dal processo.

Facciamo un esempio: lanciando il comando ifconfig visualizzo lo stato delle interfacce di rete. Vediamo quali syscall usa ifconfig eseguendo il comando:

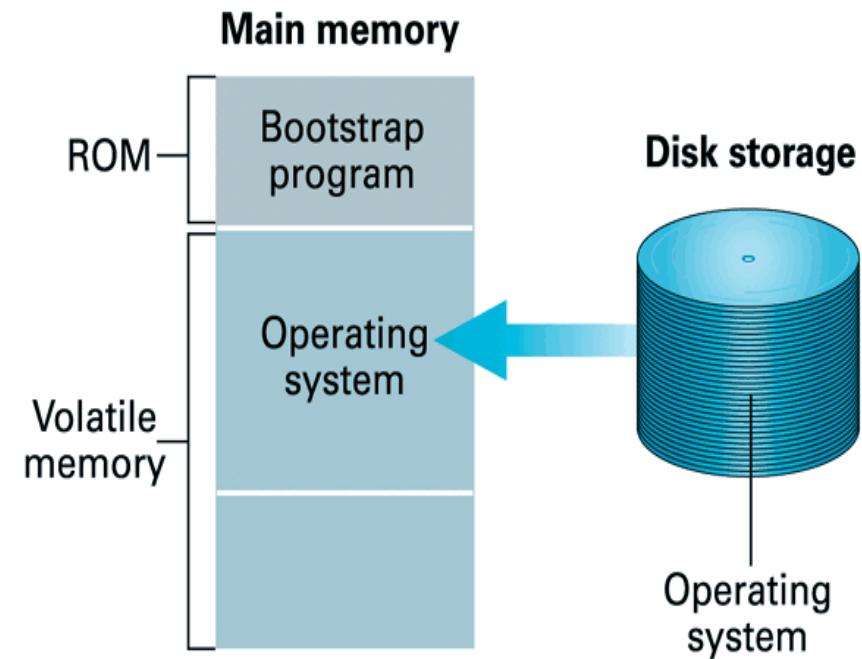
**strace** ifconfig

```
execve("/sbin/ifconfig", ["ifconfig"], /* 52 vars */) = 0
brk(NULL)                      = 0x12f3000
access("/etc/ld.so.nohwcap", F_OK) = -1 ENOENT (No such file or directory)
mmap(NULL,           8192,          PROT_READ|PROT_WRITE,
      MAP_PRIVATE|MAP_ANONYMOUS, -1, 0) = 0x7f37cb8ee000
access("/etc/ld.so.preload", R_OK) = -1 ENOENT (No such file or directory)
open("/etc/ld.so.cache", O_RDONLY|O_CLOEXEC) = 3
fstat(3, {st_mode=S_IFREG|0644, st_size=71665, ...}) = 0
mmap(NULL, 71665, PROT_READ, MAP_PRIVATE, 3, 0) = 0x7f37cb8dc000
close(3)
```

# L'avvio del sistema operativo - Bootstrap



**Step 1:** Machine starts by executing the bootstrap program already in memory. Operating system is stored in mass storage.



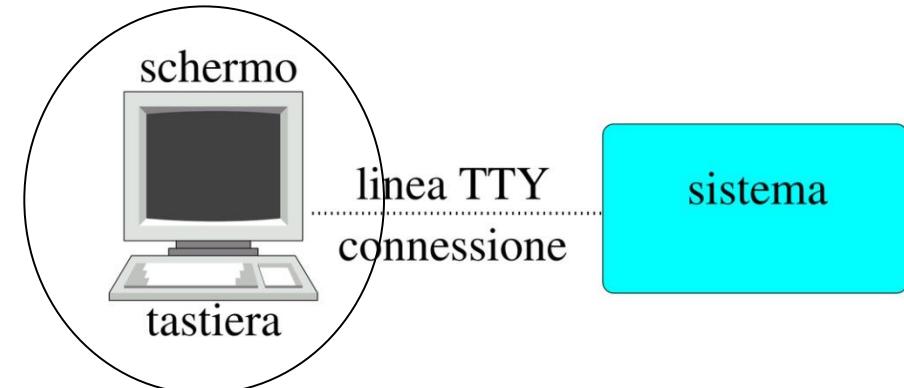
**Step 2:** Bootstrap program directs the transfer of the operating system into main memory and then transfers control to it.

# Servizi del Sistema Operativo

- ✿ **Gestione di Risorse:** allocazione, contabilizzazione, protezione e sicurezza (possessori di informazione devono essere garantiti da accessi indesiderati ai propri dati; processi concorrenti non devono interferire fra loro).
- ✿ Comunicazioni (intra e inter-computer)
- ✿ Rilevamento di errori che possono verificarsi nella CPU e nella memoria, nei dispositivi di I/O o durante l'esecuzione di programmi utente
- ✿ Gestione del **file system** — capacità dei programmi e dell'utente di leggere, scrivere e cancellare file e muoversi nella struttura delle directory
- ✿ Operazioni di I/O — il SO fornisce ai programmi utente i mezzi per effettuare l'I/O su file o periferica
- ✿ **Esecuzione di programmi** — capacità di caricare un programma in memoria ed eseguirlo, eventualmente rilevando e gestendo, situazioni di errore
- ✿ **Programmi di sistema**
- ✿ **Chiamate di sistema**
- ✿ **Interfaccia utente: a linea di comando** (*Command Line Interface, CLI*) o grafica (*Graphic User Interface, GUI*).

# Console = terminale = schermo + tastiera

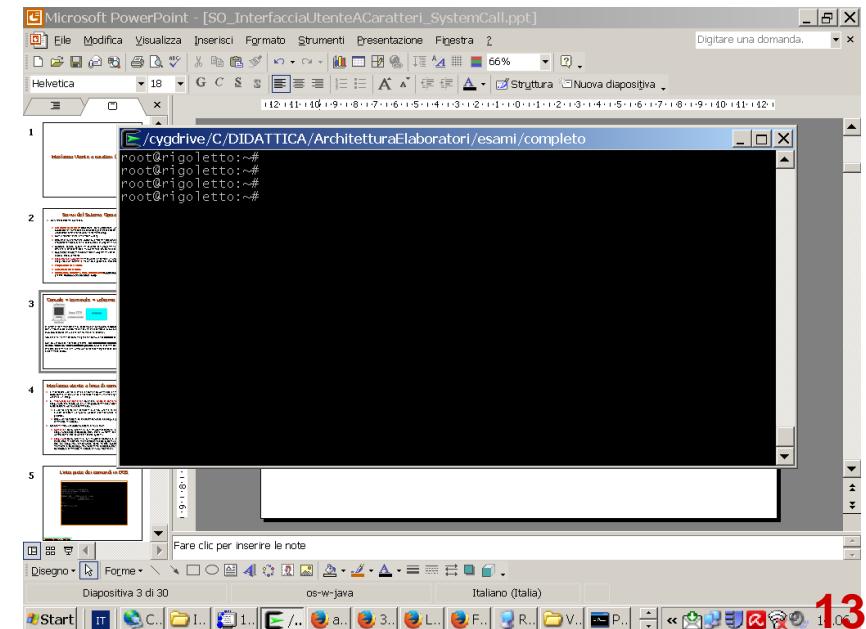
In origine i terminali (schermo+tastiera) erano **dispositivi separati** dal computer vero e proprio (detto mainframe) e comunicavano con questo mediante una linea seriale. L'output verso l'utente era di tipo solo testuale, l'input era fornito mediante tastiera.



Attualmente i terminali sono integrati nei computer (**schermo e tastiera del PC**).

Con l'avvento delle interfacce grafiche, **lo schermo del terminale viene emulato in una “finestra” dell’ambiente grafico**.

Si parla di terminale virtuale. Quando la finestra del terminale è in primo piano i caratteri digitati dalla tastiera vengono passati al terminale stesso.



# Interfaccia utente a linea di comando (CLI)

- L'interfaccia utente a linea di comando permette di impartire ordini al SO sotto forma di sequenze di caratteri alfa-numerici digitati sulla tastiera (o presi da un file).
- L' **interprete dei comandi** (o anche **Shell di comandi**) è un programma eseguibile che si occupa di un singolo terminale. Attende i caratteri digitati sulla tastiera per quel terminale.
  - L'utente digita dei caratteri, quando preme il tasto di invio (return) questi caratteri vengono passati all'interprete dei comandi che li gestisce.
  - Ricevuti i caratteri, la shell li interpreta ed esegue gli ordini ricevuti, poi si rimette in attesa di nuovi ordini.
- La shell e' programmabile perché al prompt è possibile passare uno script, ovvero una sequenza di ordini da eseguire.
- Gli ordini ricevuti possono essere di due tipi:
  - **Comandi** sono ordini la cui implementazione è contenuta nel file eseguibile della shell stessa (comandi built-in della shell). Non li troviamo perciò come file separati nel file system. Ad esempio il comando **cd**
  - **Eseguibili** sono ordini la cui implementazione è contenuta fuori della shell, cioè in altri file memorizzati nel file system. L'ordine è il nome del file da eseguire. L'interprete cerca il file specificato, lo carica in memoria e lo fa eseguire. Al termine dell'esecuzione la shell riprende il controllo e si rimette in attesa di nuovi comandi.

# L'interprete dei comandi in alcuni s.o.

- ✿ Unix, Linux:
  - ✿ Diverse Shell di comandi, tra le più utilizzate **bash** (bourne again shell).
- Windows:
  - Shell DOS
  - Emulazione di interfaccia testuale Linux: bash realizzata dalla piattaforma cygwin. Utile per far eseguire, in ambiente windows, applicazioni e servizi implementati per Linux.
  - In Windows 10 è stata aggiunta una bash (non completissima)
- Mac:
  - Diverse Shell di comandi, compresa **bash**

---
- Nel corso di sistemi operativi utilizzeremo compilatori con sola interfaccia testuale, in particolare il GNU C Compiler (gcc).
- Gli ordini al compilatore, così come l'ordine di eseguire un programma, verranno impartiti utilizzando una shell bash.
  - In Linux e su Mac esiste già un terminale con shell bash.
  - In Windows è perciò necessario installare l'emulatore cygwin oppure installare una macchina virtuale Linux.

# Interfaccia utente GUI

- ✿ Interfaccia user-friendly che realizza la metafora della scrivania (**desktop**)
  - ✖ Interazione semplice via mouse
  - ✖ Le **icone** rappresentano file, directory, programmi, azioni, etc.
  - ✖ I diversi tasti del mouse, posizionato su oggetti differenti, provocano diversi tipi di azione (forniscono informazioni sull'oggetto in questione, eseguono funzioni tipiche dell'oggetto, aprono directory – **folder**, o **cartelle**, nel gergo GUI)

# Standard POSIX

## (Portable Operating System Interface)

E' una famiglia di standard sviluppato dall'IEEE

- **IEEE 1003.1 (POSIX.1)** Definizione delle system call (operating system interface) fruibili da linguaggio C
- IEEE 1003.2 (POSIX.2) Shell e utility
- IEEE 1003.7 (POSIX.7) System administration

Noi siamo interessati allo standard IEEE 1003.1 (POSIX.1)

- POSIX.1 1988 Original standard
- POSIX.1 1990 Revised text
- POSIX.1a 1993 Addendum
- POSIX.1b 1993 Real-time extensions
- POSIX.1c 1996 Thread extensions

**POSIX.1 include alcune primitive della C Standard Library**

**POSIX.1 include alcune primitive non appartenenti alla C Standard Library**

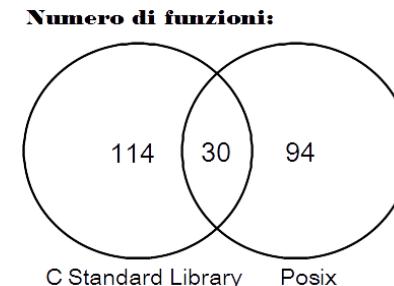
**Non tutte le primitive della C Standard Library appartengono a POSIX.1**

**Esempio:**

**open()** e' **POSIX.1**

**fopen()** e' **Standard C e POSIX.1**

**sin()** e' **Standard C**



# Standard C conforme a POSIX

## Portabilità:

Un sorgente C Standard conforme a POSIX può essere eseguito, una volta ricompilato, su qualunque sistema POSIX dotato di un ambiente di programmazione C Standard.

**Per scrivere un programma conforme a POSIX, bisogna includere gli header files richiesti dalle varie primitive usate, scelti fra:**

- header files della C Standard Library (contenenti opportune modifiche POSIX)
- header files specifici POSIX

Per ottenere la lista completa degli header necessari ad utilizzare ciascuna primitiva, utilizzate **man nome\_primitiva**

## Inoltre:

Se vogliamo compilare un programma in modo tale che dipenda solo dallo standard POSIX nella sua versione originaria (IEEE Std 1003.1) , dobbiamo inserire prima degli **#include**:

**#define \_POSIX\_SOURCE 1**

**/\* significa IEEE Std 1003.1 \*/**

# Standard C conforme a versioni specifiche di POSIX

## Portabilità:

Se vogliamo compilare un programma in modo tale che utilizzi solo funzioni aderenti allo standard POSIX, e in particolare ad una versione specifica dello standard POSIX, dobbiamo inserire un simbolo che identifica la particolare versione POSIX di nostro interesse.

Per la versione base di POSIX, prima degli #include dobbiamo inserire:

```
#define _POSIX_SOURCE 1 /* significa IEEE Std 1003.1 */
```

oppure, per aderire a specifiche versioni POSIX, dobbiamo inserire il simbolo

```
#define _POSIX_C_SOURCE VALORE
```

dove VALORE sara' uno dei seguenti

If ==1, like \_POSIX\_SOURCE; if >=2 add IEEE Std 1003.2;

    if >=199309L, add IEEE Std 1003.1b-1993;

    If >=199506L, add IEEE Std 1003.1c-1995;

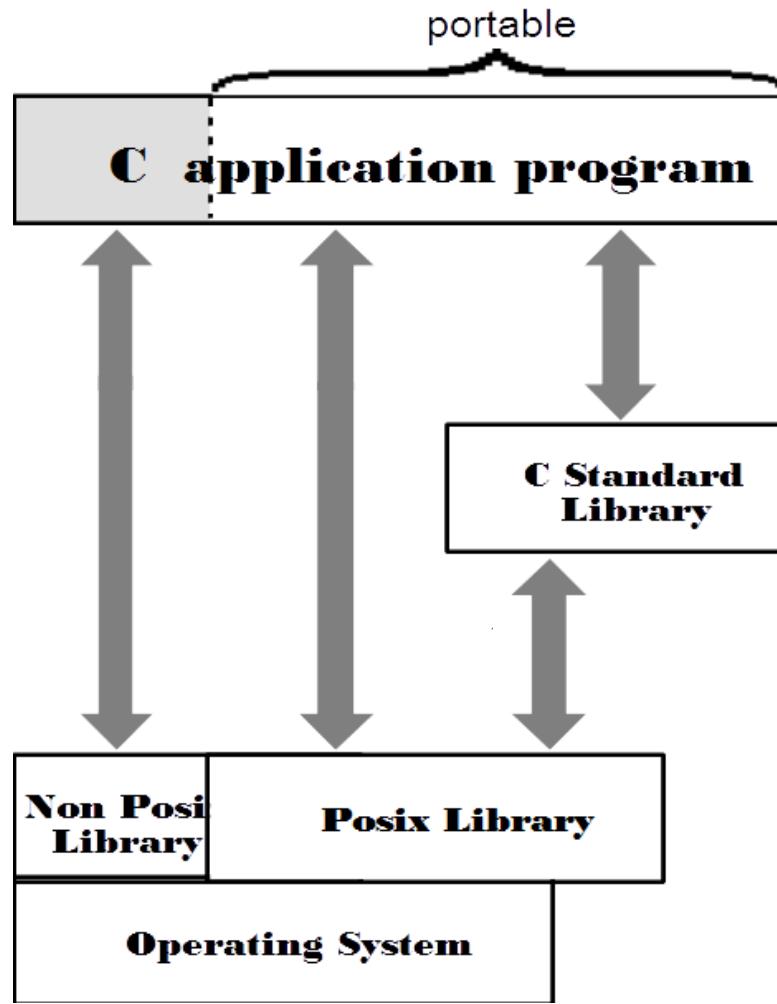
    if >=200112L, all of IEEE 1003.1-2004

if >=200809L, all of IEEE 1003.1-2008

\_POSIX\_C\_SOURCE 1 equivale a \_POSIX\_SOURCE 1

( info tratte da /usr/include/features.h )

# Standard C conforme a POSIX



# Tipi Primitivi di POSIX

## Tipi di dato interi :

definiti negli header **stdint.h** e **inttypes.h** (quest'ultimo offre alcune macro)

**int8\_t    int16\_t    int32\_t    uint8\_t    uint16\_t    uint32\_t**

**intptr\_t    uintptr\_t** (questi 2 sono interi con dimensione uguale ai puntatori ad intero)

Lo header **sys/types.h** definisce i tipi dei **dati di sistema** primitivi (dipendenti dall'implementazione del sistema). Definiti per garantire portabilita'. Sono definiti tramite **typedef**.

## Alcuni dei primitive system data types

<b>clock_t</b>	counter of clock ticks
<b>dev_t</b>	device numbers
<b>fd_set</b>	file descriptor set
<b>fpos_t</b>	file position
<b>gid_t</b>	group id
<b>ino_t</b>	inode number
<b>mode_t</b>	file types, file creation mode
<b>nlink_t</b>	number of hard links
<b>off_t</b>	offset
<b>pid_t</b>	process id
<b>size_t</b>	dimensioni (unsigned)
<b>ssize_t</b>	count of bytes (signed) (read, write)
<b>time_t</b>	counter of seconds since the Epoch
<b>uid_t</b>	user id

# Nozioni per l'uso del Terminale: File system (1)

Il filesystem è la organizzazione del disco rigido che permette di contenere i file e le loro informazioni.

Lo spazio di ciascun disco rigido è suddiviso in una o più parti dette partizioni.

Le partizioni contengono

- dei contenitori di dati detti files
- dei contenitori di files, detti directories (folders o cartelle in ambienti grafici)..

In realtà ciascuna directory può a sua volta contenere dei files e anche delle altre directories formando una struttura gerarchica

**In Windows** le partizioni del disco sono viste come logicamente separate e ciascuna e' indicata da una lettera (C; B; Z; ...).

Se un file si chiama pippo.c ed è contenuto in una directory che si chiama vittorio che a sua volta è contenuta in una directory che si chiama home che a sua volta è contenuta nella partizione chiamata C:, allora è possibile individuare univocamente il file pippo.c indicando il **percorso** mediante il quale, partendo dalla partizione C: si arriva al file pippo.c

**C:\home\vittorio\pippo.c** <- percorso per raggiungere pippo.c

Notare il carattere separatore \ (si chiama backslash) che indica dove inizia il nome di una directory o di un file.

# Nozioni per l'uso del Terminale: File system (2)

In Linux/Mac invece le partizioni sono viste come collegate tra loro.

Esiste una partizione principale il cui nome è / (slash).

Questa partizione, così come le altre partizioni, può contenere files e directories. Le directoryes possono contenere files e directories.

Se un file si chiama primo.c ed è contenuto in una directory che si chiama vittorio che a sua volta è contenuta in una directory che si chiama home che a sua volta è contenuta nella partizione principale, allora è possibile individuare univocamente il file pippo.c indicando il **percorso** mediante il quale, partendo dalla partizione / si arriva al file primo.c  
**/home/vittorio/primo.c**      <- percorso per raggiungere primo.c

Notare il carattere separatore / (slash) che indica dove inizia il nome di una directory o di un file. Quando il separatore / è all'inizio del percorso invece indica l'inizio della partizione principale, inizio che viene detto **root**..

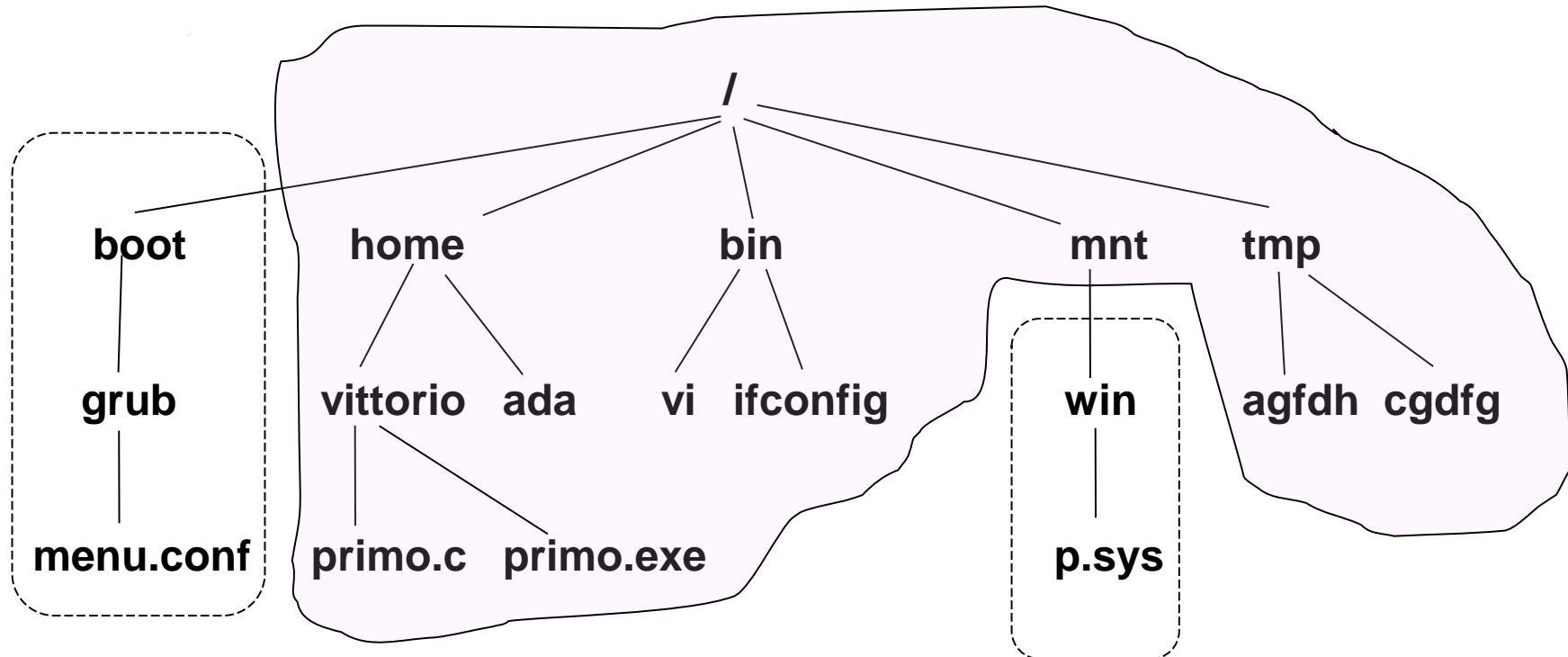
Le partizioni diverse da quella principale, si innestano (si collegano) logicamente in una qualche directory della partizione principale..

Ad esembio, una partizione chiamata boot può innestarsi direttamente nell'origine della partizione principale. Se questa partizione contiene una directory grub e quella directory contiene un file menu.conf, allora il percorso per identificare quel file menu.conf sarà:

**/boot/grub/menu.conf**      <- percorso per raggiungere il file.conf

Notare che non si capisce se un nome indica una directory o una partizione. **30**

# Nozioni per l'uso del Terminale: File system (3)



Esempio di strutturazione in directories e files delle partizioni di un filesystem Linux:

Nell'esempio, alla partizione principale **/** sono collegate (teoricamente si dice **montate**) altre due partizioni (circondate dalle linee tratteggiate) di nome **boot** e **win..**.

Notate che mentre la partizione boot è montata direttamente come fosse una directory contenuta nella directory di inizio (detta root) della partizione principale (**/**), la partizione win è montata in una sottodirectory della root.

# Nozioni per l'uso del Terminale: File system (4)

Nei sistemi **Linux/Mac** ciascun utente di un computer ha a disposizione dello spazio su disco per contenere i suoi files.

Per ciascun utente esiste, di solito, una directory in cui sono contenuti i files (intesi come directories e files) di quell'utente.

Quella directory viene detta **home dell'utente**.

Per esempio, nei pc dei laboratori del corso di laurea in Informatica di Bologna, la home dell'utente “rossi” si trova in **/home/students/rossi**

Per accedere ad un computer ciascun utente deve utilizzare farsi riconoscere mediante un nome utente (**account**) e autenticarsi mediante una **password**. L'operazione iniziale con cui l'utente si autentica per accedere ad un pc si dice **login**.

L'autenticazione degli utenti permette che il sistema operativo protegga i files di un utente impedendo l'accesso da parte di altri utenti o di persone esterne. Ciascun utente può vedere quali sono i permessi di accesso ai propri files ed eventualmente modificarli.

# Nozioni per l'uso del Terminale: File system (5)

Nel momento in cui si accede al terminale a riga di comando di un computer, il terminale **stabilisce la posizione logica attuale dell'utente all'interno del filesystem**, collocandolo inizialmente nella propria home directory.

Durante il lavoro l'utente può spostare la propria **posizione logica** in una diversa directory del filesystem.

NOTA BENE: spostarsi logicamente in una diversa directory VUOL DIRE VISITARE quella diversa directory e NON VUOL DIRE TRASFERIRE I PROPRI FILES IN QUELLA DIRECTORY

La directory in cui l'utente si trova logicamente in questo momento viene detta **directory corrente** e si dice che l'utente “**si trova nella**” directory corrente.

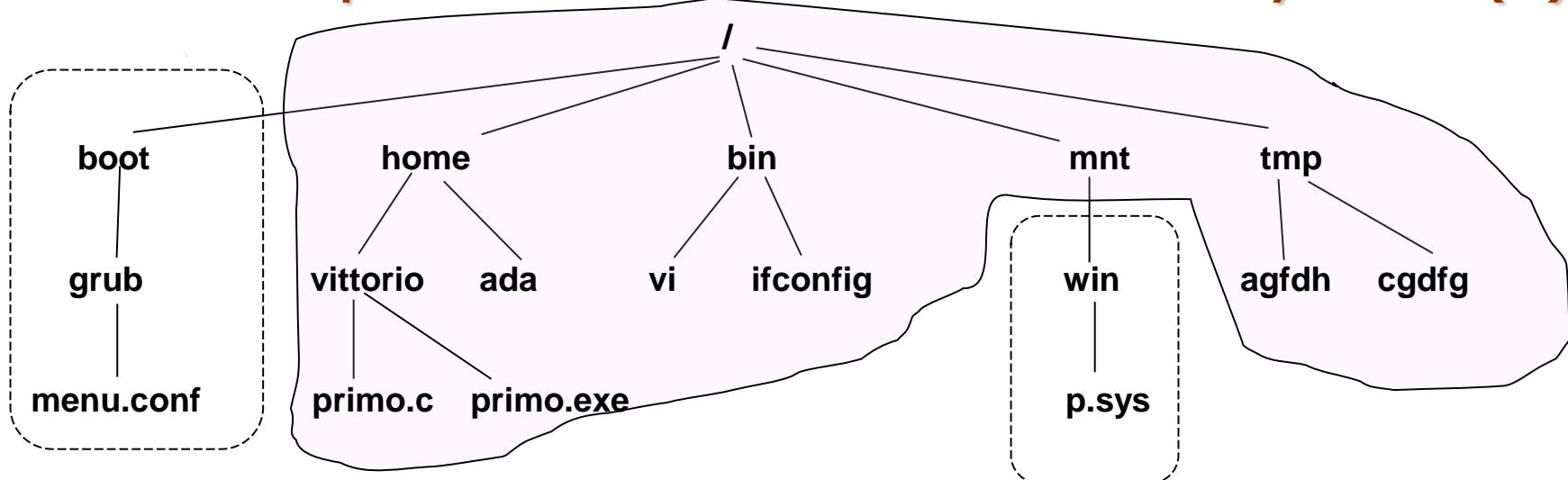
L'utente, per sapere in quale directory si trova logicamente in questo momento può eseguire il comando **pwd**, digitandolo da tastiera per farlo eseguire alla shell. Il comando pwd visualizza sullo schermo il percorso completo da / fino alla directory in cui l'utente si trova in quel momento.

```
# pwd  
/home/students/rossi/merda
```

Per spostarsi logicamente in una diversa directory, l'utente usa il comando **cd**

```
# cd /var/log
```

# Nozioni per l'uso del Terminale: File system (6)



Supponiamo di trovarci logicamente nella directory /home/vittorio

Per spostarmi logicamente nella directory /home posso usare cd in tre modi diversi

cd /home <- specifico percorso assoluto

cd .. <- specifico percorso relativo cioè partendo  
dalla directory corrente

Si noti che **il simbolo .. indica la directory superiore**

Per spostarmi dalla directory /home/vittorio alla directory /mnt/win

cd /mnt/win <- specifico percorso assoluto

cd ../../mnt/win <- specifico percorso relativo

Per spostarmi dalla directory /boot alla directory /boot/grub

cd /boot/grub <- specifico il percorso assoluto

cd ./grub <- specifico percorso relativo (**il simbolo . è la directory corrente**)

cd grub <- specifico percorso relativo (più semplice)

# FHS – Filesystem Hierarchy Standard

Attualmente versione 3.0.

Specifiche disponibili presso Linux Foundation.

[http://refspecs.linuxfoundation.org/FHS\\_3.0/fhs-3.0.pdf](http://refspecs.linuxfoundation.org/FHS_3.0/fhs-3.0.pdf)

- Obiettivo: sapere dove siano posizionati files/directory e quale sia il loro utilizzo
- Vengono specificate un numero minimo di directory
- Per ciascuna Purpose, Requirements, Specific requirements

Directory richieste in /

bin	Essential command binaries
boot	Static files of the boot loader
dev	Device files
etc	Host-specific system configuration
lib	Essential shared libraries and kernel modules
media	Mount point for removable media
mnt	Mount point for mounting a filesystem temporarily
opt	Add-on application software packages
sbin	Essential system binaries
srv	Data for services provided by this system
tmp	Temporary files
usr	Secondary hierarchy

# Nozioni per uso del Terminale: Metacaratteri

## Caratteri speciali

ne vedremo l'uso andando avanti

>	>>	<	redirezione I/O
			pipe
*	?	[...]	wildcards
`	command	'	command substitution
;			esecuzione sequenziale
	&&		esecuzione condizionale
(...)			raggruppamento comandi
&			esecuzione in background
" "		,	quoting
#			commento (tranne un caso speciale)
\$			espansione di variabile
\			carattere di escape *
<<			“here document”

# Interpretazione dei comandi bash: Espansioni

La shell legge ciascuna riga di comando, e la interpreta eseguendo alcune operazioni. Alcune di queste servono a capire dove finisce un comando e dove inizia il successivo. Altre servono ad individuare le parole (word splitting) e a identificare le parole riservate del linguaggio e a identificare la presenza di costrutti linguistici for while if. Altre ancora sostituiscono (espandono) alcune parti della riga di comando con altre, interpretando caratteri speciali. Alcuni caratteri speciali però, disabilitano alcune espansioni. In generale, la shell comincia riconoscendo i caratteri speciali. Successivamente la shell opera alcune sostituzioni nella riga di comando, effettuando le cosiddette espansioni (expansion).

Le espansioni principali, elencate in ordine di effettuazione, sono:

- **history expansion** !123
- **brace expansion** a{damn,czk,bubu}e
- **tilde expansion** ~/nomedirectory
- **parameter and variable expansion** \$1 \$? \${!var}
- **arithmetic expansion** \$(( ))
- **command substitution** (effettuata da sinistra verso destra) ` `` \$( )
- **word splitting**
- **pathname expansion** \* ? [...]
- **quote removal** rimuove unquoted ' " non generate dalle precedenti espansioni

(In alcuni sistemi sono possibili process substitution).

Vedremo i dettagli di queste espansioni man mano andando avanti.

# Nozioni per uso del Terminale: comando echo

**anticipazione:** Il comando echo permette di visualizzare a video la sequenza dei caratteri scritti subito dopo la parola echo e **fino al primo carattere di andata a capolinea** (che è inserito digitando il tasto <INVIO> o <RETURN>).

Il comando

```
echo pippo pippa pippi
```

visualizza

```
    pippo pippa pippi
```

Se ho bisogno di far stampare a video anche caratteri speciali come **punti e virgola, andate a capo (per visualizzare su più righe)**, e altri, devo inserire sia prima che dopo la stringa da stampare il separatore “ doppio apice (non sono due caratteri apici ma il doppio apice, quello sopra il tasto col simbolo 2.

Esempio: 

```
echo "pippo ; pippa pippi"
```

Esercizio: All'interno di una shell far stampare a video su due linee diverse la stringa

```
pappa
```

```
ppero
```

Impossibile se non si usano i doppi apici

Soluzione: digitare (notando i doppi apici)

```
echo "pappa<INVIO>
```

```
ppero" <INVIO>
```

# Nozioni per uso del Terminale: Variabili e Variable expansion (1)

La shell dei comandi permette di usare delle **Variabili** che sono dei simboli dotati di un **nome** (che identifica la variabile) e di un **valore (che può essere cambiato)**.

Il nome è una sequenza di caratteri anche numerici, ad es: PATH, PS1, USER PPID.

Attenzione, maiuscole e minuscole sono considerate diverse. Ad es PaTH !=PATH

Il valore è anch'esso una sequenza di caratteri compresi caratteri numerici e simboli di punteggiatura, ad es: /usr:/usr/bin:/usr/sbin 17 i686-pc-cygwin

Si noti che anche se il valore è composto solo da cifre (caratteri numerici), si tratta sempre di una stringa di caratteri.

Le variabili di una shell possono essere stabilite e modificate sia dal sistema operativo sia dall'utente che usa quella shell.

Alcune variabili ( dette d'ambiente ) vengono impostate subito dal sistema operativo non appena viene iniziata l'esecuzione della shell (ad es la variabile PATH).

Altre variabili possono essere create ex-novo dall'utente in un qualunque momento dell'esecuzione della shell.

Le variabili possono essere usate quando si digitano degli ordini per la shell. La shell **riconosce i nomi delle variabili contenuti negli ordini digitati, e cambia il contenuto dell'ordine sostituendo al nome della variabile il valore della variabile.**

Affinchè la shell **distingua il nome di una variabile**, questa deve essere **preceduta** dalla coppia di caratteri \${ e seguita dal carattere } Se, all'interno dell'ordine digitato, il nome della variabile è seguito da spazi (caratteri "bianchi") non c'è pericolo di confondere la variabile con il resto dell'ordine e si possono omettere le parentesi graffe.

# Nozioni per uso del Terminale: Variabili (2)

## assegnamenti e **variable** (e parameter) **expansion**

Ricordando che il comando echo permette di visualizzare a video la sequenza dei caratteri scritti subito dopo la parola echo e fino al primo carattere di andata a capolinea (che è inserito digitando il tasto <INVIO> o <RETURN>).

NUM=MERDA definisco una variabile di nome NUM e valore MERDA

echo \${NUM} stampo a video la variabile NUM, si vedrà MERDA

echo \${NUM}X stampo a video la variabile NUM, seguita dal carattere X  
si vedrà MERDAX

echo \$NUM stampo a video la variabile NUM si vedrà MERDA

echo \$NUMX vorrei stampare a video la variabile NUM, ma non metto le parentesi graffe, così la shell non capisce dove finisce il nome della variabile e non sostituisce il valore al nome. Non viene visualizzato nulla

echo \$NUM X come prima, ma ora c'è uno spazio tra NUM e il carattere V  
così la shell capisce che il nome della variabile finisce dove comincia lo spazio e sostituisce il valore al nome.  
Viene visualizzato MERDA X

# Nozioni per uso del Terminale: Variabili (2bis)

## Nota Bene: Assegnazione di valore ad una variabile

Quando si assegna un valore ad una variabile, **NON SONO CONSENTITI SPAZI NE' PRIMA NE' DOPO IL SIMBOLO =**

**Assegnamento corretto senza spazi prima o dopo il =**

VARIABILE=contenuto

**Assegnamento sbagliato a causa di spazio PRIMA del simbolo =**

VARIABILE =contenuto

In questo caso la shell cerca di eseguire il comando avente nome VARIABILE passandogli come argomento la stringa =contenuto

Avrei lo stesso errore se lasciassi uno spazio ANCHE dopo l'uguale

VARIABILE = contenuto

**Assegnamento sbagliato a causa di spazio DOPO il simbolo =**

VARIABILE= contenuto

In questo caso la shell cerca di eseguire il comando avente nome **contenuto** costruendo per tale comando un nuovo ambiente di esecuzione in cui colloca una variabile vuota di nome VARIABILE (vedere slide piu' avanti).

# Nozioni per uso del Terminale: Variabili (3)

Esiste una **variabile d'ambiente** particolare e importantissima, detta **PATH**

Viene impostata dal sistema operativo già all'inizio dell'esecuzione della shell.

L'utente può cambiare il valore di questa variabile.

**La variabile PATH contiene una sequenza di percorsi assoluti nel filesystem di alcune directory in cui sono contenuti gli eseguibili.** I diversi percorsi sono separati dal carattere :

Esempio di valore di PATH /bin:/sbin:/usr/bin:/usr/local/bin:/home/vittorio

Questa PATH definisce i percorsi che portano alle directory seguenti

- /bin
- /sbin
- /usr/bin
- /usr/local/bin
- /home/vittorio

Quando io ordino alla shell di eseguire un certo file binario, chiamandolo per nome, ma senza specificare il percorso completo (assoluto o relativo) per raggiungere quel file, allora **la shell cerca quel file binario all'interno delle directory specificate dai percorsi che formano la variabile PATH, nell'ordine con cui i percorsi sono contenuti nella variabile PATH**, cioè nell'esempio prima in /bin poi in /sbin etc.etc.

- Quando la shell trova il file eseguibile lo esegue.
- Se il file eseguibile non viene trovato nelle directory specificate, la shell visualizza un errore e non esegue il file.

# Usare il Terminale a linea di comando (bash)

Per aprire il terminale a riga di comando Linux-like in ambiente grafico:

In Windows cercare e cliccare l'icona di “cygwin bash shell” o “cygwin terminal”.

In Linux e Mac cliccare sul menù “terminal” o “terminal emulator” o “console”.

Si aprirà una “finestra” grafica e comparirà una piccola segnalazione **lampeggiante (cursore)** che indica che la shell è pronta ad accettare dei caratteri da tastiera.

Ad ogni istante, la shell opera stando in una posizione (directory) del filesystem denominata **directory corrente**. All'inizio dell'esecuzione della shell, la directory corrente è la home directory dell'utente che esegue la shell stessa.

L'utente può cambiare la directory corrente utilizzando il comando **cd**.

Usando l'interfaccia utente a linea di comando possono essere eseguiti

- **comandi** (piu' precisamente **comandi built-in**). Sono implementati e inclusi nella shell stessa e quindi non esistono come file separati. Sono forniti dal sistema operativo. Ad esempio cd, if, for.
- **file binari eseguibili**. Sono file che contengono codice macchina e che si trovano nel filesystem. Possono essere forniti dal sistema operativo o dagli utenti. Ad esempio, ls, vi, tar, gcc, primo.exe.
- **script**. Sono file di testo che contengono una sequenza di nomi di comandi, binari e altri script che verranno eseguiti uno dopo l'altro. Possono essere forniti dal sistema operativo o dagli utenti. Ad esempio exemplo\_script.sh

Per essere eseguito, un file binario o uno script deve avere i **permessi di esecuzione**.

Un utente può impostare il permesso di esecuzione di un proprio file usando il comando chmod come segue:      **chmod u+x esempio\_script.sh**

# Utenti e Gruppi

Nei sistemi Unix/Linux esistono le astrazioni di utente (**user**) e gruppo di utenti (**group**).

- Un utente può corrispondere ad una persona umana oppure essere solo la rappresentazione di una entità usata per indicare chi è che esegue un servizio di sistema. Ad esempio lo user mysql che esegue il servizio del database mysql.
- Un utente (**user**) è caratterizzato da una stringa chiamata **username** che contiene il nome utente (studente, vic, syslog) e da un identificatore numerico chiamato **userID** entrambi univoci nel sistema.
- Un gruppo (**group**) è caratterizzato da una stringa chiamata **groupname** che contiene il nome del gruppo (staff, admin, ) e da un identificatore numerico chiamato **groupID** entrambi univoci nel sistema. Ciascun utente appartiene ad uno o più gruppi.
- Ciascun file (e ciascuna directory) del filesystem appartiene ad un utente (detto proprietario del file,owner) che normalmente è l'utente che ha creato quel file.
- Ciascun file (e ciascuna directory) è associata ad un gruppo.
- **Un utente può tentare di accedere ad un file**, chiedendo di leggere o modificare il contenuto di un file oppure di eseguire un file eseguibile, **anche se non è il proprietario del file**.
- Viene indicato col termine **effective user** un utente quando cerca di accedere ad un file: il termine permette di distinguere tra chi sta usando il file e chi ne è il proprietario.
- **Il proprietario di un file stabilisce chi può accedere a quel suo file**, configurando i permessi di accesso a quel file. **Il proprietario stabilisce**, distinguendoli, **i permessi assegnati al proprietario del file** (sé stesso), agli utenti appartenenti allo stesso gruppo del file e, infine, **a tutti gli altri**.

# Permessi di file e directory

Ogni file ha un **proprietario** (identificato da un numero intero univoco detto **userID**) ed un **gruppo** del proprietario (identificato da un intero detto **groupID**). Allo userID corrisponde una stringa username, e al groupID corrisponde una stringa groupname. Quando un utente crea un file, il s.o. assegna l'utente come proprietario del file appena creato. Il proprietario/creatore poi può cambiare il proprietario del file con il comando  
***chown nuovoproprietario nomefile***

Ciascun file mantiene diversi diritti di lettura, scrittura ed esecuzione assegnati al proprietario, al gruppo del proprietario e a tutti gli altri.

Lettura (valore **4**, simbolo **r**)

File: lettura

Directory: elenco file/directory nella cartella (non le proprietà di file e directory)

Scrittura (valore **2**, simbolo **w**)

File: modifica

Directory: creazione, eliminazione, cambio nome file

Esecuzione (valore **1**, simbolo **x**)

File: esecuzione

Directory: accesso all'interno della directory e proprietà di suoi file e directory

user			group			others		
R 4	W 2	X 1	R 4	W 2	X 1	R 4	W 2	X 1

Comandi per cambiare proprietario, gruppo e permessi: ***chown, chgrp, chmod***

Solo il proprietario del file può cambiare proprietario, gruppo e permessi del file.

# Permessi di file e directory

Se un utente (detto user ID effettivo) vuole accedere ad un file, si applicano i seguenti criteri di utilizzo basati sui permessi di quel file

- Se l'utente (user ID effettivo) che vuole accedere ad un file è il proprietario del file, si applicano le User permission.
- Altrimenti, se il group ID effettivo corrisponde al group ID del file, si applicano le Group permission
- Altrimenti, si applicano le Other permission

user			group			others		
R 4	W 2	X 1	R 4	W 2	X 1	R 4	W 2	X 1

Solo il proprietario del file può cambiare proprietario, gruppo e permessi del proprio file.  
Comandi per cambiare proprietario, gruppo e permessi: *chown, chgrp, chmod*

Esempio di assegnazione contemporanea di permessi **mediante formato numerico:**  
assegnazione contemporanea di permessi

per owner (lettura, scrittura e esecuzione: 7),  
per group (lettura e scrittura: 6)  
e per other (sola lettura: 4)

**chmod 764 ./miofile.txt**

# Visualizzazione Permessi di file e directory

Lanciamo il comando **ls -al** nella nostra home directory per vedere tutte le informazioni (opzione -l) e quindi anche i permessi, di tutti i file (opzione -a).

```
ls -alh /home/vic/
```

Otteniamo come output:

```
drwxr-xr-x      34 vic  vic   4096 set 25 10:55 .
drwxr-xr-x  3  root root  4096 dic  9 2015 ..
-rw-r--r--  1 vic  vic  3826 giu 16 16:21 .bashrc
-rw-rw-r--  1 vic  vic    158 dic 17 2015 main.c
-rwxrwxr-x  1 vic  vic  8608 dic 17 2015 main.exe
```

Guardiamo i permessi dell'eseguibile che permette di cambiare la propria password.

```
ls -alh /usr/bin/passwd
```

Otteniamo come output:

```
-rwsr-xr-x  1 root root  51K lug 22 2015 /usr/bin/passwd
```

Notare la s **nella parte di permessi utente**, che sostituisce la x di esecuzione.

Dice che quando quell'eseguibile viene eseguito da qualcuno che puo' eseguirlo, il processo creato dall'eseguibile esegue con i permessi di chi lo ha lanciato, **ma anche con i permessi del proprietario dell'eseguibile** (root, nel nostro esempio). Serve per effettuare operazioni con i permessi dell'amministratore di sistema.

## Special Permissions

setuid	setgid	sticky
4	2	1

# Permessi speciali di file e directory

setuid - rappresentato da "s" (o da "S") nelle user permissions (settato s con chmod 4\*\*\* )

File: in esecuzione, il processo associato all'esecuzione del file ottiene anche i diritti dell'owner (l'effective uid diventa quello dell'owner del file).

Tipicamente root. Esempio del comando /usr/bin/passwd

Directory: ignorato

esempio di settaggio setuid per proprietario: `chmod u+s ./miofile`

altro esempio di settaggio numerico di setuid e altri permessi: il 4 all'inizio e' setuid

`vic@vic:~$ chmod 4761 ./main.exe`

`vic@vic:~$ ls -alh main.exe`

`-rwsrw--x 1 vic vic 8,5K dic 17 2015 main.exe`

setgid - rappresentato da "s" (o da "S") nelle group permissions (settato con chmod 2\*\*\*)

File: analogo al setuid ma per il gruppo (è l'effective gid che diventa quello del file)

Directory: implica che i nuovi file e subdirectory create all'interno della directory ereditino il gid della directory stessa (e non quello del gruppo principale dell'utente che lo ha creato). Esempio di una directory condivisa

sticky bit - rappresentato da "t" (o da "T") (settato con chmod 1\*\*\*)

File: ora ignorato

Directory: i file all'interno di una directory con sticky bit possono essere rinominati o cancellati solo dal proprietario del file, dal proprietario della directory...o da root, ovviamente!

# Esempi di cambio permessi speciali (setuid)

```
vic@vic:~$ ls -alh main.exe  
-rwxrwxr-x 1 vic vic 8,5K dic 17 2015 main.exe
```

```
vic@vic:~$ chmod u+s ./main.exe  
vic@vic:~$ ls -alh main.exe  
-rwsrwxr-x 1 vic vic 8,5K dic 17 2015 main.exe
```

```
vic@vic:~$ chmod u-s ./main.exe  
vic@vic:~$ ls -alh main.exe  
-rwxrwxr-x 1 vic vic 8,5K dic 17 2015 main.exe
```

NOTARE LE DIFFERENZE TRA s ed S

- |   |  |
|---|--|
| s | setuid e permesso di esecuzione valore 4   |
| S | setuid SENZA permesso di esecuzione. Controsenso.<br>INCONISISTENZA. Non posso eseguire il file. |

```
vic@vic:~$ chmod 4666 ./main.exe          NB: NON ho dato permessi esecuzione a owner  
vic@vic:~$ ls -alh main.exe  
-rwSr-wr- 1 vic vic 8,5K dic 17 2015 main.exe
```

NOTARE QUI SOTTO CHE NON POSSO ASSEGNAME S

La visualizzazione di S, è solo una conseguenza dell'inconsistenza tra x ed s

```
vic@vic:~$ chmod u+S ./main.exe          PROVOCA ERRORE  
chmod: invalid mode: 'u+S'
```

Try 'chmod --help' for more information.

ANALOGA DIFFERENZA SUSSISTE TRA "t" e "T" per quanto riguarda lo sticky bit

# Come eseguire da Terminale a linea di comando

## Come specificare il nome del comando o dell'eseguibile?

I **comandi** possono essere eseguiti semplicemente invocandone il nome. (es: cd ../ )

I **file eseguibili (binari o script)** devono invece essere invocati specificandone

- o **il percorso assoluto** (a partire dalla root)  
ad es per eseguire primo.exe digitò /home/vittorio/primo.exe
- oppure **il percorso relativo** (a partire dalla directory corrente)  
se la directory corrente è /home/ada allora digitò ../../vittorio/primo.exe
- oppure **il solo nome, a condizione che quel file sia contenuto in una directory specificata nella variabile d'ambiente PATH**

Ad esempio, se la variabile PATH è /bin:/usr/bin:/home/vittorio:/usr/local/bin  
allora qualunque sia la directory corrente, per eseguire il file /home/vittorio/primo.exe  
basta digitare il solo nome del file primo.exe

Esercizio:

Se la directory corrente è /home/vittorio ma quella directory non si trova nella variabile PATH, allora come posso eseguire il file primo.exe, che si trova in quella directory, specificando il percorso relativo?

./primo.exe

# Subshell

**Una subshell e' una shell (shell figlia) creata da un'altra shell (shell padre).**

**IMPORTANTE: Una subshell viene creata in caso di:**

- Esecuzione di comandi **raggruppati** (vedi dopo).
- Esecuzione di **script**.
- Esecuzione di processo in **background** (vedi dopo).
- **NB:** l'esecuzione di un comando built-in avviene nella stessa shell padre

Ogni shell ha una propria directory corrente (ereditata dalla shell padre).

Ogni shell ha delle proprie variabili.

Ogni subshell eredita dalla shell padre una copia delle variabili d'ambiente (vedi dopo).

Ogni subshell non eredita le variabili locali della shell padre.

**Quando una shell deve eseguire uno script esegue queste operazioni:**

- Legge la prima riga dello script in cui è indicato quale interprete di comandi deve eseguire lo script  
es: `#!/bin/bash`
- **Crea una subshell**
- Il nome dello script viene passato come argomento (opzione `-c`) alla nuova subshell
- La nuova subshell esegue lo script.
- Alla fine dell'esecuzione dello script la subshell termina e restituisce il controllo alla shell padre, restituendo un valore intero che indica il risultato.

# Nozioni per uso del Terminale: Variabili (4)

Ogni shell supporta due tipi di variabili

## Variabili locali

Non “trasmesse” da una shell alle subshell da essa create

Utilizzate per computazioni locali all'interno di uno script

## Variabili di ambiente

“Trasmesse” dalla shell alle subshell.

Viene creata una copia della variabile per la subshell

Se la subshell modifica la sua copia della variabile,  
la variabile originale nella shell non cambia.

Soltamente utilizzate per la comunicazione fra parent e child shell

es: variabili \$HOME \$PATH \$USER %SHELL \$TERM

Per visualizzare l'**elenco delle variabili di ambiente**, utilizzare il comando **env** (ENVironment)

Quando dichiaro una variabile con la sintassi già vista dichiaro una variabile LOCALE.

**nomevariabile=ValoreVariabile**

Per trasformare una variabile locale già dichiarata in una variabile di ambiente, devo usare il comando **export** (notare che non uso il \$ )

**export nomevariabile**

Posso anche creare una variabile dichiarandola subito di ambiente

**export nomevariabile=ValoreVariabile**

# Nozioni per uso del Terminale: Variabili (5)

Esempio per esplicitare differenza tra var locali e var d'ambiente: ./var\_caller.sh

# var\_caller.sh

```
echo "caller"  
# setto la var locale PIPPO  
# la var d'ambiente PATH esiste già
```

```
PIPPO=ALFA  
echo "PATH = ${PATH}"  
echo "PIPPO = ${PIPPO}"
```

```
echo "calling subshell"
```

**./var\_called.sh**

```
echo "ancora dentro caller"  
echo "variabili sono state modificate ?"  
  
echo "PATH = ${PATH}"  
echo "PIPPO = ${PIPPO}"
```

# var\_called.sh

```
echo "called"  
echo "le variabili sono state passate ? "
```

```
echo "PATH = ${PATH}"  
echo "PIPPO = ${PIPPO}"
```

```
echo "modifico variabili "
```

```
PIPPO="${PIPPO}:MODIFICATO"  
PATH="${PATH}:MODIFICATO"
```

```
echo "PATH = ${PATH}"  
echo "PIPPO = ${PIPPO}"
```

```
echo "termina called"
```

# Nozioni per uso del Terminale: Variabili (6)

Quando invoco uno script,  
viene eseguita una nuova shell  
al termine dell'esecuzione quella shell viene eliminata

Per ogni eseguibile invocato,  
viene collocata in memoria una copia dell'ambiente di esecuzione,  
l'eseguibile può modificare il proprio ambiente,  
al termine dell'esecuzione l'ambiente viene eliminato dalla memoria.

# Script execution senza creazione di subshell

Normalmente, se una shell lancia uno script, questo viene eseguito in una subshell

- con l'interprete di comandi indicato nella prima riga speciale dello script `#!/bin/bash`, se esiste quella riga,
- o con lo stesso interprete della shell chiamante, se quella prima riga non esiste.

Se lo script modifica le proprie variabili, la shell padre non si accorge delle modifiche.

**Però, una shell puo' eseguire uno script senza creare la subshell in cui lo script dovrebbe essere eseguito.**

Come ?

**source nomescript**

Oppure

**▪ nomescript**

In tal modo non viene considerata la prima riga speciale dello script.

**A cosa serve? A modificare le variabili della shell padre mediante uno script.**

Le variabili modificate dallo script sono proprio quelle della shell (padre, o meglio unica) , quindi la shell vede modificate le proprie variabili.

**source** e **▪** sono due comandi built-in ovvero implementati all'interno della shell

# Script execution senza creazione di subshell (2)

Attenzione che il comando source va usato solo se siamo sicuri che all'interno dello script da eseguire ci sono dei comandi che possono essere correttamente interpretati dalla shell bash chiamante.

Se invochiamo con source uno script che necessita di un interprete diverso provochiamo dei problemi, poiché **non verrà lanciato l'interprete corretto indicato nella prima riga dello script**.

Ad esempio, se lo script perl **myperl.pl** contiene le seguenti 3 righe:

```
#!/usr/bin/perl
@famiglia = ("padre", "madre", "figlio", "figlia");
for ($i=0; $i<=#famiglia; $i++) { print "$famiglia[$i]\n"; }
```

ed io, all'interno di una bash, eseguo lo script con source

```
source ./myperl.pl
```

provoco degli errori perché non viene lanciato l'interprete /usr/bin/perl ed è la bash chiamante che cerca di interpretare i comandi perl

```
bash: ./myperl.pl: line 3: syntax error near unexpected token `('
bash: ./myperl.pl: line 3: `@famiglia = ("padre", "madre", "figlio", "figlia");'
```

# Nozioni per uso del Terminale: Variabili (7)

Esempio per esplicitare differenza tra var locali e var d'ambiente: ./var\_caller.sh

## # var\_caller2.sh

```
echo "caller"  
# setto la var locale PIPPO  
# la var d'ambiente PATH esiste già
```

```
PIPPO=ALFA  
echo "PATH = ${PATH}"  
echo "PIPPO = ${PIPPO}"
```

```
echo "calling subshell"
```

```
source ./var_called2.sh
```

```
echo "ancora dentro caller"  
echo "variabili sono state modificate ?"
```

```
echo "PATH = ${PATH}"  
echo "PIPPO = ${PIPPO}"  
echo "NUOVA= ${NUOVA}"
```

## # var\_called2.sh

```
echo "called"  
echo "le variabili sono state passate ? "
```

```
echo "PATH = ${PATH}"  
echo "PIPPO = ${PIPPO}"
```

```
echo "modifico variabili "
```

```
PIPPO="${PIPPO}:MODIFICATO"  
PATH="${PATH}:MODIFICATO"
```

```
echo "creo nuova variabile"  
NUOVA=NUOVOCONTENUTO
```

```
echo "PATH = ${PATH}"  
echo "PIPPO = ${PIPPO}"  
echo "NUOVA= ${NUOVA}"
```

```
echo "termina called"
```

```
# che accade se DEcommento qui sotto?  
# exit 13
```

# Nozioni per uso del Terminale: Variabili (8)

## Creazione di variabili d'ambiente da passare a subshell e Campo di visibilità di variabili

È possibile definire una o più variabili nell'ambiente (nella subshell) di un eseguibile che si sta per fare eseguire, senza farle ereditare a quelli successivi, semplicemente scrivendo le assegnazioni prima del nome del comando.

Per esempio:

```
var="stringa" comando          # comando vede e puo' usare var  
echo ${var}                      #echo non vede la variabile var
```

Attenzione, se esiste già una variabile d'ambiente con quello stesso nome, il comando lanciato vede solo la variabile nuova, alla fine del comando torna visibile la variabile vecchia.

Per esempio:

```
export var="contenutoiniziale"  
var="stringa" comando          # comando vede var che vale "stringa"  
echo ${var}                      #echo vede la variabile che vale "contenutoiniziale"
```

# Nozioni per uso del Terminale: Variabili (9)

Esempio per esplicitare creazione di variabili da passare a subshell

Notare che tali variabili diventano automaticamente **di ambiente per la subshell**

```
# init_var_caller3.sh
#!/bin/bash

VAR="contenutoiniziale"
# non cambia se lascio VAR locale
# o se la imposto come variab. di ambiente
# export VAR

echo "VAR = ${VAR}"

VAR="stringa" ./init_var_called.sh

# non cambia se lo chiamo con source
# provarlo anche cosi'
# VAR="stringa" source /init_var_called.sh

echo "VAR = ${VAR}"
```

```
# init_var_called.sh
#!/bin/bash

echo "la variabile e' stata passata ? "
echo "VAR = ${VAR}"

# Verifico se nuova VAR e' di ambiente
echo "env | grep VAR"
env | grep VAR
```

# Nozioni per uso del Terminale: Variabili (10)

## Variabili Vuote vs. Variabili non esistenti

C'e' differenza tra  
una variabile che esiste ma e' vuota  
ed una variabile che invece non esiste.

- Se una variabile non e' mai stata dichiarata allora non esiste.
- Se a una variabile e' stato assegnato come valore la stringa vuota "" allora esiste ma e' vuota.

Posso eliminare una variabile esistente (vuota o no) col comando **unset**  
**unset nomevariabile**

Dopo averla eliminata, quella variabile non esiste.

Attenzione, che una variabile vuota o non esistente puo' provocare errori sintattici a runtime negli script in cui si confronta il valore delle variabili.

[ \$var = "" ]      errore sintattico se \$var e' vuota oppure se non esiste  
                          e' come se ci fosse scritto                        [ = "" ]

Occorre sempre quotare il nome della variabile

[ "\$var" = "" ]      corretto sintatticamente se \$var e' vuota e anche se var non esiste  
[ \$var = "" ]      SBAGLIATO se var vuota o non esiste, come se fosse scritto [ = "" ]

[ -n "\$var" ]      # corretto , restituisce true se var non vuota, false se var vuota  
[ -n \$var ]      # SBAGLIATO perche' restituisce vero se var non esiste

# Nozioni per uso del Terminale: funzionalita' **history history expansion**

La funzionalita' **history** memorizza i comandi lanciati dalla shell e permette di visualizzarli ed eventualmente rilanciarli. La storia dei comandi viene mantenuta anche dopo la chiusura della shell.

Il comando built-in **history** visualizza un elenco numerato dei comandi precedentemente lanciati dalla shell, con numero crescente dal comando più vecchio verso il più recente. Il numero assegnato ad un comando quindi non cambia quando lancio altri comandi. Il numero serve a rilanciare quel comando.

<i>più vecchio</i>	180	ls
	181	./sizeof_vettore.exe
	182	clear
	183	cat sizeof_pached.c
	184	gcc -ansi -o sizeof_packed.exe sizeof_packed.d
<i>più recente</i>	185	./sizeof_packed.exe

Se lancio il comando **!NUMERO** eseguo il comando che nella history e' indicato col numero NUMERO. Se ad esempio lancio

**!181**

allora eseguo **./sizeof\_vettore.exe**

Se lancio il comando **!stringa** allora eseguo il comando più recentemente lanciato (cioè quello col numero più grande) che nella history inizia con stringa. Se ad esempio lancio

**!c**

allora eseguo **cat sizeof\_pached.c**

# Nozioni per uso del Terminale: Comando **set**

Il comando built-in **set** svolge diversi compiti:

**set** lanciato senza nessun parametro visualizza tutte le variabili della shell, sia quelle locali che quelle d'ambiente. Inoltre visualizza le funzioni implementate nella shell (le vedremo più avanti (forse)).

**set** lanciato con dei parametri serve a settare o resettare una opzione di comportamento della shell in cui viene lanciato.

Ad esempio

**set +o history** disabilita la memorizzazione di ulteriori comandi eseguiti nel file di history. I comandi lanciati prima della disabilitazione rimangono nel file di history.

**set -o history** abilita la memorizzazione dei comandi eseguiti mettendoli nel file di history.

**set -a** causa il fatto che le variabili create o modificate vengono immediatamente fatte diventare variabili d'ambiente e vengono ereditate dalle eventuali shell figlie.

**set +a** causa il fatto che le variabili create sono variabili locali. È il modo di default.

Vedere il comando **man set** per leggere tutte le possibili opzioni di comportamento della shell che possono essere attivate o disattivate col comando **set**.

Se il man non trova le info su set, installate il pacchetto manpages-posix-dev

# Nozioni per uso del Terminale: Comando **set**

## Risposta per Tarlo6 - Creare variabili locali dopo set -a

Dopo avere eseguito in una bash il comando **set -a**

le variabili create successivamente sono variabili di ambiente e non variabili locali.

Per configurare comunque una variabile affinché sia una variabile locale (non di ambiente) occorre utilizzare il comando **export** con il flag **-n**

Ad esempio, lanciando il seguente script **var\_callerLocale.sh**, in cui la variabile PLUTO viene dichiarata locale mediante il comando **export -n PLUTO** ottengo che la variabile PLUTO non esista nell'ambiente di esecuzione dello script **var\_calledLocale.sh** chiamato dal primo script. La variabile PLUTO non era di ambiente.

**var\_callerLocale.sh**

```
#!/bin/bash  
  
set -a  
PIPPO=pippo  
PLUTO=pluto  
echo "PIPPO = ${PIPPO}"  
echo "PLUTO = ${PLUTO}"  
  
export -n PLUTO  
. /var_calledLocal.sh
```

**var\_calledLocale.sh**

```
#!/bin/bash  
  
echo dentro  
var_calledLocal.sh  
  
echo "PIPPO = ${PIPPO}"  
echo "PLUTO = ${PLUTO}"
```

L'output  
dell'esecuzione  
è quello qui a destra:

PIPPO = pippo  
PLUTO = pluto  
PIPPO = pippo  
**PLUTO =** **64**

# Parametri a riga di comando passati al programma (1)

## Cosa sono gli argomenti o parametri a riga di comando di un programma

Sono un insieme ordinato di caratteri, separati da spazi, che vengono passati al programma che viene eseguito in una shell, nel momento iniziale in cui il programma viene lanciato.

Quando da una shell digito un comando da eseguire, gli argomenti devono perciò essere digitati assieme (e di seguito) al nome del programma per costituire l'ordine da dare alla shell. Ciascun argomento è separato dagli altri mediante uno o più spazi (carattere blank, la barra spaziatrice della tastiera).

Esempio:      chmod u+x /home/vittorio/primo.exe

L'intera stringa di caratteri **chmod u+x /home/vittorio/primo.exe** si chiama **riga di comando**

Il primo pezzo **chmod** è il nome dell'eseguibile (o anche **argomento di indice zero**). Ciascuno degli altri pezzi è un argomento o parametro.

Nell'esempio, il pezzo **u+x** è **l'argomento di indice 1**.

Nell'esempio, il pezzo **/home/vittorio/primo.exe** è **l'argomento di indice 2**.

Nell'esempio, si dice che il numero degli argomenti passati è **2**.

Il programma, una volta cominciata la propria esecuzione, ha modo di conoscere il numero degli argomenti che gli sono stati passati e di ottenere questi argomenti ed utilizzarli.

# Avvio della shell bash

**La shell bash si comporta in maniera diversa a seconda di quali argomenti a riga di comando le vengono passati nel momento in cui ne viene lanciata l'esecuzione.**

Distinguiamo 3 modi in cui può essere eseguita la bash:

## **shell non interattiva**

shell figlia che esegue script

lanciata con argomenti      **-c** percorso\_script\_da\_eseguire

## **shell interattiva NON di login**

quella che vediamo all'inizio nella finestra di terminale

lanciata senza nessuno degli argomenti    **-c**   **-l**   **--login**

## **shell interattiva di login**

è come la shell non di login, ma inizia chiedendo user e password

lanciata con argomenti    **-l**   oppure   **--login**

# shell bash interattiva "di login" o "non di login"

La shell interattiva bash si comporta inizialmente in due modi differenti a seconda di come viene lanciata cioe' a seconda di quali argomenti a riga di comando le vengono passati.

**Shell bash interattiva di login:** quando viene lanciata **con** una delle opzioni **-l** oppure **--login**.

La shell interattiva **di login**, nel momento in cui comincia la sua esecuzione, cerca di eseguire (se esistono) i seguenti files:

1. il file "/etc/profile"
2. poi uno solo (il primo che trova) tra i file ".bash\_profile", ".bash\_login" e ".profile" collocati nella home directory dell'utente e che risulti essere disponibile;
3. poi il file ".bashrc" collocato nella *home directory* dell'utente;

Nel momento in cui termina, la shell di login esegue il file .bash\_logout collocato nella home dell'utente (se il file esiste).

**Shell bash interattiva non di login:** quando viene lanciata **senza** alcuna delle due opzioni **-l** oppure **--login**.

La shell interattiva **non di login**, nel momento in cui comincia la sua esecuzione, cerca di eseguire (se esiste) il solo file ".bashrc" collocato nella *home directory* dell'utente.

Per entrambe le shell, l'utente puo' modificare i file di configurazione nella propria home directory, per customizzare il comportamento della shell.

# **shell bash "non interattiva"**

**La shell non interattiva bash è la shell lanciata per eseguire uno script.**

**Viene specificato un argomento –c nomescriptdaeseguire.**

**A differenza della shell interattiva, la shell non interattiva NON esegue i comandi contenuti in nessuno dei file (di sistema o dell'utente) che customizzano il comportamento della shell interattiva ( /etc/profile .bash\_profile .bash\_login .profile .bashrc ).**

# Parametri a riga di comando passati al programma (2)

## Separatore di comandi ; e Delimitatore di argomenti "

### Problema: Comandi Multipli su una stessa riga di comando

La bash permette che **in una stessa riga di comando possano essere scritti più comandi**, che verranno eseguiti uno dopo l'altro, **non appena termina un comando viene eseguito il successivo**.

Il carattere **;** è il **separatore tra comandi**, che stabilisce cioè dove finisce un comando e dove inizia il successivo.

Ad es: se voglio stampare a video la parola pippo e poi voglio cambiare la directory corrente andando in /tmp potrei scrivere in una sola riga i due seguenti comandi:

```
echo pippo ; cd /tmp
```

**Diventa però impossibile stampare a video frasi strane tipo: pippo ; cd /bin che contiene purtroppo il carattere di separazione ;**

Per farlo si include la frase completa tra doppi apici. Infatti, **il doppio apice " (double quote) serve a delimitare l'inizio e la fine di un argomento, così che il punto e virgola viene visto non come un delimitatore di comando ma come parte di un argomento.**

```
echo "pippo ; cd /tmp "
```

In questo modo si **visualizza** la frase **pippo ; cd /tmp** e non si cambia directory

## Parametri a riga di comando passati al programma (3)

### Quoting di stringhe " " e Quoting di singoli caratteri \

Consideriamo ancora il comando appena visto **echo " pippo ; cd /tmp "**

## **NOTA BENE 1:**

**Oltre al delimitatore di argomenti “ esiste anche il delimitatore “**  
Vedremo la differenza piu' avanti parlando di substitution.

## **NOTA BENE 2:**

**Delimitandola con un delimitatore, la stringa " pippo ; cd /tmp" appare al comando echo come un unico argomento.**

## **NOTA BENE 3:**

E' possibile disabilitare l'interpretazione del separatore ; facendolo precedere da un ulteriore carattere speciale detto carattere di escape \

In tal modo, il comando `echo pippo \\; cd /tmp`

visualizzera' pippo ; cd /tmp

**NOTA BENE 4: ESCAPE per QUOTING di singoli caratteri speciali**

In generale, precedendo un carattere speciale con il carattere \ (quoting di singolo carattere) si ottiene che il carattere speciale verrà utilizzato come un carattere qualunque, senza la sua speciale interpretazione da parte della shell.

# Brace Expansion - generazione stringhe (1)

## concetto di base

Quando passo alla bash una riga di comando da eseguire, la bash per prima cosa cerca di capire se nella riga sono presenti delle coppie di parentesi graffe che rappresentano un ordine di generare delle stringhe secondo delle regole.

- Un ordine di brace expansion è **una stringa di testo**,
  - racchiusa tra separatori quali spazi, tab o andate a capo
  - e al cui interno compaiono una coppia di graffe non precedute da un \$,
  - e al cui interno non ci sono spazi bianchi o tab.
- Questa stringa che ordina una brace expansion è formato da tre parti, di cui la prima (preambolo) e l'ultima (postscritto) possono non essere presenti.
- La parte di mezzo è quella racchiusa all'interno di una coppia di parentesi graffe.
- Dentro le graffe sono presenti una o più stringhe separate da virgole.
- **Ciascuna stringa rappresenta una possibile scelta di stringhe che possono essere aggiunte al preambolo e seguite dal postscritto per formare delle nuove stringhe di testo.**

Ad esempio, se la riga di comando è fatta così:

```
echo va{acaga,ffancu,ammori,catihafat}lo
```

il comando viene espando in questo modo

```
echo vaacagalo vaffanculo vaammorilo vacatihofatlo
```

ottenendo il gentile output

vaacagalo vaffanculo vaammorilo vacatihofatlo **71**

# Brace Expansion - generazione stringhe (2)

## spazi bianchi nelle stringhe

Possono mancare preambolo o postscritto o entrambi

a{bb,cc,ddd} diventa abb acc addd

**Non possono essere presenti spazi bianchi o tab** altrimenti la brace expansion non viene riconosciuta e non viene applicata l'espansione.

Il comando: echo a{bb,cc, dd}ee

ottiene questo output: a{bb,cc, dd}ee

Analogamente, il comando echo a{bb,cc,d d}ee

ottiene questo output : a{bb,cc,d d}ee

**Se voglio far generare stringhe con spazi bianchi, devo proteggere i singoli spazi con dei caratteri backslash**

Ad esempio, echo a{bb,cc,d\ d}ee

ottiene questo output: abbee accee ad dee

Ad esempio, echo aa\ a{bb,cc,dd}ee

ottiene questo output: aa abbee aa accee aa addee

**Non posso proteggere tutto l'ordine di brace expansion con doppi apici perché disabilitano l'interpretazione dell'espansione, ma posso proteggere ciascuna singola stringa (quella tra due virgole)**

Il comando echo "a{bb,cc,d d}ee" ottiene in output

a{bb,cc,d d}ee

mentre il comando echo a{bb,cc,"d d"}ee ottiene in output

abbee accee ad dee

# Brace Expansion - generazione stringhe (3) annidamento e variabili

## Annidamento delle brace expansion

E' possibile inserire degli ordini di brace expansion all'interno di altri ordini di brace expansion.

Il comando

```
echo /usr/{ucb/{ex,edit},lib/{bin,sbin}}
```

ottiene questo output

```
/usr/ucb/ex /usr/ucb/edit /usr/lib/bin /usr/lib/sbin
```

E' possibile inserire più livelli di annidamento delle brace expansion

## Variabili nelle brace expansion

E' possibile inserire delle variabili negli ordini di brace expansion  
all'interno di altri ordini di brace

A=bin

B=log

C=boot

```
echo ${A}${${B}${C},${C},${A}${B}}a
```

visualizza

```
binlogboota binboota binbinloga
```

# Brace Expansion - generazione stringhe (4)

## brace expansion con Sequence Expression

Esiste una particolare forma di brace expansion che consente di generare stringhe elencando un intervallo di caratteri che possono essere usati come possibili scelte. L'intervallo viene indicato mediante i due estremi connessi con due punti

Il comando  
ottiene questo output

```
echo a{b..k}m  
abm acm adm aem afm agm ahm aim ajm akm
```

Il comando  
ottiene questo output

```
echo a{4..7}m  
a4m a5m a6m a7m
```

E' possibile annidare queste sequence expression all'interno di brace expansion  
annidate

Il comando  
ottiene questo output

```
echo a{b,c{4..7}}m  
abm ac4m ac5m ac6m ac7m
```

NB: Esiste una forma più complessa di sequence expression, in cui si può stabilire un incremento non unitario nell'intervallo di caratteri, ma questa forma non è supportata in tutte le versioni della bash, quindi non ne parliamo.

# Tilde Expansion ~

La tilde expansion riguarda 5 casi essenziali:

1. un carattere tilde isolato
  2. un carattere tilde seguito da slash non quotato
  3. un carattere tilde seguito da slash non quotato seguito da altri caratteri
- In questi casi la tilde viene sostituita dal percorso assoluto della home directory dell'utente che sta eseguendo la riga di comando, l'effective user.

Supponendo che l'utente che esegue i comandi sia l'utente vittorio

cd ~	cambia la directroy corrente in	/home/vittorio
echo ~/	visualizza	/home/vittorio/
echo ~/vaff	visualizza	/home/vittorio/vaff

4. una parola che inizia con la tilde seguita da un nome utente
  5. una parola che inizia con la tilde seguita da un nome utente, seguita da slash non quotato a cui possono seguire altri caratteri
- In questi casi la tilde più nome utente viene sostituita dal percorso assoluto della home directory dell'utente specificato dal nome.

Supponendo che esista un utente panzieri e che a eseguire sia vittorio

echo ~panzieri	visualizza	/home/panzieri
echo ~panzieri/ciao	visualizza	/home/panzieri/ciao

Se l'utente specificato non esiste, l'espansione non viene fatta, stringa invariata

echo ~panzieriNonEsiste	visualizza	~panzieriNonEsiste
-------------------------	------------	--------------------

# Wildcards \* ? [...]

## Pathname substitution

I Metacaratteri \* e ? sono caratteri che vengono inseriti dall'utente nei comandi digitati e che la shell interpreta cercando di sostituirli con una sequenza di caratteri per ottenere i nomi di files nel filesystem

Con cosa sono sostituiti?

\* può essere sostituito da una qualunque sequenza di caratteri, anche vuota.

? può essere sostituito da esattamente un singolo carattere.

[elenco] puo' essere sostituito da un solo carattere tra quelli specificati in elenco.

Esempi: usiamo il comando **ls** che visualizza i nomi dei file nella directory specificata.

Nessuna sostituzione

ls /home/vittorio                         visualizza i nomi di tutti i file della directory

ls /home/vittorio/primo.c                 visualizza il nome del solo file primo.c

Sostituzione di \* con una qualunque sequenza di caratteri, anche vuota, che permetta di ottenere il nome di uno o più file

ls /home/vittorio/\*.exe                         visualizza il nome di quei file della directory vittorio  
   il cui nome termina per .exe (cioè primo.exe)

ls /home/vittorio/primo\*                         visualizza i nomi di quei file della directory vittorio  
   il cui nome inizia per primo, cioè primo.c primo.exe

Sostituzione di ? con un singolo carattere (NON vuoto),

ls /home/vittorio/pri?o.c                         visualizza il nome del file primo.c di directory vittorio

# Wildcards [...]

Cosa posso mettere dentro le parentesi quadre? E con cosa viene sostituito ?

[abk] puo' essere sostituito da un solo carattere tra a b oppure k.

[1-7] puo' essere sostituito da un solo carattere tra 1 2 3 4 5 6 oppure 7.

[c-f] puo' essere sostituito da un solo carattere tra c d e oppure f.

[[:digit:]] puo' essere sostituito da un solo carattere numerico (una cifra).

[[:upper:]] puo' essere sostituito da un solo carattere maiuscolo.

[[:lower:]] puo' essere sostituito da un solo carattere minuscolo.

Notare che le parentesi quadre selezionano uno solo tra i caratteri elencati dentro.

Nell'elenco possono comparire diverse sequenze di parentesi quadre.

Le sequenze speciali [:digit:] [:upper:] [:lower:] **devono stare dentro altre parentesi quadre esterne.**

Es: Supponiamo che in una directory ci siano i file: aB a1B a2B akB akmB akmtB

Allora:

```
ls a[[:digit:]]B  
visualizza a1B a2B
```

```
ls a[[:lower:]][[[:lower:]][[[:lower:]]]B  
visualizza akmtB
```

Notare la differenza tra I seguenti comandi (occhio alle parentesi quadre annidate)

```
ls a[[:lower:]][[[:lower:]]]B [ ] [ ]  
visualizza akmB
```

```
ls a[[:lower:]][[:lower:]]B [ ] [ ]  
visualizza akB
```

# Wildcards [...] - esempio di uso sbagliato

Non posso annidare delle parentesi quadre se non per contenere le parole riservate

[:digit:] [:upper:] [:lower:]

in una directory che contiene i file akB akmB a1B a2B

se scrivo

```
ls a[[:lower:][:digit:]]B  
visualizzo akB a1B a2B
```

se scrivo

```
ls a[[:lower:][12]]B
```

le parentesi quadre [12] sono interne ad altre parentesi quadre, quindi non vengono sostituite con niente, ed il comando risponde:

```
ls: cannot access a[[:lower:][12]]B: No such file or director
```

# Comandi della bash ed eseguibili utili

## Comandi

### Comandi ed eseguibili

pwd cd mkdir rmdir ls rm echo cat set mv ps sudo du kill bg fg  
read wc killall

### Istruzioni di controllo di flusso

for do done                  while do done                  if then elif then else fi

### Espressione condizionale (su file o su variabile)

[ condizione di un file ]

### Valutazione di espressione matematica applicata a variabili d'ambiente (( istruzione con espressione ))

## Eseguibili binari forniti dal sistema operativo

editor interattivi  
vi nano (pico)

## utilità

man more less grep find tail head cut tee ed tar gzip diff patch gcc make

# Comandi della bash (in ordine di importanza)

<b>pwd</b>	mostra directory di lavoro corrente .
<b>cd <u>percorso directory</u></b>	cambia la directory di lavoro corrente .
<b>mkdir <u>percorso directory</u></b>	crea una nuova directory nel percorso specificato
<b>rmdir <u>percorso directory</u></b>	elimina la directory specificata, se è vuota
<b>ls -alh <u>percorso</u></b>	stampa informazioni su tutti i files contenuti nel percorso
<b>rm <u>percorso file</u></b>	elimina il file specificato
<b>echo <u>sequenza di caratteri</u></b>	visualizza in output la sequenza di caratteri specificata
<b>cat <u>percorso file</u></b>	visualizza in output il contenuto del file specificato
<b>env</b>	visualizza le variabili ed il loro valore
<b>which <u>nomefileeseguibile</u></b>	visualizza il percorso in cui si trova (solo se nella PATH) l'eseguibile
<b>mv <u>percorso file</u> <u>percorso nuovo</u></b>	sposta il file specificato in una nuova posizione
<b>ps aux</b>	stampa informazioni sui processi in esecuzione
<b>du <u>percorso directory</u></b>	visualizza l'occupazione del disco.
<b>kill -9 <u>pid processo</u></b>	elimina processo avente identificativo pid_processo
<b>killall <u>nome processo</u></b>	elimina tutti i processi con quel nome nome_processo
<b>bg</b>	ripristina un job fermato e messo in sottofondo
<b>fg</b>	porta il job più recente in primo piano
<b>df</b>	mostra spazio libero dei filesystem montati
<b>touch <u>percorso file</u></b>	crea il file specificato se non esiste, oppure ne aggiorna data.
<b>more <u>percorso file</u></b>	mostra il file specificato un poco alla volta
<b>head <u>percorso file</u></b>	mostra le prime 10 linee del file specificato
<b>tail <u>percorso file</u></b>	mostra le ultime 10 linee del file specificato
<b>man <u>nomecomando</u></b>	è il manuale, fornisce informazioni sul comando specificato
<b>find</b>	cercare dei files
<b>grep</b>	cerca tra le righe di file quelle che contengono alcune parole
<b>read <u>nomevariabile</u></b>	legge input da standard input e lo inserisce nella variabile specificata
<b>wc</b>	conta il numero di parole o di caratteri di un file
<b>true</b>	restituisce exit status 0 (vero)
<b>false</b>	restituisce exit status 1 (non vero)

# Funzione di Autocompletamento della bash. Tasto TAB (tabulazione)

Mentre sto digitando dei comandi può capitare di dover specificare il percorso assoluto o relativo di un file o di una directory.

Se comincio a scrivere questo percorso, **posso premere il tasto TAB** (tabulazione) il quale attiva la funzione di autocompletamento dei nomi di files o directory.

Tale funzione produce ogni volta uno dei quattro seguenti risultati:

1. Se non esiste nessun percorso che comincia con la parte di percorso scritta  
**Non accade nulla, viene solo lanciato un beep di avvertimento.**
2. Se esiste un solo percorso che comincia con la parte di percorso scritta  
**Viene aggiunta alla parte scritta la parte mancante per completare il percorso.**
3. Se esistono più percorsi che cominciano con la parte di percorso scritta e tutti questi percorsi hanno una parte di percorso comune oltre a quella già scritta  
**Viene aggiunta alla parte scritta la parte comune a tutti i percorsi.**
4. Se esistono più percorsi che cominciano con la parte di percorso scritta ma tutti questi non hanno altra parte di percorso in comune oltre a quella già scritta  
**non accade nulla, viene solo lanciato un beep di avvertimento.**

In questo caso, **se premo due volte TAB (rapidamente)**, viene visualizzato l'elenco dei **possibili percorsi che possono essere scelti per completare il percorso già scritto**.

# Parametri a riga di comando passati al programma (4)

## Parameter Expansion

Come utilizzare in uno script gli argomenti a riga di comando passati allo script

Esistono variabili d'ambiente che contengono gli argomenti passati allo script

**\$#** il numero di argomenti passati allo script

**\$0** il nome del processo in esecuzione

**\$1** primo argomento, **\$2** secondo argomento, ....

**\$\*** tutti gli argomenti passati a riga di comando concatenati e separati da spazi

**\$@** come **\$\*** ma se quotato gli argomenti vengono quotati separatamente

Esempio: All'interno di uno script posso usarle così :

file esempio\_script.sh

```
echo "ho passato $# argomenti alla shell"  
echo "tutti gli argomenti sono $*"
```

**NOTA BENE: I parametri NON POSSONO essere modificati**

**NOTA BENE: Il programma vede i parametri COSÌ COME SONO DIVENTATI DOPO LA EVENTUALE SOSTITUZIONE DEI METACARATTERI \* e ?**

Ad esempio, se nella directory corrente ci sono i seguenti file x.c, y.c e z.c, ed io lancio lo script, che contiene le 2 righe sopra riportate, in due modi diversi, vengono stampati in output i seguenti argomenti:

SENZA metacaratteri

```
./esempio_script.sh pippo  
ho passato 1 argomenti alla shell  
tutti gli argomenti sono pippo
```

CON metacaratteri

```
./esempio_script.sh *.c  
ho passato 3 argomenti alla shell  
tutti gli argomenti sono x.c y.c z.c
```

# Parametri a riga di comando passati al programma (5)

File esempio\_args.sh

```
#!/bin/bash

echo "ho passato $# argomenti alla shell"
echo "il nome del processo in esecuzione e' $0"
echo "gli argomenti passati a riga di comando sono $*"

for name in $* ; do
    echo "argomento e' ${name}";
done
```

eseguitelo chiamandolo con diversi argomenti e delimitatori

./esempio_args.sh	
./esempio_args.sh	alfa beta gamma
./esempio_args.sh	“alfa beta gamma”
./esempio_args.sh	“alfa beta” gamma

NB: la variabile name dichiarata nel for rimane utilizzabile anche dopo l'uscita dal for poiché il for viene eseguito nella bash stessa, non in una bash figlia.  
La variabile name fuori dal for avrà l'ultimo valore che le era stato assegnato

# Parametri a riga di comando passati al programma (6)

## Differenze tra \$\* e \$@

I parametri \$\* e \$@ sono uguali quando non quotati dai ", cioè sono la concatenazione separata da blank dei singoli argomenti.

\$\* == \$@ ---> \$1 \$2 \$3 ... \$n

I parametri \$\* e \$@ si comportano diversamente quando sono quotati con " in particolare:

"\$\*" ---> "\$1 \$2 \$3 ... \$n"      quotati tutti gli argomenti assieme

"\$@" ---> "\$1" "\$2" "\$3" ... "\$n"      quotato singolarmente ogni argomento

# Parametri a riga di comando passati al programma (6bis)

Il parametro \$@ è simile a \$\* cioè contiene tutti gli argomenti passati allo script, ma quando quotato con i “ ” mantiene quotati i singoli argomenti e permette di non spezzare gli argomenti che contengono degli spazi.

File esempio\_\\\$\\@.sh.

Eseguitelo con diversi argomenti e delimitatori

esempio\_\\\$\\@.sh alfa beta gamma

esempio\_\\\$\\@.sh “alfa beta” gamma

```
echo 'for con $* non quotato'  
for name in $* ; do  
    echo "argomento ${name}" ;  
done  
  
echo 'for con "$*" quotato'  
for name in "$*" ; do  
    echo "argomento ${name}" ;  
done  
  
echo 'for con $@ non quotato'  
for name in $@ ; do  
    echo "argomento ${name}" ;  
done  
  
echo 'for con "$@" quotato'  
for name in "$@" ; do  
    echo "argomento ${name}" ;  
done
```

**NON SOLO PER I  
MANIACI**

**NB: \$@ si usa anche  
quando uno script  
deve eseguire un  
altro comando  
passandogli tutti gli  
argomenti che ha  
ricevuto a riga di  
comando**

# Valutazione Aritmetica di espressioni **con soli interi** (1): operatori **(( ))** e **\$(( ))**

E' possibile valutare una stringa come se fosse una espressione costituita da operazioni aritmetiche **tra soli numeri interi**

**L'operatore (( )) racchiude TUTTA una riga di comando semplice**, che deve essere una espressione (più un eventuale assegnamento).

L'operatore **(( ))** esegue la riga di comando che racchiude valutando aritmeticamente gli operandi.  
Ad esempio

`(( NUM=3+2 ))`

assegna 5 alla variabile NUM

**L'operatore \$(( )) invece serve se dovete racchiudere solo UNA PARTE di una riga di comando, che deve essere una espressione (più un eventuale assegnamento).**

La bash

- prima valuta aritmeticamente l'espressione racchiusa dall'operatore **\$(( ))**
- poi, nella riga di comando, **mette al posto** del **\$((...))** il risultato calcolato dall'operatore **\$(( ))**
- infine, esegue la riga di comando modificata

Ad esempio, nella riga di comando

`echo stampa pippo$((3+2))`

la bash

prima valuta l'espressione **\$((3+2))** e ne calcola il risultato che è 5  
poi nella riga di comando originale sostituisce 5 al posto di **\$((3+2))**  
ottenendo la nuova riga di comando

`echo stampa pippo5`

infine esegue quest'ultima riga di comando visualizzando a video

`stampa pippo5`

# Valutazione Aritmetica di espressioni **con soli interi** (2): operatori (( )) e \$(( ))

Errori sintattici nell'espressione provocano errori.

```
NUM=1  
NUM=${NUM}+3  
echo  
${NUM}  
stampa a video la stringa 1+3
```

```
NUM=1  
((NUM=${NUM}+3))  
echo ${NUM}  
uso corretto di operatore (( ))  
stampa a video la stringa 4
```

```
NUM=1  
NUM=(( ${NUM}+3))  
echo ${NUM}  
uso SBAGLIATO di operatore (( ))  
stampa a video  
"syntax error near unexpected token ("
```

```
NUM=1  
NOMEFILE=pippo${NUM}+3  
echo ${NOMEFILE}  
stampa a video la stringa pippo1+3
```

```
NUM=1  
(( NOMEFILE=pippo${NUM}+3 ))  
echo ${NOMEFILE}  
uso sbagliato di operatore (( ))  
impossibile valutare aritmeticamente pippo  
stampa a video la stringa 3
```

```
NUM=1  
NOMEFILE=pippo$(( ${NUM}+3 ))  
echo ${NOMEFILE}  
uso corretto di operatore $(( ))  
stampa a video la stringa pippo4
```

# Valutazione Aritmetica di espressioni **con soli interi** (3): operatori (( )) e \$(( ))

Se dovete racchiudere tutto un comando, allora DOVETE usare (( )) e NON potete usare \$(( ))  
Errori sintattici nell'espressione provocano errori.

Ad esempio:

```
A=1  
$(( B=$A+1 ))
```

```
-bash: 2: command not found
```

La bash valuta il contenuto dentro le tonde, poi sostituisce al contenuto quello che ha ottenuto dalla valutazione, infine esegue il comando dopo la sostituzione. Il comando dopo la sostituzione è 2. La bash cerca di eseguire 2 che non è un comando esistente e quindi genera un errore.

Analogamente:

```
B=3  
while read A && $(( A!=B )) ; do echo $A ; done
```

digitare qualcosa a tastiera, ad esempio 3 accade

```
-bash: 0: command not found
```

# Valutazione Aritmetica di espressioni **con soli interi** (4): operatori (( )) e \$(( ))

Le valutazioni aritmetiche possono contenere :

- o degli operatori aritmetici + - \* / %
- o degli assegnamenti
- o delle parentesi tonde () per accorpare operazioni e modificare precedenze.

Quando usate dentro una valutazione aritmetica, le parentesi tonde non creano una nuova bash.

Come vedremo più avanti, le valutazioni aritmetiche possono essere utilizzate come condizione di while e di if

```
NUM=33
while (( $(NUM=$(NUM)*$NUM)*${NUM}%10) != 2 )); do echo ${NUM} ; done
```

# Valutazione matematica più complesse: il programma Basic Calculator **bc** e il suo linguaggio di programmazione (1)

Rospi maledetti, questo mi basta che sappiate che esiste,  
nel caso vi dovesse servire ve lo studierete e approfondirete da soli:

Un esempio: la seguente concatenazione di comandi

```
echo " ( 32.16 - 14.03 ) / 3.33 " | bc -l -q
```

visualizza sullo standard output

```
5.44444444444444444444
```

# Valutazione matematica più complesse: il programma Basic Calculator **bc** e il suo linguaggio di programmazione (2)

Rospi maledetti, questo mi basta che sappiate che esiste,  
nel caso vi dovesse servire ve lo studierete e approfondirete da soli:

Un esempio piu' complesso con la definizione di una funzione utente:  
la seguente concatenazione di comandi

```
echo ' /* radice.b */
define r (x) {
    auto z, y
    z=0
    y=0
    while (1) {
        y=(z*z)
        if (y>x) {
            /* È stato superato il valore massimo. */
            z=(z-1)
            return (z)
        }
        z=(z+1)
    }
}
```

"calcolo la radice quadrata intera, r (x): "

r(625) '| bc -l -q

visualizza la parte intera della radice quadrata intera di 625, ovvero 25.

**calcolo la radice quadrata intera, r (x): 25**

# Variable expansion

Qui si sarebbe dovuto collocare la nozione di variable expansion, cioè il fatto che la bash espande il nome delle variabili, quando precedute dal \$, sostituendolo con il contenuto delle variabili stesse.

Ma questo argomento lo abbiamo anticipato e lo abbiamo già visto per poter usare le variabili negli esempi per spiegare altri argomenti.

Un caso particolare di variable expansion non è ancora stato trattato, il caso dei riferimenti indiretti a variabili, che viene presentato nella slide successiva.

# Riferimenti Indiretti a Variabili Indirect References to Variables

## operatore \${!} solo in bash versione 2

(1)

Supponiamo di avere una prima variabile varA che contiene un valore qualunque.  
Supponiamo di avere una altra variabile il cui valore è proprio il nome della prima variabile.

Voglio usare il valore della prima variabile sfruttando solo il nome della seconda variabile il cui valore è proprio il nome della prima variabile. Si dice che la seconda variabile è un riferimento indiretto alla prima variabile.

Accedere al valore di una prima variabile il cui nome è il valore di una seconda variabile è possibile nella bash a partire dalla versione 2.  
Si sfrutta un operatore \${!}

Esempio:

```
varA=pippo  
nomevar=varA  
echo ${!nomevar}
```

stampa a video pippo

# Riferimenti Indiretti a Variabili

## (2) operatore \${!}

### solo in bash versione 2

File `esempio_while.sh` permette di riferirsi alle var \$1 \$2 \$3  
da provare chiamandolo con diversi argomenti e delimitatori

`esempio_while.sh`

`esempio_while.sh alfa beta gamma`

`esempio_while.sh "alfa beta gamma"`

`esempio_while.sh "alfa beta" gamma`

```
#!/bin/bash
echo "ho passato $# argomenti alla shell"
echo "il nome del processo in esecuzione e' $0"
echo "gli argomenti passati a riga di comando sono $*"
```

NUM=1

```
while (( "${NUM}" <= "$#" ))
do
    # notare il ! davanti al NUM
    echo "arg ${NUM} is ${!NUM} "
    ((NUM=${NUM}+1))
done
```

# Exit Status

## Valore restituito da un programma al chiamante

### Differenza tra valore restituito e output

Ogni programma o comando restituisce un valore numerico compreso tra **0** e **255** per indicare se c'è stato un errore durante l'esecuzione oppure se tutto è andato bene. Un risultato **0 indica tutto bene** mentre un risultato **diverso da zero indica errore**.

Tale risultato non viene visualizzato sullo schermo bensì viene passato alla shell che ha chiamato l'esecuzione del programma stesso. In tal modo il chiamante può controllare in modo automatizzato il buon andamento dell'esecuzione dei programmi.

Il risultato non è l'output fatto a video, che invece serve per far vedere all'utente delle informazioni.

### Come restituire il risultato in un programma C – l'istruzione return;

vedi esempio primo.c

### Come restituire il risultato in uno script bash – il comando exit

esempio: **exit 9** fa terminare lo script e restituisce 9 come risultato

### Come catturare il risultato di un programma chiamato da uno script

Si usa una variabile d'ambiente predefinita **\$?** che viene modificata ogni volta che un programma o un comando termina e in cui viene messo il risultato numerico restituito dal comando o programma

**./primo.exe**

**echo "il processo chiamato ha restituito come valore di uscita \$?"**

# Exit Status riservati

Per convenzione, gli eseguibili restituiscono un valore intero compreso tra **0 e 255** per indicare se è accaduto un errore e quale errore è accaduto.

Il valore 0 indica che l'esecuzione si è svolta correttamente.

Exit Code Number	Meaning	Example	Comments
1	catchall for general errors	let "var1 = 1/0"	miscellaneous errors, such as "divide by zero"
2	misuse of shell builtins, according to Bash documentation		Seldom seen, usually defaults to exit code 1
126	command invoked cannot execute		permission problem or command is not an executable
127	"command not found"		possible problem with \$PATH or a typo
128	invalid argument to <a href="#">exit</a>	exit 3.14159	<a href="#">exit</a> takes only integer args in the range 0 – 255
128+n	fatal error signal "n"	<b>kill -9</b> \$PPID of script	\$? returns 137 (128 + 9)
130	script terminated by Control-C		Control-C is fatal error signal 2, (130 = 128 + 2, see above)
255*	exit status out of range	exit -1	<a href="#">exit</a> takes only integer args in the range 0 – 255

# Exit Status di Espressione valutata aritmeticamente

**La valutazione aritmetica** effettuata tramite gli operatori \$(( )) , oppure anche (( )) se comprende tutta la riga di comando, **restituisce un valore di Exit Status che sarà:**

**Diverso da** zero se durante la valutazione aritmetica **è accaduto un errore**. Il valore restituito indica il tipo di errore restituito.

(( ls 5 )) non valutabile aritmeticamente. \$? conterrà 1

**Uguale a zero se** la valutazione aritmetica fornisce un **risultato logico true**

(( 5 >= 2 ))

**Diverso da zero se la valutazione aritmetica fornisce un risultato logico false**

(( 5 <= 2 ))

**Uguale a zero se la valutazione aritmetica fornisce un risultato intero diverso da zero**

(( 4 )) \$? conterrà 0

(( VAR=5+3 ))

**Diverso da zero** se la valutazione aritmetica fornisce un risultato intero uguale a zero

(( 0 )) \$? conterrà 1

(( VAR=6-2\*3 )) \$? conterrà 1

**Se l'assegnamento è interno all'espressione (cioè non è eseguito per ultimo),** allora il risultato dell'espressione è quello del confronto eseguito per ultimo.

(( (VAR=6-2\*3) != 1 )) assegna 0 a VAR ma \$? conterrà 0 perché la condizione è vera

# OCCHIO: Errori con la valutazione aritmetica

```
$ NUM=13
```

```
$ echo $?
```

```
0
```

```
$ echo ${NUM}
```

```
13
```

```
$ (( NUM=${NUM}+4 ))
```

```
$ echo $?
```

```
0
```

```
$ echo ${NUM}
```

```
17
```

```
$ (( NUM=ALFA ))
```

causa errore

```
$ echo $?
```

```
1
```

valore di errore

```
$ echo ${NUM}
```

```
0
```

contenuto errato

# Liste di comandi

Una lista di comandi è un elenco di comandi da lanciare in esecuzione in successione. Sintatticamente, ciascun elemento dell'elenco deve essere separato dal successivo da un punto e virgola. Ciascun elemento dell'elenco può essere :

- **comando semplice (o chiamata di script o di eseguibile binario)**  
es: cd ./script.sh primo.exe
- **espressione valutata aritmeticamente**  
(( VAR=(5+3)\*(2+\$VAR) ))
- **sequenza di comandi connessi da | pipe** *(le vedremo poco più avanti)*  
cat file.txt | grep stringa
- **sequenza di comandi condizionali** *(le vedremo poco più avanti)*  
gcc file.c && ./file.exe
- **raggruppamento di comandi** *(le vedremo poco più avanti)*  
( cat file1.c ; cat file 2,c )
- **espressione condizionale** *(le vedremo poco più avanti)*  
[[ -e file.txt && \$1 -gt 13 ]]

Esempio di lista di comandi: NUM=7; ./pippo.exe || if((\${NUM}>2)); then exit 3; fi; echo ok

**Il risultato Exit Status restituito da una lista di comandi è l'Exit Status restituito dall'ultimo comando che è stato lanciato dalla lista di comandi stessa.**

NB: poiché le sequenze condizionale e le espressioni condizionali contengono dei comandi semplici e possono essere terminate senza avere eseguito tutti i comandi, in funzione dei risultati restituiti dai comandi eseguiti in precedenza, **può capitare che l'ultimo comando eseguito non sia l'ultimo a destra elencato nella lista** **99**

# Compound Commands – Comandi composti Costrutti per controllo di flusso di comandi (1)

*Versione semplificata*

for varname in elencoword ; do list ; done

for (( expr1 ; expr2 ; expr3 )) ; do list ; done

if listA ; then listB ; [ elif listC ; then listD ; ] ... [ else listZ ; ] fi

**while** list; do list; done

NOTA BENE:

Le espressioni expr\* dentro il for (( )) sono **sempre** valutate aritmeticamente, quindi devono essere espressioni interpretabili aritmeticamente.

Invece, i comandi dentro list\* sono valutati aritmeticamente solo se racchiudo i singoli comandi dentro doppie parentesi tonde.

Il risultato restituito da list\* e' il risultato dell'ultimo comando eseguito della lista oppure zero se nessun comando viene eseguito.

# Compound Commands – Comandi composti Costrutti per controllo di flusso di comandi (2)

## Esempi

```
for name in a b c ; do echo ${name} ; rm ${name} ; done
```

```
for (( i=0; $i<13; i=$i+2 )) ; do echo ciao$i ; done
```

```
if ls ./main.c && gcc -o main.exe main.c && ./main.exe ; then  
    echo main returns $?
```

```
fi
```

```
if [[ -e main.c && -e Makefile ]] && make && ./main.exe ; then  
    echo compiled program returns $?
```

```
fi
```

```
if [ -e main.c -a -e Makefile ] && make && ./main.exe ; then  
    echo compiled program returns $?
```

```
fi
```

```
while OUT=`./script1.sh` ; script2.sh $OUT ; do echo ancora done
```

```
i=0; while (( $i < 30 )) ; do echo $i ; (( i=$i+1 )) ; done
```

# Sequenze di comandi condizionali e non

## Sequenze non condizionali (vedi una slide precedente)

Il metacarattere “;” viene utilizzato per eseguire due o più comandi in sequenza ed indica la fine degli argomenti passati a ciascun comando riga di coman

```
date ; ls /usr/vittorio/ ; pwd
```

## Sequenze condizionali

“||” viene utilizzato per eseguire due comandi in sequenza, ma il secondo viene eseguito solo se il primo termina con un exit code **diverso da 0 (failure)**

“&&” viene utilizzato per eseguire due comandi in sequenza, ma il secondo viene eseguito solo se il primo termina con un exit code **uguale a 0 (success)**

## Esempi

Eseguire il secondo comando in caso di successo del primo

```
$ gcc prog.c -o prog && prog
```

Eseguire il secondo comando in caso di fallimento del primo

```
$ gcc prog.c || echo Compilazione fallita
```

# prossime slides

File descriptor

tabelle dei file aperti

stream di I/O predefiniti

ereditarietà dei file aperti

command substitution

quoting di stringhe:        " "    ''

# File Descriptors

Il **file descriptor** è un'astrazione per permettere l'accesso ai file.

Ogni file descriptor e' rappresentato da un integer.

Il concetto di file descriptor esiste sia usando linguaggio C ed anche in bash, perché è un concetto fornito dal sistema operativo.

```
#define MAXSIZE 100
#define nomefile "/home/vic/piffero.txt"
void main(void) {
    int fd, ris; char buffer[MAXSIZE];
    fd = open( nomefile, O_RDONLY );
    if( fd < 0 ) {    perror("open failed: "); exit(1); }

    /* lettura fino a raggiungere fine file */
    do {
        ris=read( fd, buffer, MAXSIZE );
        if( ris<0 ) {    perror("read failed: "); exit(1); }
    } while( ris>0);

    close(fd);
}
```

# File Descriptors e Tabelle dei File Aperti

Il **file descriptor** è un'astrazione per permettere l'accesso ai file. Ogni file descriptor è rappresentato da un integer.

Ogni processo ha la propria **file descriptor table** che contiene (**indirettamente**) le informazioni sui file attualmente utilizzati (aperti) dal processo stesso. In particolare, la file descriptor table contiene un file descriptor (un intero) per ciascun file usato dal processo. Per ciascuno di questi file descriptor, la tabella del processo punta ad una **tabella di sistema** che contiene le informazioni sui tutti i file attualmente aperti dal processo stesso.

Si noti che due diversi processi possono avere due diversi file descriptor con stesso valore, ma che fanno riferimento a file diversi.

Tabelle dei file aperti  
di ciascun processo

Process A	0	ptr
	1	ptr
	2	
	3	ptr

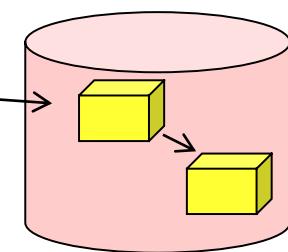
Process B		
	1	ptr

Tabella di Sistema  
dei file aperti

0	
1	info sui file
2	info sul file
3	
4	
5	info sul file
6	
7	



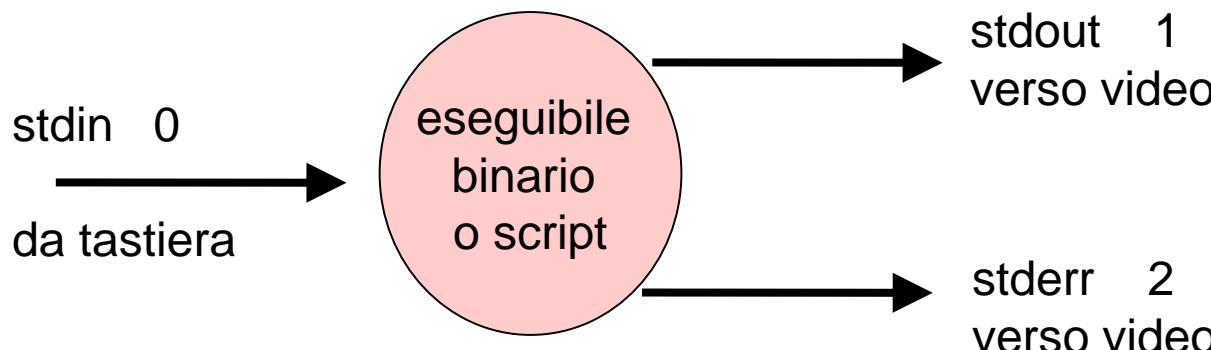
Disk



Monitor

In POSIX ogni processo è inizialmente associato a 3 fd standard  
stdin (0), stdout (1), stderr (2)

# Stream di I/O predefiniti dei processi (1)



Quando un programma entra in esecuzione l'ambiente del sistema operativo si incarica di aprire 3 flussi di dati standard, che sono:

**STANDARD INPUT (stdin)** serve per l'input normale (per default da tastiera). Viene identificato da una costante valore numerico **0**.

**STANDARD OUTPUT (stdout)** serve per l'output normale (per default su schermo video). Viene identificato da una costante valore numerico **1**.

**STANDARD ERROR (stderr)** serve per l'output che serve a comunicare messaggi di errore all'utente (per default anche questo su schermo video). Viene identificato da una costante valore numerico **2**.

**Come fare output in un programma C – la funzione printf();**

esempio: vedere il file primo.c

**Come fare output in uno script bash – il comando echo**

esempio già visto: echo "ciao bella"

# Stream di I/O predefiniti dei processi (1bis)

## Chi e come produce dati diretti verso lo standard output

- Da linguaggio di scripting bash

echo "stringa"

```
printf "%f %.6s" 3.99999 piripicchio
```

NB: e' la printf della bash non del C

vedere

man 1 printf

confrontarlo con man 3 printf

- Da linguaggio C

```
printf ( "%f %.6s" , 3.99999 , "piripicchio");
```

```
fprintf ( stdout, "%f %.6s" , 3.99999 , "piripicchio");
```

## Chi e come produce dati diretti verso lo standard error

- Da linguaggio di scripting bash, solo in caso di errori

ls filechenonesiste

produce "ls: cannot access filechenonesiste: no such file or directory"

- Da linguaggio C

```
fprintf ( stderr, "%f %.6s" , 3.99999 , "piripicchio");
```

## Chi e come legge dati provenienti dallo standard input

- Da linguaggio di scripting bash, solo in caso di errori

read nomevar

- Da linguaggio C

```
fgets( buffer , buffersize , stdin );
```

```
scanf ( "%i" , &intvar );
```

# Stream di I/O predefiniti dei processi (1tris)

Un esempio d'uso in C: legge da standard input e manda su standard error

```
/* stdin_stderr.c                                     premere CTRL D per chiudere stdin */
#include <stdlib.h>
#include <unistd.h>
#include <stdio.h>

int main (void)
{
    #define LINESIZE 1000
    char line[LINESIZE], *p;
    while (1) {
        p=fgets ( line , LINESIZE , stdin );
        if( p ) { /* lettura ok */
            fprintf ( stderr , "%s", line );
        }
        else if( feof ( stdin ) ) { /* EOF reached */
            return(0);                  /* return ok */
        }
        else {                      /* error */
            return(1);
        }
    }
    return(0);                  /* mai raggiunto */
}
```

# Stream di I/O predefiniti dei processi (1ter)

## I processi figli ereditano gli Stream dei padri

Una shell B figlia di una shell padre A (e in generale, un processo B figlio di un processo A) eredita una copia della tabella dei file aperti del padre, quindi padre e figlio leggono e scrivono sugli stessi stream.

Se padre e figlio scrivono contemporaneamente potrebbero scrivere cose strane. Ereditare una copia degli stream del padre permette, ad esempio, che l'output di uno script sia visibile nella finestra di output della shell interattiva che l'ha lanciato.

**NB: Vengono ereditati gli stream predefiniti ed anche tutti gli altri stream.**

Tabelle dei file aperti  
di ciascun processo

Process  
A  
padre

0	ptr
1	ptr
2	ptr
3	ptr

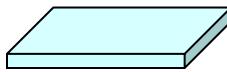
Process  
B  
figlio

0	ptr
1	ptr
2	ptr
3	ptr

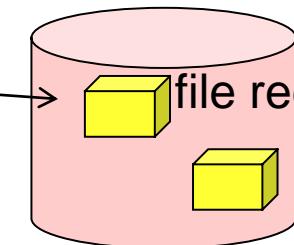
Tabella di Sistema  
dei file aperti

0	
1	info sui file
2	info sul file
3	info su file
4	
5	info sul file
6	
7	

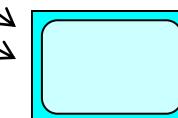
Tastiera



Disk



Monitor



# Stream di I/O predefiniti dei processi (2): command substitution

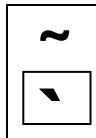
**Scopo:** sostituire a run time, in uno script, la riga di comando di un programma con l'output su stdout prodotto dall'esecuzione del programma stesso.

**Esempio:** come catturare, in una variabile, l'output di un programma chiamato da uno script. ( fa eseguire primo.exe)

```
OUT=`./primo.exe`  
echo "l'output del processo e' ${OUT}"
```

**Nota Bene:** L'apice giusto da usare è quello che in alto tende a sinistra e in basso tende a destra. Viene chiamato backticks o backquotes.

Nelle tastiere americane si trova nel primo tasto in alto a sinistra, accoppiato e sotto alla tilde. Non è l'apostrofo italiano ' (detto single quote) , il tasto del backquotes nelle tastiere italiane non esiste. Usare tastiera americana.



**Sintassi alternativa per la command substitution :** \$( rigadicomando )

esempio: OUT= \$( ./primo.exe ) *NB: sono parentesi TONDE*

In entrambe le sintassi, le eventuali wildcards ? \* [] vengono interpretate dalla shell e sostituite. Per disabilitare (escape) la sostituzione delle wildcards, si circonda la riga di comando con dei caratteri opportuni (quotes).

# Stream di I/O predefiniti dei processi (2): command substitution (2)

**supponiamo**

1. Che nella home directory dell'utente esista un file di nome prova-6.txt contenente una sola riga di testo "asdrubale non ragiona"
2. Che ci troviamo in una directory diversa dalla home directory.
3. Che in quella directory esista uno script esempio\_command\_substitution.sh contenente quello che segue

```
NUM=5
echo "output dello script: " `cat ~/${1-$(( ${NUM} +1 ))}.txt | wc -l`
```

4. Infine supponiamo di eseguire quello script invocandolo con i seguenti argomenti:

```
./esempio_command_substitution.sh prova 5
```

L'output dello script sarà il seguente  
output dello script: 1

Ciò dimostra che la bash, prima sostituisce in quest'ordine tilde, metacaratteri, variabili, e poi esegue la command substitution

# Quoting di stringhe: command substitution & escape

In una riga di comando, le eventuali wildcards ? \* [] variabili etc etc vengono interpretate dalla shell e sostituite. **Per disabilitare (escape) la sostituzione delle wildcards, si circonda la riga di comando con dei caratteri opportuni (quotes).**

Esempio di command substitution e sostituzione di wildcards e variabili

```
echo Dear ${USER} the files are a[:digit:]B and the date is: `date`
```

```
Dear vittorio the files are a1B a2B and the date is: Tue, Sep 15, 2015 12:34:52 PM
```

" " **Double quote** per escape wildcards e spazi (quoting parziale di stringhe)

Impedisce di usare il ; come separatore di comandi,

**Impedisce la sostituzione di wildcards**

ma **permette** di sostituire le **variabili** con il loro contenuto

e **permette** l'esecuzione di **comandi** (command substitution).

```
echo " Dear ${USER} the files are a[:digit:]B and the date is: `date` "
```

```
Dear vittorio the files are a[:digit:]B and the date is: Tue, Sep 15, 2015 12:35:44 PM
```

' ' **Single quote** escape wildcards, command substitution, variable substitution, spazi

Impedisce di usare il ; come separatore di comandi,

**Impedisce la sostituzione di wildcards**

e Impedisce di sostituire le variabili con il loro contenuto

e Impedisce l'esecuzione di comandi (command substitution).

```
echo ' Dear ${USER} the files are a[:digit:]B and the date is: `date` '
```

```
Dear ${USER} the files are a[:digit:]B and the date is: `date`
```

# Quotes: command substitution & escape (2)

esempi

```
echo Dear ${USER} the date is: `date` ; echo sei in ritardo  
Dear vittorio the date is: Tue, Sep 15, 2015 12:58:21 PM  
sei in ritardo
```

```
echo " Dear ${USER} the date is: `date` ; echo sei in ritardo "  
Dear vittorio the date is: Tue, Sep 15, 2015 12:58:07 PM ; echo sei in ritardo
```

```
echo ' Dear ${USER} the date is: `date` ; echo sei in ritardo '  
Dear ${USER} the date is: `date` ; echo sei in ritardo
```

# ATTENZIONE: la bash processa l'output prodotto dalla command substitution (1)

supponiamo che nella directory corrente esistano solo i due script seguenti, outputconasterisco.sh e chiama\_outputconasterisco.sh.

outputconasterisco.sh

```
echo '*'
```

chiama\_outputconasterisco.sh

```
./outputconasterisco.sh  
echo "riga di separazione"  
echo `./outputconasterisco.sh`
```

Eseguendo lo script `./chiama_outputconasterisco.sh` ottengo il seguente output

```
*
```

riga di separazione

chiama\_outputconasterisco.sh outputconasterisco.sh

**Notare che nel comando contenente `echo `./outputconasterisco.sh`` l'asterisco buttato sullo standard output è stato interpretato dalla bash e sostituito con i nomi dei file presenti nella directory corrente.**

# Espressioni CONDIZIONALI (1)

- Le espressioni condizionali sono dei particolari comandi che valutano alcune condizioni e restituiscono un exit status di valore 0 per indicare la verità dell'espressione o di valore diverso da zero per indicarne la falsità.
- Ciascuna espressione condizionale si scrive mettendo le condizioni da valutare tra doppie parentesi quadre [[ .... ]]
- Le condizioni che possono essere inserite in una espressione condizionali sono condizioni create appositamente, e **NON POSSONO ESSERE COMANDI**.
- Le condizioni all'interno delle [[ ]] possono essere composte tra loro mediante degli operatori logici ! (not), && (and), || (or) e mediante parentesi tonde per stabilire l'ordine di valutazione. ad esempio [[ ( (condA)&&(condB) ) || condC ]]
- All'interno delle espressioni condizionali [[ ]] la bash **effettua solo** le interpretazioni **variable expansion, arithmetic expansion con \${()}}** ma non (), **command substitution**, process substitution, and quote removal, **ma solo negli operandi**.
- Sono invece **disabilitate** le interpretazioni **Word splitting, brace expansion e pathname expansion** e **NON POSSONO COMPARIRE DEI COMANDI**
- Gli operatori di condizione (quelli con il - davanti, ad esempio -e nomefile ) per essere riconosciuti e valutati correttamente devono essere **NON quotati**. e non possono essere generati da command substitution.

Quindi:

- **non posso eseguire comandi ma posso eseguire command substitution (i backtick)** ma solo negli operandi, non per generare operatori.
- le doppie parentesi tonde senza \$ sono interpretate non come valutazione aritmetica ma come accorpamento logico di comandi per definire l'ordine di valutazione.

# Espressioni CONDIZIONALI (2)

## COMPORRE CONDIZIONI DENTRO ESPRESSIONI CONDIZIONALI

Notare che in una stessa espressione condizionale [[ ]] io posso effettuare sia confronti aritmetici (**specificando opportuni operatori -eq -ne -le -lt -ge -gt**), ma anche confronti non aritmetici (specificando altri operatori).

Posso infatti verificare **condizioni non aritmetiche che riguardano stringhe**, usando gli **operatori di confronto lessicografico tra stringhe == = != < <= > = >**

Posso anche verificare se delle stringhe sono vuote o no (con gli operatori **-z -n**).

Posso verificare **condizioni sui file** (operatori **-d -e -f -h -r -s -t -w -x -O -G -L** ).

Posso **confrontare le date di ultima modifica di due files** (operatori **-nt -ot** ).

Quindi, con le espressioni condizionali posso verificare espressioni aritmetiche ma **NON POSSO eseguire assegnamenti a variabili**.

**NOTA BENE: NEGLI OPERANDI dei confronti aritmetici possono comparire valutazioni aritmetiche effettuate mediante \$(( )) ma NON POSSO USARE VALUTAZIONI ARITMETICHE COME CONDIZIONI ISOLATE perché vengono fraintese.**

SI      [[ \$NUM -lt \$(( \$VAR \* ( 3 + \$MUL ) )) ]]

NO      [[ \$(( \$VAR < 3 + \$MUL )) ]]      non errore sintattico ma fraintende

NO      [[ pippo ]]                                **fraintende**, restituisce exit status 0

NO      [[ 3 ]]                                        **fraintende**, restituisce exit status 0

NO      [[ 0 ]]                                        **fraintende**, restituisce exit status 0

# Espressioni CONDIZIONALI (3)

## DIFFERENZE TRA ESPRESSIONI CONDIZIONALI E VALUTAZIONI ARITMETICHE

Gli operatori di valutazione aritmetica **(( )) o \$(( ))** valutano aritmeticamente tutto il comando che specifico all'interno, quindi , l'operatore di valutazione aritmetica :

- puo' contenere solo espressioni valutabili aritmeticamente
- può comporre espressioni aritmetiche mediante operatori logici && (AND) || (OR) e ! (NOT).
- non può contenere espressioni condizionali
- non può contenere comandi

SI      **(( \$VAR \* ( 3 + \$MUL ) < 4 && 7 > \$VAR ))**

NO      **(( \$VAR < 3 + \$MUL && [[ \$NUM -lt 5 ]] ))**      errore sintattico

# Espressioni CONDIZIONALI (4)

Esempi di espressioni corrette o sbagliate

[[ ls / ]]	<b>syntax error</b>
[[ \$(( "11" > "2" )) ]]	<b>Fraintende.</b> produce exit status 0 (true) sempre
[[ (( "11" > "2" )) ]]	<b>Fraintende.</b> produce exit status 1 (false) perché le tonde parentesi non valutano aritmeticamente e la valutazione è lessicografica (primo 1 a sinistra precede primo 2 a destra).
[[ -e /usr/include/stdio.h ]]	OK. Esiste il file /usr/include/stdio.h ? true va bene
[[ "-e /usr/include/stdio.h" ]]	<b>Fraintende</b> , restituisce true ma per sbaglio, infatti...
[[ "-e /usr/include/stdio" ]]	<b>Fraintende</b> , restituisce true ma stdio non esiste
[[ "-e" /usr/include/stdio.h ]]	<b>syntax error</b>

Per effettuare confronti aritmetici, quindi, non posso usare la coppia di doppie parentesi tonde senza \$ ma devo utilizzare gli appositi operatori di confronto aritmetico, che sono **-eq**, **-ne**, **-lt**, **-le**, **-gt**, or **-ge**

NUM=11; [[ \${NUM} < 3 ]];	<b>Sembra Strano</b> ma va bene. Exit status 0 (true) perché il confronto è eseguito lessicograficamente tra stringhe.
NUM=11; [[ \${NUM} -le 3 ]];	OK. ha exit status 1 (false) perché confronta aritmeticamente le stringhe.

Non posso annidare espressioni condizionali perché sono anch'esse dei comandi.

[[ -e /usr/include/stdio.h && [[ -e /usr/include/stdio.h ]]]	<b>syntax error</b>
--	---------------------

Non posso usare command substitution per generare operatori

[[ `echo -e /usr/include/stdio.h` ]]	<b>Fraintende</b>
[[ -e `echo /usr/include/stdio.h` ]]	OK

# Espressioni CONDIZIONALI (5) - versioni

*enhanced brackets*

**[[ condiz ]]**

*single brackets*

**[ condiz ]**

*test*

**test condiz**

Esistono 3 operatori analoghi per le espressioni condizionali, al cui interno specificare gli operatori per Condizioni di file, Confronto tra stringhe, Confronto aritmetico. L'operatore **[[ ]]** è più recente e non esiste nelle bash molto vecchie.

L'operatore **[[ ]]** permette di **comporre tra loro piu' condizioni**, utilizzando gli stessi **operatori logici** usati in C ovvero **!** (negazione) **&&** (and) e **||** (or).

Inoltre, **all'interno del blocco [[ ]] posso usare parentesi tonde** per raggruppare espressioni e modificare la precedenza degli operatori  
**e posso andare a capo**.proseguendo l'espressione

Diversamente, i due operatori **[ ]** e **test** permettono di comporre tra loro piu' condizioni, utilizzando però **operatori logici diversi**, e precisamente **!** (negazione) **-a** (and) e **-o** (or).

Inoltre, con questi due operatori, **NON POSSO usare parentesi tonde** per raggruppare espressioni e modificare la precedenza degli operatori  
**e NON posso andare a capo** se non usando il \ a fine riga .

# Espressioni CONDIZIONALI (6)

Le espressioni condizionali `[[ expression ]]` restituiscono un exit status 0 or 1 in dipendenza della valutazione della condizione esplicitata nella espressione. Tale risultato si ritrova come al solito nella variabile \$?

All'interno delle espressioni condizionali `[[ ]]`

- sono **disabilitate** le interpretazioni di tipo **Word splitting** e **pathname expansion**
- sono **abilitate** invece variable expansion, arithmetic expansion (solo quelle con \$() ma non con () senza \$), command substitution, process substitution, e quote removal.
- Gli operatori di condizione (quelli con il - davanti, ad esempio `-e nomefile` ) per essere riconosciuti e valutati correttamente devono essere **NON quotati** in alcun modo.

Usando l'operatore doppia parentesi quadra `[[ ]]` le espressioni condizionali possono essere collegati con gli operatori logici usati anche in C, quali `! && ||` e raggruppati con parentesi tonde.

Le precedenze degli operatori logici decrescono in questo ordine: `! && ||`

NOTA BENE per le prossime pagine:

Se tra gli argomenti degli operatori compare un file allora:

- se per questo argomento viene specificato /dev/fd/n allora l'operatore controlla il file descriptor n.
- se per questo argomento viene specificato uno dei file /dev/stdin /dev/stdout /dev/stderr allora l'operatore controlla il file descriptor di valore 0 1 e 2.

# Espressioni CONDIZIONALI (7)

Alcuni operatori per verificare **condizioni su file** :

<b>-d file</b>	True if <u>file exists and is a directory.</u>
<b>-e file</b>	True if <u>file exists.</u>
<b>-f file</b>	True if <u>file exists and is a regular file.</u>
<b>-h file</b>	True if <u>file exists and is a symbolic link.</u>
<b>-r file</b>	True if <u>file exists and is readable.</u>
<b>-s file</b>	True if <u>file exists and has a size greater than zero.</u>
<b>-t fd</b>	True if file descriptor fd is open and refers to a terminal.
<b>-w file</b>	True if <u>file exists and is writable.</u>
<b>-x file</b>	True if <u>file exists and is executable.</u>
<b>-O file</b>	True if <u>file exists and is owned by the effective user id.</u>
<b>-G file</b>	True if <u>file exists and is owned by the effective group id.</u>
<b>-L file</b>	True if <u>file exists and is a symbolic link. (deprecated, see -h)</u>
<b>file1 -nt file2</b>	True if file1 is newer (according to modification date) than file2, or if file1 exists and file2 does not.
<b>file1 -ot file2</b>	True if file1 is older than file2, or if file2 exists and file1 does not.

Nota Bene: Ne esistono altre, per vedere quali guardare man bash nella parte intitolata CONDITIONAL EXPRESSIONS.

# Espressioni CONDIZIONALI (8)

Alcuni operatori per verificare **condizioni su stringhe, aritmetiche e altre varie**:

**-o optname** True if shell option optname is enabled. See the list of options under the description of the **-o** option to the **set** command.

## Operatori su stringhe

**-z string** True if the length of string is zero.

**-n string** True if the length of string is non-zero.

string1 == string2

string1 = string2 True if the strings are equal

string1 != string2 True if the strings are not equal.

string1 < string2 True if string1 sorts before string2 lexicographically.

string1 > string2 True if string1 sorts after string2 lexicographically.

## Operatori aritmetici su stringhe

arg1 OP arg2 **OP** is one of **-eq**, **-ne**, **-lt**, **-le**, **-gt**, or **-ge**. These arithmetic binary operators return true if arg1 is equal to, not equal to, less than, less than or equal to, greater than, or greater than or equal to arg2, respectively. Arg1 and arg2 may be positive or negative integers.

# Esempio d'uso di Espressioni CONDIZIONALI (1)

Due porzioni di codice bash che fanno la stessa cosa usando in un caso le espressioni condizionali ed una valutazione aritmetica come condizione dell'if, e nel secondo caso invece usando direttamente l'espressione condizionale come lista di comandi dell'if che ne valuta l'exit status :

```
[[ -e ${name} ]]
if (( $? == 0 )) ; then
    echo "esiste ${name}, lo elimino" ;
    rm -f ${name}
fi ;
```

analogamente

```
if [[ -e ${name} ]] ; then
    echo "esiste ${name}, lo elimino" ;
    rm -f ${name}
fi ;
```

# Esempio d'uso di Espressioni CONDIZIONALI (1b)

1)	var="prova" [[ -n \${var} ]] ; echo \$?	output 0
2)	var="" [[ -n \${var} ]] ; echo \$?	output 1
3)	[[ -n "" ]] ; echo \$?	output 1
4)	unset var [[ -n \${var} ]] ; echo \$?	output 1
5)	[[ -n ]] ; echo \$? output bash: unexpected argument `]]' to conditional unary operator bash: syntax error near `]]'0	

NOTARE LA DIFFERENZA TRA I CASI 4 e 5\*:

nel caso 4 la bash capisce che si tratta di espr condizionale, riconosce l'operatore -n e, prima di tentare di fare l'espansione della variabile var, correttamente considera 0 la lunghezza della variabile che non esiste.

Nel caso 5, invece, la bash dice che manca l'argomento.

# Esempio d'uso di Espressioni CONDIZIONALI (2)

Due porzioni di codice bash che fanno la stessa cosa usando due diversi tipi di espressioni condizionali: le single brackets [ ] e le extended brackets [[ ]]

```
if [ -d ${name} -a ${#name} -lt 10 ] ; then
    echo "ok ${name}" ;
else
    echo "no ${name}";
fi ;
```

Analogamente

```
if [[ -d ${name} && ${#name} -lt 10 ]] ; then
    echo "ok ${name}" ;
else
    echo "no ${name}";
fi ;
```

**Attenzione all'interpretazione di &&**  
**può essere**  
**operatore AND logico in Espressioni CONDIZIONALI**  
**o operatore in SEQUENZE di COMANDI condizionali**

**QUI && è AND LOGICO**

```
if [[ -e ${name} && ${#name} -lt 10 ]]; then
    echo "ok ${name}";
fi
```

**QUI && è operatore in sequenza di comandi condizionale**

```
if [[ -e prova.c ]]; && gcc -o prova.exe prova.c ; then
    echo "posso eseguire prova.exe"
fi
```

# Evitare Errori Più Comuni (1)

**METTETE SPAZI PRIMA E DOPO le [[ e le ]]  
ed anche PRIMA E DOPO gli operatori (es. -)**

Ad esempio, l'espressione condizionale seguente

```
if [[-d /usr/include/stdio.h ]] ; then echo esiste ; fi
```

provoca errore, perché la bash crede che [[-d sia un comando da eseguire, infatti avvisa:

**[-d: command not found**

perché MANCA LO SPAZIO TRA le [[ e il -d

Infatti, **il parser della bash riconosce le espressioni condizionali prima separando la riga in parole delimitate da spazi. Se mancano gli spazi le espressioni condizionali non vengono riconosciute.**

Analogamente per gli spazi prima e dopo qualunque operatore, aritmetico, lessicografico, su file, insomma tutti.

Il comando

```
if [[ -dFILECHENONESISTE ]] ; then echo esiste ; fi
```

esegue e mette in output esiste.

Sembra dire che FILECHENONESISTE esiste perché senza spazi viene valutata (E NON ESEGUITA) la stringa -dFILECHENON ESISTE che essendo non vuota restituisce vero.

# Evitare Errori Più Comuni (2)

Cosa posso mettere dentro un if ?  
Liste di Comandi o Espressioni condizionali

OK               if  ls prova ; then echo ciao ; else echo fanculo ; fi  
OK, ma strano   if `ls prova` ; then echo ciao ; else echo fanculo ; fi  
OK               if [[ -e prova ]] ; then echo ciao ; else echo fanculo ; fi

Cosa posso mettere dentro le [[ ]] ?  
solo gli operatori delle espressioni condizionali,  
NON dei comandi,  
se non come command substitution negli operandi

OK               if [[ "aaa" == `cat prova` ]] ; then echo ciao ; else echo fanculo ; fi  
OK               if [[ -e prova ]] ; then echo ciao ; else echo fanculo ; fi  
**NOOO**           if [[ ls prova ]] ; then echo ciao ; else echo fanculo ; fi  
OK               if [[ -e `ls pro?a.c` ]] ; then echo esiste prova.c ; fi

# Evitare Errori Più Comuni (3)

**NO parentesi tonde tra le [ ] semplici**

OK

```
if [[ ( $var ne 13 || $var -ne 17 ) && -d /tmp ]] then echo ciao ; fi
```

**Syntax error! NO!** if [ ( \$var ne 13 -o \$var -ne 17 ) -a -d /tmp ] then echo ciao; fi

**SI composizioni logiche dentro  
a valutazioni aritmetiche (( ))**

OK

```
if (( $var < 13 || $var > 17 )) ; then echo ciao ; fi
```

**SI composizioni logiche dentro  
a espressioni condizionali [[ ]]**

**ma con operatori -a -o senza tonde () in []**

OK

```
if [[ $var -lt 13 || $var > 17 ]] then echo ciao ; fi
```

# Espressioni CONDIZIONALI (9)

NOTA BENE:

**RIBADISCO CHE NON POSSO eseguire dei COMANDI all'interno dell'operatore espressione condizionale. Posso mettere solo delle espressioni con operatori di confronto o di condizioni su file oppure delle command substitution.**

Cioe' **non posso eseguire** un comando (ad esempio come quello che segue) perche' il comando specificato tra le parentesi quadre semplicemente NON VIENE ESEGUITO poiche' **all'interno delle espressioni condizionali non e' previsto che venga eseguito un comando**. Diverso è il caso delle command substitution.

**NO !!!!!!! ERROR !!!!!!**

```
if [[ ls nomefile.txt ]] ; then echo "il file esiste" ; else echo "il file non esiste" ; fi
```

**Se occorre eseguire un comando e valutarne il risultato, NON DEVO METTERE il comando all'interno di una espressione condizionale ma devo metterlo semplicemente come condizione di un if, cosi':**

**SI**

```
if ls nomefile.txt ; then echo "il file esiste" ; else echo "il file non esiste" ; fi
```

# Quoting '\$'stringa'

## Usare caratteri non stampabili in una stringa

Parole aventi forma                    \$'charsequence'                    sono trattate in modo speciale.

La sequenza charsequence puo' contenere backslash-escaped characters.

- 1) La parola viene espansa in una stringa single-quoted, cioe' **perde il \$ all'inizio ma mantiene i due ' all'inizio e alla fine** (come se \$ non esistesse).
- 2) le backslash-escaped characters, se presenti, sono sostituite come specificato nello standard ANSI C:

**\a alert (bell)**

**\e**

**\f form feed**

**\r carriage return**

**\v vertical tab**

**\' single quote**

**\nnn** the eight-bit character whose value is the octal value nnn (one to three digits)

**\xHH** the eight-bit character whose value is the hexadecimal value HH  
(one or two hex digits)

**\cx** a control-x character, as if the dollar sign had not been present.

**\b backspace**

**\E an escape character**

**\n new line**

**\t horizontal tab**

**\\" backslash**

**\\" double quote**

Sta cosa tornera' utile per specificare il contenuto della variabile **IFS** poiche' questa contiene anche caratteri non stampabili.

# Word Splitting: CARATTERI SEPARATORI IN ELENCHI

La variabile IFS contiene i caratteri che fungono da separatori delle parole negli elenchi,  
IFS=\$' \t\n'

Notare che IFS di default contiene uno spazio bianco, un tab e un newline (a capo).

Se devo lanciare dei comandi in cui devo trattare dei nomi di file che contengono degli spazi bianchi, se non posso fare diversamente devo i) usare degli elenchi separati da newline o tab, e ii) togliere dai separatori lo spazio bianco.

IFS=\$' \t\n'

Poi eseguirò il comando che dovevo lanciare e dopo rimetterò lo IFS come era prima.

Es: directory che contiene due files, "aa bb.txt" e "aa cc.txt"

Vedere che succede se lancio

```
for name in `ls aa*` ; do echo ${name} ; done
```

Visualizzo

```
aa  
bb.txt  
aa  
cc.txt
```

TRUCCO OSCENO MA FUNZIONA

OLDIFS=\${IFS}

IFS=\$'\t\n'

```
for name in `ls -1 aa*` ; do echo ${name} ; done
```

IFS=\${OLDIFS}

## Word Splitting: CARATTERI SEPARATORI IN ELENCHI (2)

Precisazione per TarloI (sconosciuto)

perche', se tolgo spazio da IFS, bash riconosce grammatica?

perché i separatori contenuti in IFS sono utilizzati per individuare in modo specifico le separazioni tra gli elenchi di nomi.

I separatori usati per individuare le separazioni tra parole chiave del linguaggio sono invece non modificabili e sono sempre gli spazi bianchi, i tab e le andate a capo

# read - Lettura da standard input (tastiera o file) (1)

Uno script può leggere dallo standard input delle sequenze di caratteri usando un comando chiamato **read**.

Il comando read riceve la sequenza di caratteri digitate da tastiera fino alla pressione del tasto INVIO (RETURN) e mette i caratteri ricevuti in una variabile che viene passata come argomento alla read stessa. Se invece lo standard input è stato ridiretto da un file, allora la read legge una riga di quel file ed una eventuale read successiva legge la riga successiva.

La read restituisce un risultato che indica se la lettura è andata a buon fine, cioè restituisce:

- 0** se non si arriva a fine file e viene letto qualcosa,
- >0** se si arriva a fine file

```
while true ; do
    read RIGA
    if (( "$?" != 0 ))
    then
        echo "eof reached "
        break
    else
        echo "read \"${RIGA}\" "
    fi
done
```

va bene anche while (( 1 )) ;

# read - Precisazione su raggiungimento di fine file (2)

Può accadere che la lettura incontri la fine del file senza incontrare l'andata a capo.

Capita se leggo da file e nel file l'ultima riga **non ha** l'andata a capo \n alla fine.

In tal caso la read mette, nella variabile che gli viene passata, tutti i caratteri non ancora letti che precedono la fine del file, e poi restituisce un valore >0 per indicare che il file è stato usato fino alla fine.

Quindi, quando la read dice che è arrivata alla fine del file di input, possono essere accaduti due eventi diversi:

- 1) la read ha incontrato subito la fine del file e quindi nella variabile non è stato messo nulla, e quindi nella variabile la read mette la stringa vuota "".
- 2) la read ha letto dei caratteri e poi ha incontrato la fine del file, e quindi nella variabile troverò i caratteri letti ma la read restituisce comunque un valore >0.

**Perciò, quando si fa una lettura con la read, se la read dice di essere arrivata a fine file occorre comunque controllare se nella variabile letta c'è qualcosa dentro.**

Vedere la pagina successiva per esempi di controllo.

# read - Precisazione su raggiungimento di fine file (3)

## procedure di lettura corrette e tra loro equivalenti

Occorre una nozione aggiuntiva: la stringa \${#VAR} viene interpretata dalla bash sostituendola con la stringa di cifre che rappresenta il numero di caratteri di cui la variabile VAR, se esiste, è formata (la lunghezza della variabile VAR).

Se la variabile non esiste allora la stringa viene sostituita dalla stringa vuota.

Esempio:      VAR="ciao"; echo \${#VAR} ;      *produce in output 4*

**Quando si fa una lettura con la read, se la read dice di essere arrivata a fine file occorre comunque controllare se nella variabile letta c'è qualcosa dentro.**

Il controlli seguenti sono equivalenti:

- accettano in input anche righe vuote (riga con la sola andata a capo) che lasciano la variabile RIGA vuota nel caso che non si sia ancora raggiunta la fine del file.

```
while read RIGA; if (( $?==0 )); then true; elif (( ${#RIGA} != 0 )); then true; else false; fi ;  
do echo read "${RIGA}" ; done
```

OR Logico dentro espressione condizionale

```
while read RIGA ; [[ $? == 0 || ${RIGA} != "" ]] ; do echo "read ${RIGA}" ; done
```

```
while read RIGA ; [[ $? -eq 0 || ${#RIGA} > 0 ]] ; do echo "read ${RIGA}" ; done
```

```
while read RIGA ; [[ $? == 0 ]] || [[ -n ${RIGA} ]] ; do echo "read ${RIGA}" ; done
```

# read - Lettura da standard input (tastiera o file) (4)

**Se al comando read vengono passati come argomenti una o più variabili**, allora il contenuto della variabile **IFS** viene usato per separare la linea letta in parole e per **assegnare alle variabili passate le parole lette**, in particolare:

- Se la riga letta contiene piu' parole del numero delle variabili passate alla read, allora ciascuna variabile viene riempita con una parola estratta dalla linea letta, tranne l'ultima variabile che riceve tutto quello che resta della linea.
- Se invece la riga letta contiene meno parole del numero di variabili passate alla read, allora solo le prime variabili ricevono una parola, alle altre e' assegnato il valore vuoto. Esistono alcune opzioni interessanti **-u** **-N** **-r** ed altre meno necessarie **-e** **-n** **-t**. Il risultato restituito da read e' sempre 0 tranne che in caso di eof (o fd non valido o timeout scaduto, se specificati).

Se eseguo il comando

```
read varA varB varC
```

e scrivo a tastiera la frase

prima seconda terza

le variabili assumono valore

```
varA="prima" varB="seconda" varC="terza"
```

se invece scrivo a tastiera la frase

prima seconda terza quarta

le variabili assumono valore

```
varA="prima" varB="seconda" varC="terza quarta"
```

se invece scrivo a tastiera la frase

prima seconda

le variabili assumono valore

```
varA="prima" varB="seconda" varC=""
```

# read - Precisazione su lettura di riga con spazi iniziali (5)

Può accadere che una riga digitata da tastiera oppure anche una riga di un file, abbiano all'inizio degli spazi bianchi oppure delle tabulazioni.

Ad esempio, un file denominato `file_con_spazio_iniziale_nella_riga.txt` potrebbe contenere una riga così fatta: " **K 23F G2**"

In tal caso, una `read` (a cui viene passata UNA variabile) che legge quella riga NON mette nella variabile di lettura gli spazi iniziali ma solo i caratteri a partire dal primo carattere non bianco.

Perciò, una lettura fatta come qui sotto indicato

```
read RIGA < file_con_spazio_iniziale_nella_riga.txt  
echo \"\$RIGA\"
```

causerebbe l'output seguente:

" **K 23F G2**"

in cui, evidentemente, non sono stati letti i caratteri bianchi e le tabulazioni iniziali.

Ciò è dovuto al fatto che la `read` tenta di leggere le parole in una riga, non la riga.

Per leggere correttamente anche gli spazi bianchi, occorre dire alla bash che gli spazi bianchi e le tabulazioni NON SONO delimitatori delle parole.

Occorre a tal scopo settare preventivamente la variabile IFS come VUOTA

```
IFS=""; read RIGA < file_con_spazio_iniziale_nella_riga.txt  
echo \"\$RIGA\"
```

causa l'output corretto seguente:

" **K 23F G2**"

# read - Lettura di un numero specificato di caratteri (6)

L'opzione **-N** della **read** permette di specificare il numero di caratteri che devono essere letti.

Esempio: Legge 4 caratteri dallo standard input e li mette nella variabile **STRINGA**

```
read -N 4 STRINGA
```

Notare che non vengono più separate le word, anche gli spazi e i tab sono considerati caratteri qualsiasi.

Invece l'andata a capo \n viene ancora considerata un terminatore che interrompe la read.

**Se durante la lettura viene raggiunta la fine riga, la read termina anche se non ho letto tutti i caratteri richiesti. In tal caso, nella variabile trovo meno caratteri di quelli che avevo richiesto. La read successiva partirà dalla riga successiva.**

Se una read chiede meno caratteri di quelli presenti nella riga digitata dall'utente, che fine fanno i caratteri residui? **Ciascuna read comincia la lettura proprio dai caratteri residui (cioè non letti) dalla read che l'ha preceduta.**

Vedere l'esempio qui di lato e commentarlo.

## Esempi di comandi e i loro output

```
vic@vic:~$ cat miooutput.txt
messaggio1
messaggio2
vic@vic:~$ exec 103< miooutput.txt
vic@vic:~$ read -N 4 -u 103 RIGA
vic@vic:~$ echo $RIGA
mess
vic@vic:~$ read -N 4 -u 103 RIGA
vic@vic:~$ echo $RIGA
aggi
vic@vic:~$ read -N 4 -u 103 RIGA
vic@vic:~$ echo $RIGA
o1
vic@vic:~$ read -N 4 -u 103 RIGA
vic@vic:~$ echo $RIGA
mess
vic@vic:~$ read -N 4 -u 103 RIGA
vic@vic:~$ echo $RIGA
aggi
vic@vic:~$ read -N 4 -u 103 RIGA
vic@vic:~$ echo $RIGA
o2
vic@vic:~$ read -N 4 -u 103 RIGA
vic@vic:~$ echo $?
1
vic@vic:~$ echo $RIGA

vic@vic:~$ exec 103<-
vic@vic:~$
```

# Stream di I/O Non Predefiniti (1)

## Apertura, File Descriptor, accesso

Uno script bash può avere necessità di usare dei file su disco per fare I/O anche se non vengono passati mediante stdin ed stdout.

Ricordiamo che ad stdin, stdout e stderr sono associati dei file descriptor (rispettivamente 0, 1, 2) che permettono di accedere a quegli stream.

E' possibile **aprire un altro file da disco, ottenere un altro file descriptor che lo rappresenta ed utilizzarne quel nuovo file descriptor per accedere al file aperto.**

All'apertura del file, l'utente può decidere il file descriptor (il numero) che rappresenterà il file aperto, ma se tale fd è già usato avvengono problemi. In alternativa (procedura vivamente consigliata) l'utente può chiedere al sistema operativo di scegliere un fd libero.

Gli operatori sono indicati nella seconda e terza colonna della seguente tabella:

Modo Apertura	Utente sceglie fd (n è il numero scelto dall'utente)	Sistema sceglie fd libero e lo inserisce in variabile
Solo Lettura	<b>exec n&lt; PercorsoFile</b>	<b>exec {NomeVar}&lt; PercorsoFile</b>
Scrittura	<b>exec n&gt; PercorsoFile</b>	<b>exec {NomeVar}&gt; PercorsoFile</b>
Aggiunta in coda	<b>exec n&gt;&gt; PercorsoFile</b>	<b>exec {NomeVar}&gt;&gt; PercorsoFile</b>
Lettura e Scrittura	<b>exec n&lt;&gt; PercorsoFile</b>	<b>exec {NomeVar}&lt;&gt; PercorsoFile</b>

NB: i simboli < > >> <> devono essere attaccati (**senza spazi**) al numero o alla }

# Stream di I/O Non Predefiniti (2)

## Esempi: Apertura di file in Lettura e in Scrittura

uso una variabile che chiamo FD in cui verrà messo il file descriptor del file aperto.  
Nel comando **read** specifico l'opzione **-u** (seguita dal file descriptor del file aperto) per indicare al comando read da quale file aperto deve essere effettuata la lettura.

# esempio:

# effettuo le letture dal file mioinput.txt aprendolo in lettura

```
exec ${FD}< /home/vittorio/mioinput.txt
while read -u ${FD} StringaLetta ;
do
    echo "ho letto: ${StringaLetta}"
done
```

# esempio:

# scrivo l'output dei comandi echo sul file miooutput.txt aprendolo in scrittura

```
exec ${FD}> /home/vittorio/miooutput.txt
for name in pippo pippa pippi ; do
    echo "inserisco ${name}" 1>&${FD}
done
```

# Stream di I/O Predefiniti e Non (1)

## Dove trovo i file descriptor aperti da una bash?

Suppongo di avere una bash interattiva aperta.

La variabile \$\$ mi dice il PID process identifier della shell corrente.

Supponiamo che il PID della mia shell sia 1231.

Nella directory /proc/ esiste una sotto-directory per ciascun processo in esecuzione del processo stesso.

Quindi il seguente comando visualizza il contenuto della directory corrispondente alla shell corrente

```
ls /proc/$$/
```

Nella sotto-directory propria di ciascun processo, esiste una sotto-directory **fd** in cui sono presenti dei file speciali che sono i file aperti da quel processo.

Guarda caso, trovo sempre (tranne casi speciali) i file aperti aventi nome 0 1 2

Se nella mia bash apro un altro file, ad esempio col comando

```
exec {FD}< /tmp/caz.txt
```

e scopro che il file aperto ha file descriptor 7

```
echo ${FD}
```

```
7
```

se guardo nella directory /proc/1231/fd/ vedo che è stato aggiunto un file speciale di nome 7.

```
ls /proc/$$/fd/
```

# Stream di I/O Predefiniti e Non (2)

## Chiusura di file mediante il suo file descriptor

**Qualunque sia il modo di apertura** con cui ho aperto un file (lettura scrittura o entrambi), la chiusura di un file puo' essere effettuata utilizzando il comando exec con il seguente strano operatore

```
exec n>&-
```

dove n e' il file descriptor del file da chiudere.

Analogamente, se la variabile FD contiene il valore del file descriptor da chiudere, posso chiudere quel file utilizzando la seguente strana sintassi:

```
exec {FD}>&-
```

Nota bene, se dopo la chiusura del file utilizzo il file descriptor, la bash produce un errore.

```
exec 103> /home/vittorio/mioinput.txt
```

```
echo "messaggio1" 1>&103
```

```
# chiudo
```

```
exec 103>&-
```

```
echo "messaggio2" 1>&103
```

```
bash: 103: Bad file descriptor
```

← produce un messaggio di errore

# Ridirezionamenti di Stream di I/O (0)

## 1) RIDIREZIONAMENTO DI FILE DESCRIPTOR DI PROCESSI FIGLI

Quando lanciamo un comando o processo o script all'interno di una bash il processo figlio ottiene una copia di tutti i file descriptor del padre, quindi lavora con gli stessi stream aperti del padre.

Però il padre, nel momento in cui lancia il processo figlio, può decidere di cambiare gli stream da far usare al figlio, associando, a ciascun file descriptor da passare al figlio, uno stream diverso.

In tal caso, i file descriptor passati al figlio avranno lo stesso identificatore numerico di quelli del padre, ma saranno associati a stream diversi.

Il padre continuerà ad usare i suoi file descriptor associati ai vecchi stream.

## 2) AUTO-RIDIREZIONAMENTO , ovvero RIDIREZIONAMENTO DI PROPRI FILE DESCRIPTOR

Un processo può decidere di aprire nuovi file, chiudere file aperti o di associare un proprio file descriptor ad un altro stream (ridirezionamento).

In quest'ultimo caso, i file descriptor ridirezionati mantengono il loro valore ma sono associati a stream diversi. Da quel momento in avanti, il processo usando i vecchi file descriptor accederà ai nuovi stream.

Apertura chiusura e ridirezionamento di propri file sono effettuati mediante il comando exec

# Ridirezionamenti di Stream di I/O (1)

## Ridirezionamenti:

- < ricevere input da file.
- > mandare std output verso file eliminando il vecchio contenuto del file
- >> mandare std output verso file aggiungendolo al vecchio contenuto del file
- | ridirigere output di un programma nell' input di un altro programma

## Ricevere input da file.

L'utente puo' utilizzare lo standard input di un programma per dare input non solo da tastiera ma anche da file, **ridirezionando il contenuto di un file sullo standard input del programma, al momento dell'ordine di esecuzione del programma**:

program < nome\_file\_input

**il programma vedrà il contenuto del file nome\_file\_input come se venisse digitato da tastiera.**

Emulare la fine del file di input da tastiera: **Ctrl+D**

Notare che usando il ridirezionamento dell'input, c'è un momento in cui tutto il contenuto del file di input è stato passato al programma ed il programma si accorge di essere arrivato alla fine del file.

Se invece non faccio il ridirezionamento dell'input e fornisco l'input da tastiera, non incontro mai una fine del file di input. Per produrre da tastiera lo stesso effetto della terminazione del file di input devo digitare contemporaneamente i tasti CTRL e D che inviano un carattere speciale che indica la fine del file.

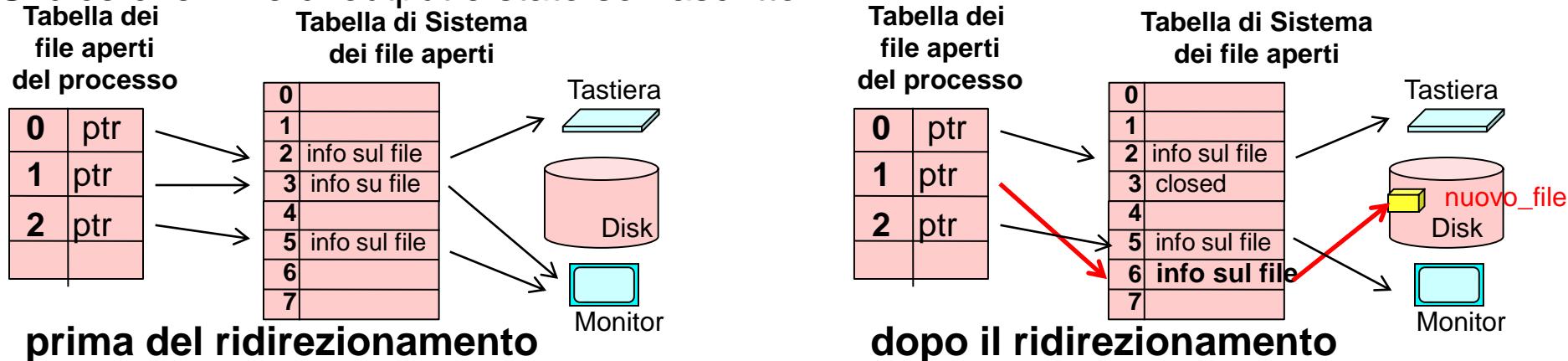
# Ridirezionamenti di Stream di I/O (2)

Analogamente **lo standard output** di un programma può essere **ridirezionato su un file**, su cui sarà scritto tutto l'output del programma invece che su video

program > nome\_file\_output

Nel file nome\_file\_output troveremo i caratteriche il programma voleva mandare a video.  
Il precedente contenuto del file verrà perso ed **alla fine dell'esecuzione del programma nel file troveremo solo l'output generato dal programma stesso.**

Si dice che il file di output è stato sovrascritto.



Il ridirezionamento dello standard output può essere fatto senza eliminare il vecchio contenuto del file di output bensì mantenendo il vecchio contenuto ed **aggiungendo il coda al file l'output del programma**

program >> nome\_file\_output

# Ridirezionamenti di Stream di I/O (3)

Supponiamo che un programma *program* mandi in output le due seguenti righe:

  pippo

  pappa

Supponiamo che il file *nome\_file\_output* contenga queste tre righe:

  uno

  due

  tre

Se eseguiamo il programma ordinando, con il ridirezionamento, di aggiungere l'output in coda al file *nome\_file\_output*, così:

*program >> nome\_file\_output*

alla fine dell'esecuzione il contenuto del file *nome\_file\_output* sarà:

  uno

  due

  tre

  pippo

  pappa

Se eseguiamo il programma ridirezionando l'output sul file *nome\_file\_output*, così:

*program > nome\_file\_output*

alla fine dell'esecuzione il contenuto del file *nome\_file\_output* sarà solo:

  pippo

  pappa

# Ridirezionamenti di Stream di I/O (4)

I due ridirezionamenti (input ed output) possono essere fatti **contemporaneamente**

program < nome\_file\_input > nome\_file\_output

O analogamente

program > nome\_file\_output < nome\_file\_input

In questo modo, il contenuto del nome\_file\_input viene usato come se fosse l'input da tastiera per il programma program, e l'output del programma viene scritto nel file nome\_file\_output.

Inoltre, in bash si può **ridirezionare assieme standard output e standard error su uno stesso file**, sovrascrivendo il vecchio contenuto:

program &> nome\_file\_error\_and\_output

Infine, in bash si può **ridirezionare standard ouput e standard error su due diversi file**, sovrascrivendo il vecchio contenuto:

program 2> nome\_file\_error > nome\_file\_output

# Ridirezionamenti di Stream di I/O (5)

Si noti che i **ridirezionamenti non modificano il valore dei file descriptor che vengono ridiretti** e nemmeno il numero di file descriptor dello script che li effettua. Questo accade perché il sistema operativo usa proprio il valore intero del file descriptor da ridirigere per indicare il file su cui viene ridiretto.

Ad esempio, se una bash lancia uno script `fd_di_script.sh` ridirezionando entrambi gli stream di output predefiniti su uno stesso file, quello script continua a vedere i due file descriptor 1 e 2 anche se questi fanno scrivere su uno stesso file.

ad esempio, lo script `fd_di_script.sh` visualizza l'elenco dei suoi file descriptor, così:

```
#!/bin/bash  
ls /proc/$$/fd/
```

Eseguiamo lo script ridirezionando entrambi gli stream di output predefiniti su uno stesso file:

```
./fd_di_script.sh &> out.txt
```

Nel file `out.txt` vedremo che sono indicati i tre file descriptor 0 1 2 come sempre.

# Ridirezionamenti di Stream di I/O (6)

## Generalizzazione operatori > <

In generale,

se una bash ha uno stream (un file aperto)  
e quello stream è identificato da un file descriptor di valore **N**,  
allora,  
è possibile ridirigere su un altro file  
lo stream indicato da quel file descriptor,  
usando una sintassi che specifica  
il valore intero N di quel file descriptor.

### **N>** NomeFileTarget

ridireziona il file descriptor N sul file **con nome** NomeFileTarget  
come già visto, se si omette N si intende standard output.  
usare **>>** per append

### **<N** NomeFileSource

ridireziona il file con nome NomeFileSource sul file descriptor N del  
programma specificato alla sinistra dell'operatore.  
Come già visto, se si omette N si intende standard input.

# Ridirezionamenti di Stream di I/O (7)

## PIPE | Connettere due processi mediante Ridirezione di stdout su stdin

E' possibile far eseguire contemporaneamente due processi mandando lo standard output del primo nello standard input del secondo, mediante l'operatore pipe |.

```
program1 | program2
```

I due processi eseguono in contemporanea.

Quando il primo processo termina o chiude il suo standard output, il secondo processo vede chiudersi il proprio standard input.

E' possibile connettere più processi in una sequenza di pipe

```
program1 | program2 | program3
```

# Ridirezionamenti di Stream di I/O (8)

## nuova bash per eseguire comandi composti in PIPE

Attenzione! In uno script dove compare una pipe, SE un comando a destra o a sinistra della pipe è un comando composto (dei loop) oppure è uno script, ALLORA QUEL COMANDO ESEGUE IN UNA SHELL BASH FIGLIA.

Guardiamo il seguente script `pipe.sh`

```
MIAVAR="iniziale"
echo prima ${MIAVAR}
ps
echo "poffarre" | while read MIAVAR ; do ps; echo dentro ${MIAVAR}; done
echo dopo ${MIAVAR}
```

eseguendo lo script `pipe.sh`, ottengo il seguente output

**prima** iniziale

PID TTY	TIME	CMD
1830 pts/0	00:00:00	bash
3990 pts/0	00:00:00	bash
3991 pts/0	00:00:00	ps

<- bash di shell interattiva  
<- bash che esegue pipe.sh

PID TTY	TIME	CMD
1830 pts/0	00:00:00	bash
3990 pts/0	00:00:00	bash
3993 pts/0	00:00:00	bash
3994 pts/0	00:00:00	ps

<- bash di shell interattiva  
<- bash che esegue pipe.sh  
<- bash che esegue while

**dentro poffarre**

la variabile MIAVAR creata in terza bash ha assunto valore "poffarre"  
MIAVAR ha mantenuto valore originale, non ha contenuto "poffarre"

**dopo iniziale**

# Ridirezionamenti di Stream di I/O (9)

## Operatore >& per ridirezionamento tra file descriptor

Se una bash ha due stream (due file aperti) entrambi di output (o entrambi di input), e ciascuno stream è identificato da un file descriptor di valore **N** ed **M** rispettivamente, allora

e' possibile ridirigere lo stream **N** sullo stream **M** mediante l'operatore

**N>&M**

Dopo di questo, ciò che scrivo su N viene scritto su M. Lo stream N mantiene il valore N del suo file descriptor ma, nella tabella dei file aperti del processo, il suo puntatore alla tabella di sistema viene sostituito da una copia del puntatore dello stream M

Esisteranno da quel momento due file descriptor N ed M di valore diverso ma che puntano allo stesso file aperto.

ls pippo.txt 2>&1

ridireziona lo stderr di ls sullo stdout di ls

Tabella dei  
file aperti  
del processo

<b>0</b>	ptr
<b>N</b>	ptr
<b>M</b>	ptr

Tabella di Sistema  
dei file aperti

<b>0</b>	
<b>1</b>	info sui file
<b>2</b>	info sul file
<b>3</b>	
<b>4</b>	
<b>5</b>	info sul file
<b>6</b>	
<b>7</b>	

prima del ridirezionamento

dopo il ridirezionamento

<b>0</b>	ptr
<b>N</b>	ptr
<b>M</b>	ptr

<b>0</b>	
<b>1</b>	info sui file
<b>2</b>	info sul file
<b>3</b>	
<b>4</b>	
<b>5</b>	info sul file
<b>6</b>	
<b>7</b>	

# Ridirezionamenti di Stream di I/O (10)

## Attenti alla differenza tra > e >&

Attenzione a non confondersi

```
cat out.txt 2>1
```

qui 1 è visto come il nome di un file  
si ridirige lo stderr di cat sul file 1  
non sullo stdout di cat

```
cat out.txt 2>&1
```

qui 1 è visto come file descriptor di un file aperto  
si ridirige lo stderr di cat sullo stdout di cat

# Ridirezionamenti di Stream di I/O (11)

## Ordine dei Ridirezionamenti con file descriptor (1)

E' importante l'ordine con cui compongo gli operatori di ridirezionamento di file descriptor. Sono eseguiti da sinistra verso destra.

ls pippo.txt 2> error.txt 1>&2

### Il primo ridirezionamento 2> error.txt

apre il file error.txt e mette le info sul file aperto nella nuova posizione 6 della tabella di sistema.

Poi copia nello spazio occupato dal puntatore del file descriptor 2 l'indirizzo della riga nuova della tabella di sistema.

Quindi ora fd 2 punta al file error. txt mentre fd 1 scrive ancora su video

### Il secondo ridirezionamento 1>&2

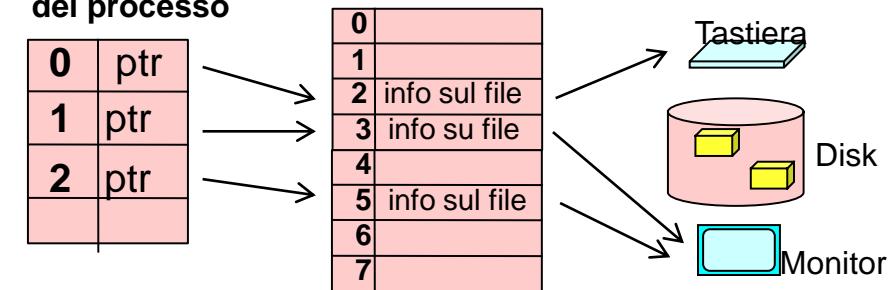
copia il puntatore del file descriptor 2 nello spazio occupato dal puntatore del file descriptor 1

Quindi ora sia fd 1 che fd 2 puntano alla stessa riga della tabella di sistema ed entrambi scrivono sul file error.txt

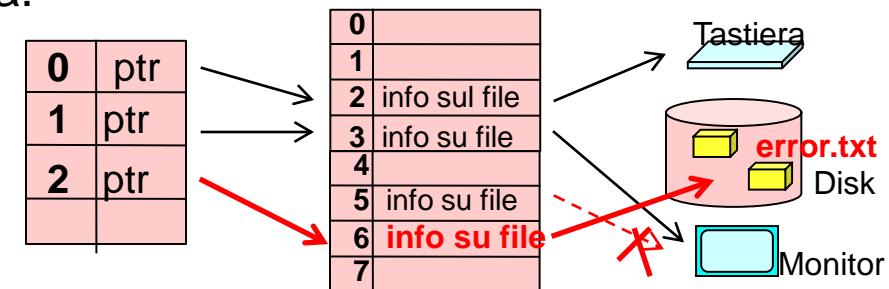
Tabella dei file aperti del processo

0	ptr
1	ptr
2	ptr

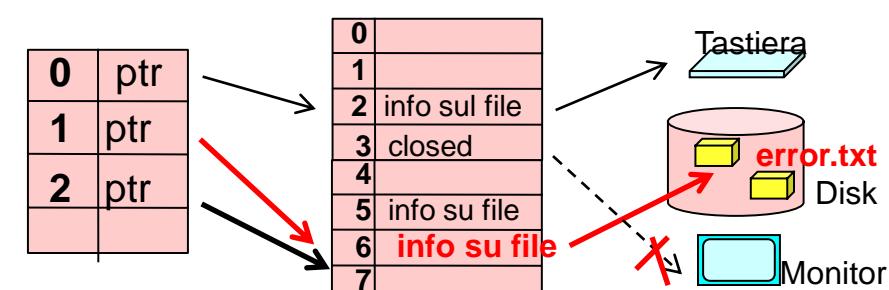
Tabella di Sistema dei file aperti



0	ptr
1	ptr
2	ptr



0	ptr
1	ptr
2	ptr



# Ridirezionamenti di Stream di I/O (12)

## Ordine dei Ridirezionamenti con file descriptor (2)

Scambiamo l'ordine degli operatori di ridirezionamento dell'esempio precedente.

```
ls pippo.txt 1>&2 2> error.txt
```

### Il primo ridirezionamento 1>&2

copia il puntatore del file descriptor 2  
nello spazio occupato dal puntatore  
del file descriptor 1

Quindi ora sia fd 1 che fd 2 puntano  
alla stessa riga della tabella di sistema  
ed entrambi scrivono su video

### Il secondo ridirezionamento 2>error.txt

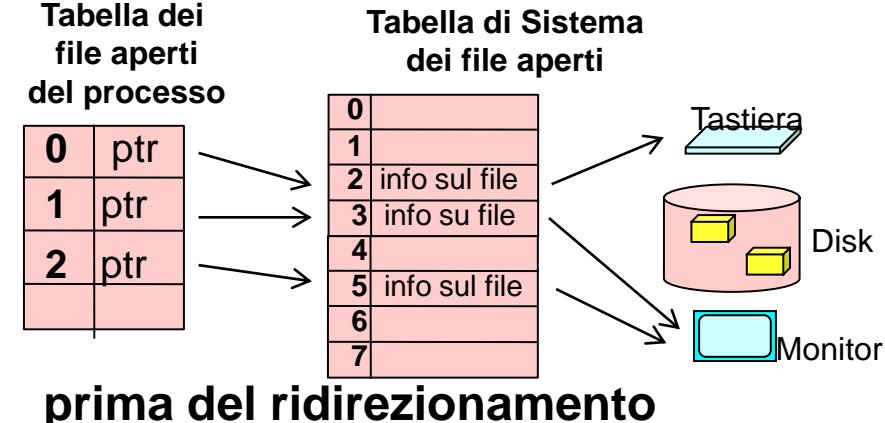
apre il file error.txt e mette le info sul file aperto  
nella nuova posizione 6 della tabella di sistema.

Poi copia nello spazio occupato dal puntatore  
del file descriptor 2 l'indirizzo della riga nuova  
della tabella di sistema.

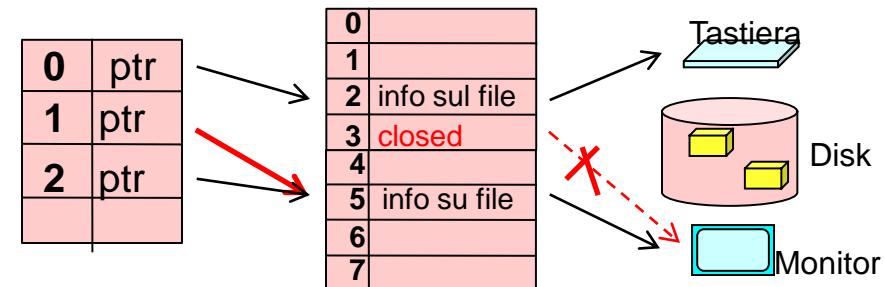
Quindi ora fd 1 scrive su video mentre  
fd 2 scrive sul file error.txt

Tabella dei  
file aperti  
del processo

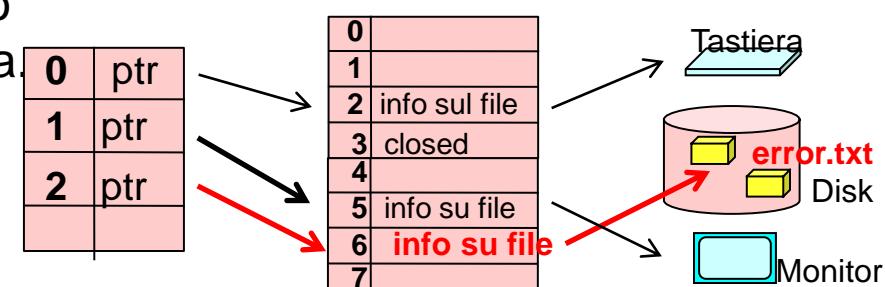
0	ptr
1	ptr
2	ptr



0	ptr
1	ptr
2	ptr



0	ptr
1	ptr
2	ptr



# Ridirezionamenti di Stream di I/O (13)

## Ordine dei Ridirezionamenti con file descriptor (3)

Confrontiamo i risultati dei due precedenti ridirezionamenti in cui cambia solo l'ordine. Si esegue da sinistra a destra.

ls pippo.txt 2> error.txt 1>&2

ridireziona stderr di ls sul file error.txt e poi ridireziona stdout di ls su stderr di ls che attualmente punta su error.txt,  
quindi **entrambi stdout e stderr di ls finiscono nel file error.txt**

invece

ls pippo.txt 1>&2 2> error.txt

ridireziona stdout di ls su stderr di ls che attualmente punta a video  
ridireziona stderr di ls su error.txt  
quindi alla fine **stderr punta ad error.txt**  
**mentre stdout scrive su video**

Tabella dei file aperti del processo

0	ptr
1	ptr
2	ptr

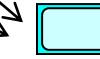
Tabella di Sistema dei file aperti

0	
1	
2	info sul file
3	info su file
4	
5	info sul file
6	
7	

Tastiera



Disk



Monitor

prima del ridirezionamento

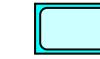
0	ptr
1	ptr
2	ptr

0	
1	
2	info sul file
3	closed
4	
5	closed
6	info su file
7	

Tastiera



Disk



Monitor

dopo il ridirezionamento

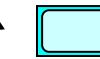
0	ptr
1	ptr
2	ptr

0	
1	
2	info sul file
3	closed
4	
5	info su file
6	info su file
7	

Tastiera



Disk



Monitor

dopo il ridirezionamento

# Ridirezionamenti di Stream di I/O (14)

## Esempio: ridirigere il solo stderr sullo stdin di un altro programma

Voglio ridirigere il solo stderr del comando ls, usandolo come stdin del comando grep e buttando via lo stdout di ls stesso.

```
ls nonesiste.txt 2>&1 > /dev/null | grep such
```

ridireziona stderr di ls su stdout di ls,  
ridireziona stdout di ls su /dev/null facendo buttare via l'output  
passa il nuovo stdout di ls come stdin di grep  
quindi il vecchio stderr di ls finisce nello stdin di grep

Notare le differenze tra il precedente ridirezionamento e quello qui sotto, in cui l'ordine dei due ridirezionamenti è invertito:

```
ls nonesiste.txt > /dev/null 2>&1 | grep such
```

ridireziona stdout di ls su /dev/null  
ridireziona stderr di ls su stdout di ls che ora punta a /dev/null  
quindi entrambi stdout e stderr di ls finiscono nel device /dev/null  
Al comando grep non arriva niente di niente.

# Ridirezionamenti di Stream di I/O (15)

## Scorciatoia |& invece di composizione 2>&1 |

Come visto nella pagina precedente, il Ridirezionamento di entrambi gli stream di output ed error verso lo stdin di altro programma, puo' essere fatto utilizzando la combinazione di operatori

```
2>&1 |
```

Provarlo eseguendo i due seguenti comandi in una directory in cui non esiste un file che si chiama pippo.txt, in modo da generare un messaggio di errore "no such file or directory", ridirezionarlo sullo standard output, collegarlo allo standard input di grep, selezionare la sola riga che contiene such e mandarla a video.

```
ls pippo.txt 2>&1 | grep such
```

```
ls * 2>&1 | grep such
```

Nota bene: **esiste un operatore apposito** che rappresenta una scorciatoia **dell'operatore composito 2>&1 |** che fa la stessa cosa, ed e' |&

```
ls pippo.txt |& grep such
```

# Ridirezionamenti di Stream di I/O (16)

E' importante notare **la differenza nelle tempistiche di esecuzione** dei programmi quando questi sono collegati dal separatore ; o dalla |

program1 ; program2 ; program3

Con il separatore ; io faccio eseguire i diversi programmi uno dopo l'altro, cioè prima che parta il secondo programma deve finire il primo e così via.

Inoltre l'output di un programma non viene ridirezionato nell'input del programma successivo.

program1 | program2 | program3

Invece, con la | i programmi specificati partono assieme e l'output di un programma viene ridirezionato nell'input del programma successivo.

# Ridirezionamenti di Stream di I/O (17)

E' possibile ridirigere contemporaneamente standard output e standard error di un programma program1 ridirigidolo verso lo standard input di un programma program2, utilizzando l'operatore |&

```
program1 |& program2
```

Con l'operatore composito |& i due programmi specificati partono assieme e l'output (sia cout che cerr) del primo un programma sono ridirezionati insieme nell'input del secondo programma.

# Auto-Ridirezionamento (18)

Una bash può ridirigere un proprio stream aperto verso un nuovo file descriptor. Da quel momento la bash vedrà il nuovo stream mediante il vecchio file descriptor. Gli autoridirezionamenti sono effettuati con i consueti operatori applicati ai file descriptor ma usati come argomenti della funzione exec.

Esempio:

Supponiamo di avere un file righedicomando.txt così fatto:

```
echo ciao  
echo ${BASHPID}  
ls /proc/${BASHPID}/fd/  
sleep 10
```

Proviamo ad eseguire i seguenti comandi in una shell interattiva

```
exec {NUOVOFD}< righedicomando.txt  
exec 0>&${NUOVOFD}
```

La bash usa come stdin il file righedicomando.txt , quindi visualizzerà i fd della bash stessa, poi aspetterà 10 secondi e infine terminerà chiudendo la finestra interattiva.

# Ridirezionamenti di Stream di I/O (19)

## Ridirezionamento per blocchi di comandi

Per i costrutti linguistici bash che eseguono blocchi di comandi ( for, while, if then else) è possibile applicare un ridirezionamento unico per tutti i comandi del blocco di comandi, compresi i comandi eseguiti nella condizione.

Ad esempio, eseguendo il seguente script, applico un ridirezionamento dello standard output a tutti i comandi all'interno del loop del while :

(file riduzione1BloccoWhile.sh)

```
NUM=1
echo "${NUM}"
while (( ${NUM} <= "3" )) ; do
    echo "${NUM}"
    ((NUM=${NUM}+1))
done > pippo.txt
echo "${NUM}"
```

Dopo l'esecuzione dello script, nel file pippo.txt troveremo le 3 righe:

```
1
2
3
```

mentre a video vediamo le 2 righe

```
1
4
```

# Ridirezionamenti di Stream di I/O (20)

## Ridirezionamento per blocchi di comandi

E' possibile applicare un **ridirezionamento** anche per flussi di input.

Supponiamo di avere un file `Assoluzionilnaspettate.txt` strutturato come nell'esempio:  
una riga con il reo, seguita da una riga con l'accusa, e così via:

<i>read dentro condizione while</i>	vittorio	ghini	17/07/1994
	blasfemia		assolto per insufficienza di prove
	giovanni	pau	15/07/1995
	ubriachezza		denuncia ritirata
	luca	andreucci	03/01/1992
	vilipendio		assolto per scomparsa del denunciante

Eseguiamo lo script `ridirezionelInputBloccoFor.sh` che segue

```
while read nome cognome data ; do
    if read accusa verdetto ; then
        echo $cognome errore $verdetto
    else
        echo terminazione inaspettata del file di input
        exit 1
    fi
done < Assoluzionilnaspettate.txt
```

# Ridirezionamenti di Stream di I/O (21)

## Esempi Ridirezionamento per blocchi di comandi

riduzione1BlocchifElse.sh

### Ridirezionamento per blocchi di comandi

```
NUM=1
echo "${NUM}"
if (( "${NUM}" <= "3" )) ; then
    ((NUM=${NUM}+1))
    echo "${NUM}"
else
    ((NUM=${NUM}+2))
    echo "${NUM}"
fi > pippo.txt
echo "${NUM}"
```

L'output del ramo if e del ramo else finiscono entrambi nel file pippo.txt. Il primo e l'ultimo echo vanno in stdout

riduzione1Annidata.sh

### Annidamento dei ridirezionamenti

```
NUM=1
echo "${NUM}"
if (( "${NUM}" <= "3" )) ; then
    ((NUM=${NUM}+1))
    echo "${NUM}"
    echo "vaffa" > cacchio.txt
else
    ((NUM=${NUM}+2))
    echo "${NUM}"
fi > pippo.txt
echo "${NUM}"
```

L'output in pippo.txt rimane quello dell'esempio di sinistra, mentre nel file cacchio.txt mi ritroco la riga con vaffa

# Ridirezionamenti di Stream di I/O (22)

## Esempi Ridirezionamento per blocchi di comandi

ridirezioneBlocchIfElse.sh

**NB: Anche i comandi dentro la condizione dell' if vengono ridirezionati assieme a quelli del blocco if then else**

```
if  ls ./out1.txt ; then
    echo "esiste"
else
    echo "non esiste"
fi &> pippo.txt
```

Se il file ./out1.txt esiste, allora nel file pippo.txt trovo,  
./out1.txt  
esiste

Se invece il file ./out1.txt non esiste,  
allora nel file pippo.txt trovo,  
ls: cannot access './out1.txt':  
 No such file or directory  
non esiste

ridirezioneBloccoWhile.sh

**NB: Anche i comandi dentro la condizione di for e while vengono ridirezionati come quelli del blocco do done**

```
while  ls ./out1.txt ; do
    echo "esiste ma ora ... "
    rm ./out1.txt
done &> pippo.txt
echo "non esiste "
```

Se il file ./out1.txt esiste, allora nel file pippo.txt trovo,  
./out1.txt  
esiste ma ora ...

ls: ./out1.txt': No such file or directory  
Se invece il file ./out1.txt non esiste,  
allora nel file pippo.txt trovo solo,  
ls: ./out1.txt': No such file or directory

# Ridirezione dell'input passato a riga di comando

## Here Documents <<

La word che segue il metacarattere << viene utilizzata come delimitatore finale dell'input da passare al comando a sinistra del metacarattere.

Viene ridirezionato nell'input tutto quello che compare tra la word esplicitata dopo il metacarattere << e fino a dove quella word compare ancora all'inizio di una riga.

NON vengono espansi eventuali metacaratteri presenti nella word.

Utilità del ridirezionamento: poter passare input come se provenisse da un file ma senza dover scrivere un file.

### Esempio:

```
while read A B C ; do echo $B ; done <<FINE
```

```
uno due tre quattro
```

```
alfa beta gamma
```

```
gatto cane
```

```
FINE
```

```
echo ciao
```

```
produce in output
```

```
due
```

```
beta
```

```
cane
```

```
ciao
```

# Raggruppamento di comandi (1)

**Se si racchiude una sequenza di comandi tra parentesi tonde, allora in esecuzione viene creata una subshell per eseguire quella sequenza dei comandi.**

**Il risultato restituito dalla subshell** (restituito dalla parentesi tonda) **è il risultato dell'ultimo comando eseguito nella subshell**, cioè l'ultimo comando eseguito tra quelli dentro le parentesi tonde.

Tutti i comandi condividono gli stessi stdin/stdout/stderr **utilizzandoli in sequenza**. Quindi all'output del primo comando dentro le parentesi viene concatenato l'output del secondo comando poi quello del terzo etc etc

**Ciò permette di trattare / ridirigere input ed output di tutti i comandi dentro le parentesi tonde come se fossero un solo comando.**

Esempio: con il comando:

**ls; pwd; whoami > out.txt**

visualizzo

nomi files in directory corrente

/home/vittorio

E dentro il file out.txt trovo

vittorio

Esempio: con il comando tra parentesi

**( ls; pwd; whoami ) > out.txt**

non visualizzo nulla

e dentro il file out.txt trovo

a1B a2B aB akB akmB akmtB

/home/vittorio

vittorio

# Raggruppamento di comandi (2)

stdin stdout e stderr dei singoli comandi dentro le parentesi tonde vengono concatenati

## concatenazione stdout

```
( cat file1.txt ; cat file2.txt ) | grep stringa
```

il comando grep legge, come se provenissero da tastiera, le righe di entrambi i file prima le righe di file1.txt e poi le righe di file2.txt

## concatenazione stderr

```
( cat file1.txt ; cat file2.txt ) 2| grep stringa
```

il comando grep legge, come se provenissero da tastiera, le righe di entrambi i file prima le righe di file1.txt e poi le righe di file2.txt

## concatenazione stdin

```
cat file1.txt | ( read RIGA1 ; usa RIGA1 ; read RIGA2 ; usa RIGA2 )
```

i due comandi read leggono una la prima e l'altro la seconda riga prodotte da cat

# Raggruppamento di comandi (3)

la bash è un po' stronza e cerca di ottimizzare, nonostante la nostra volontà

Esempio per far vedere che :

- **se dentro la parentesi tonda metto un solo comando, allora la bash padre non crea una altra shell figlia in cui far eseguire il singolo comando**

```
ps ; ( ps )
```

vedere che l'output dei due ps mostra una sola bash in entrambi i casi

lanciare poi

```
ps ; ( ps ; ps )
```

e vedere che nell'output dei due ps interni compaiono due bash, quella padre e una figlia

# Commenti Aggiuntivi da fare sulla PROSSIMA SLIDE

## Quella su uso di ridirezionamenti e GNU Coreutils

- Far vedere il comando **man man** ed evidenziare il concetto **di sezione del man** e le due **sezioni 1** (executable programs and shell commands) e **sezione 3** (library calls).
- Far capire che conviene (se possibile) usare in cascata più eseguibili già esistenti invece che scrivere un programma apposta da zero.
- Citare il pacchetto **coreutils** e ricordare che proviene dall'unione di più pacchetti precedenti (fileutils, shellutils, textutils) e suggerire di guardare cosa altro c'è .
- Descrivere l'esercizio proposto e la soluzione
- Descrivere le utilities **head tail sed cut cat grep** e poi **tee**.
- Occhio al parametro 4- passato a cut.
- Evidenziare che la maggior parte delle utilities prevedono un doppio comportamento, ovvero:
  - possono accettare dopo le opzioni uno o piu' argomenti che specificano il nome del/dei file da cui leggere input.
  - possono leggere input da stdin se non c'e' l'argomento nomefile o se c'e' un – come argomento finale.
- Fare un esempio in cui uso tail senza specificare un argomento nomefile per fargli usare input proveniente da stdin ed evidenziare il comportamento differente rispetto a come l'ho usato nell'esercizio
  - `cat dati.txt | tail -n 3`
- Aggiungere un esempio con l'utility **tee**
- Far vedere **tail -f** e mostrare che non viene gestita mutua esclusione sui file

# Esempio di uso di ridirezionamenti e GNU Coreutils

Cosa si puo' fare con sequenze di comandi, raggruppamenti, ridirezionamenti, ...?

Ne approfitto per farvi vedere alcune utilities che manipolano file di testo, appartenenti al progetto GNU Coreutils (unificazione dei vecchi pacchetti Fileutils, Shellutils e Textutils).

Vedi <http://www.gnu.org/software/coreutils/coreutils.html>

Dato un file di testo, di nome dati.txt, utilizzare programmi disponibili comunemente in un sistema linux per ottenere il seguente risultato:

Prendere le prime 2 righe del file e le ultime 3 righe del file stesso.

Di queste righe selezionare solo quelle che contengono la sequenza AL

Nelle righe rimaste, sostituire le lettere AL con le lettere CUF

Nelle righe cosi' modificate eliminare i primi 3 caratteri (mantenere dal 4° in poi)

Scrivere le righe modificate nel file output.txt

**dati.txt**

pappappero  
caracavALo  
piripiccione  
ammappete  
uffauffa  
pedalando  
avvAllare  
remare

**output.txt**

acavCUFo  
CUFlare

Soluzione:

(head -n 2 dati.txt ; tail -n 3 dati.txt ) | grep AL | sed 's/AL/CUF/g' | cut -b 4- > output.txt

# Esempi di uso di utilities in Coreutils

```
cat dati.txt | tail -n 3
```

```
tail -f /var/log/messages
```

```
cat dati.txt | tee a.txt b.txt
```

# sed - stream editor (coreutils) (1)

l'editor di stream, **sed** prevede una quantita' assurda di possibili comandi, vediamone alcuni come esempi. Lanciare man sed per ulteriori dettagli.

Nell'esempio precedente, `sed 's/AL/CUF/g'` Il carattere **g** serve a far sostituire, in ciascuna linea processata, **tutte** le occorrenze delle stringhe AL. In assenza del carattere g, in ciascuna riga verrebbe modificata solo la prima stringa AL incontrata.

## Esempi con sed

Sostituisce **la prima occorrenza** di togli con metti in ciascuna riga del file nomefile.

```
sed 's/togli/metti/' nomefile
```

Rimuovere **il primo tra i caratteri** a che trova in ciascuna riga del file nomefile

```
sed 's/a//'
```

Rimuovere il carattere in prima posizione di ogni linea che si riceve dallo standard input.

**^** significa inizio linea, **.** significa un carattere qualunque

```
sed 's/^..//'
```

Rimuovere **l'ultimo carattere** di ogni linea ricevuta dallo stdin. **\$** significa fine linea, il **.** significa un carattere qualunque

```
sed 's/..$/..$/'
```

Eseguo **due rimozioni insieme** ; Rimuovere il primo e l'ultimo carattere in ogni linea.

```
sed 's/..$/..$/'
```

Rimuove I primi 3 caratteri ad inizio linea.

```
sed 's/....//'
```

Rimuove I primi 4 caratteri ad inizio linea.

```
sed -r 's/..{4}//'
```

# sed - stream editor (coreutils) (2)

## Continua esempi con sed

To remove last n characters of every line (nell'esempio 3 caratteri)

```
sed -r 's/.{3}$//'
```

To remove everything except the 1st n characters in every line

```
sed -r 's/(.{3}).*\^1/'
```

To remove everything except the last n characters in a file

```
sed -r 's/.*(.{3})\^1/'
```

To **remove multiple characters** present in a file (**g means all occurrences** ):

```
sed 's/[aoe]//g'
```

To remove **all occurrences** of a pattern

```
sed 's/lari//g'
```

To delete only nth occurrences of a character in every line (2 occurrences in the example)

```
sed 's/u//2'
```

To delete everything in a line followed by a character

```
sed 's/a.*//'
```

To remove all alpha-numeric characters present in every line

```
sed 's/[a-zA-Z0-9]//g'
```

# Process Identifier di Shell bash: \$\$ e \$BASHPID

- Ogni Processo è identificato da un identificatore numerico univoco, il PID.
- Anche le shell in esecuzione posseggono un loro PID.
- Se occorre conoscere il PID di una shell in esecuzione, si usa la variabile **\$\$** che viene espansa con il PID della shell corrente.

Esempio:

```
echo il pid della shell è $$  
il pid della shell è 14726
```

- Se uso la variabile **\$\$** all'interno di uno script, vedo il PID della bash che esegue lo script.
- **Esiste una eccezione di comportamento.** Se raggruppo dei comandi facendoli eseguire in una subshell (), allora dentro le () la variabile **\$\$** mi fa vedere il PID della bash più esterna, non della subshell ().

Esempio:

```
echo -n pid fuori $$ ; ( echo -n pid dentro $$ ; pwd )  
pid fuori 14726 pid dentro 14726 /home/studente
```

- Se occorre usare il PID di una subshell specificata con (), occorre usare la variabile d'ambiente BASHPID. **La variabile BASHPID contiene il PID della bash corrente, anche se questa è una bash creata con ()**.

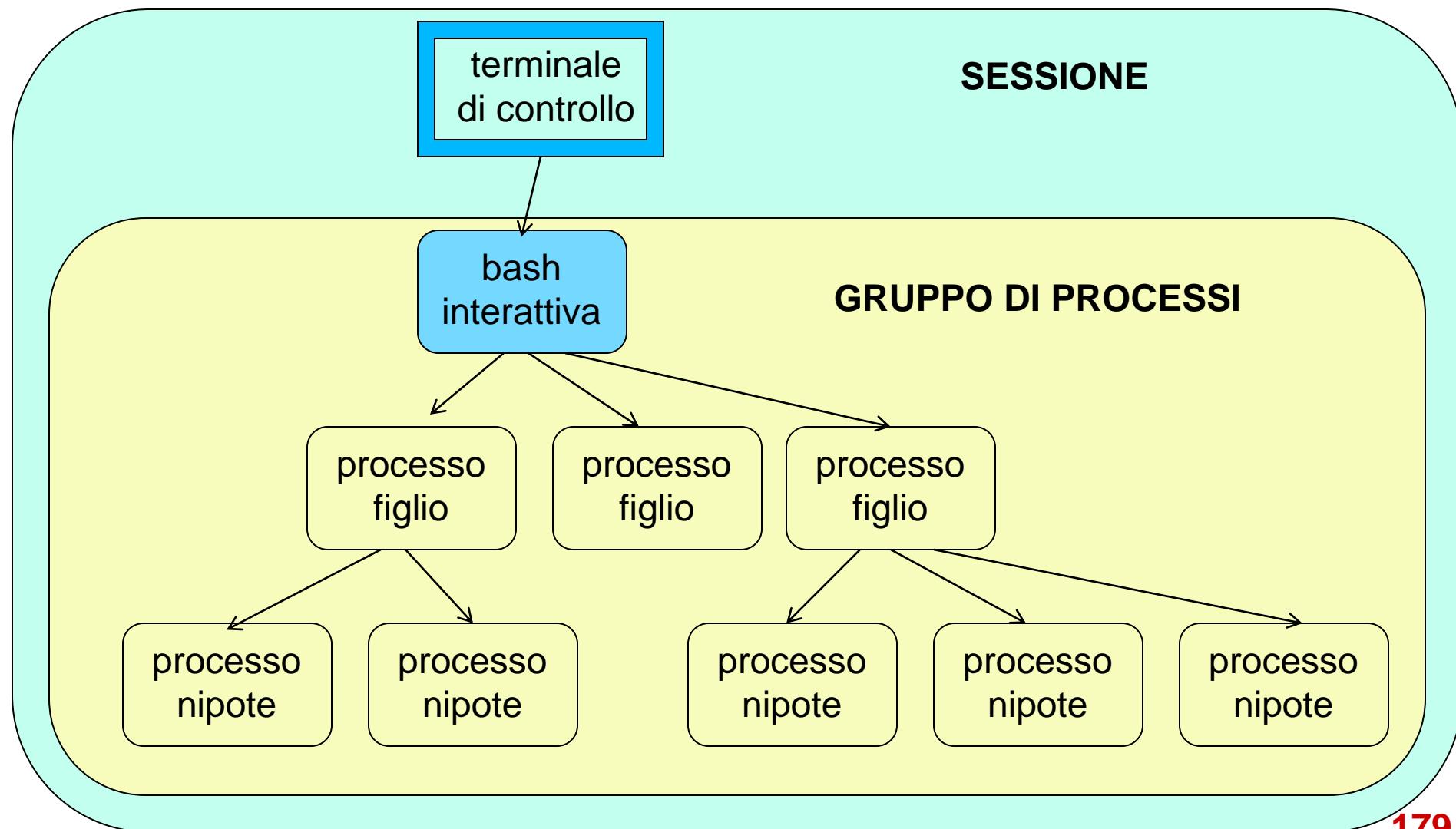
Esempio:

```
echo -n pid fuori $$ ; ( echo -n pid dentro $BASHPID; pwd )  
pid fuori 14726 pid dentro 22399 /home/studente
```

- Posso usare sempre la variabile BASHPID al posto della **\$\$**, però la var BASHPID è definita solo in bash e solo in bash delle versioni > 4. BASHPID è meno portabile

# Concetti di Processo, Sessione, Gruppo di Processi, Terminale di controllo del gruppo di processi (0)

- Scenario



# Concetti di Processo, Gruppo di Processi, Terminale di controllo del gruppo di processi (1)

- **Processi:** Un processo è la più piccola unità di elaborazione completa ed autonoma che può essere eseguita in un computer.
- Un **processo** è un insieme di thread di esecuzione operanti all'interno di un contesto, il quale comprende uno spazio di indirizzamento in memoria ed una tabella dei descrittori di file aperti per quel processo.
- **Gruppo di processi** (process group): Un processo può lanciare l'esecuzione di altri processi: questi altri processi appartengono allo stesso gruppo di processi del processo padre, a meno che non si svolgano azioni che modificano il gruppo di appartenenza.
- **Terminale di controllo:** Un processo lanciato in esecuzione può avere un "controlling terminal" (un terminale da cui è controllato, che è l'astrazione di terminale (console=video+tastiera) da cui prende gli standard input output ed error).
- **Terminale di controllo del gruppo di processi** Un processo lanciato in esecuzione eredita lo stesso "controlling terminal" dal padre che lo ha lanciato, a meno che non si svolgano azioni che sganciano il processo dal terminale di controllo. Quindi tutti i processi di uno stesso gruppo di processi condividono lo stesso terminale di controllo.

# Creazione della Sessione

- Per gestire l'insieme di processi, il kernel necessita di raggruppare i processi in modo più complesso che non la semplice relazione padre-figlio.
- Perciò viene usata l'astrazione di "**sessione**" e di "**gruppo di processi**".
- Un utente normalmente apre una **shell interattiva** (di login o no) che viene inserita dal sistema operativo in un terminale (la window che rappresenta la console monitorvideo+tastiera) e da questa shell eseguirà operazioni varie, tra cui l'esecuzione di comandi, eseguibili binari e script.
- Il terminale in cui la shell interattiva esegue è detto "**terminale di controllo**" (controlling terminal).
- La shell interattiva all'inizio **crea una sessione**, specificando un nuovo sessionId, e **lega la sessione al terminale di controllo**. Questa shell interattiva diventa così il leader della sessione.
- I processi discendenti di quella shell apparterranno alla stessa sessione, a meno che non si eseguano operazioni di distacco.
- La shell interattiva prende come stdin stdout ed stderr quelli che il terminale gli fornisce.
  - I comandi, eseguibili binari e script lanciati dalla shell interattiva ereditano i file aperti del padre, quindi ereditano anche gli stdin, stdout ed stderr del terminale.

# Motivazione della Sessione

- Quando un utente si disconnette da un sistema, il kernel deve terminare tutti i processi che l'utente sta ancora eseguendo
  - altrimenti, gli utenti lascerebbero un gran numero di vecchi processi in attesa di input che non potranno mai arrivare.
- Come determinare quali processi terminare?
- Per semplificare questa attività, i processi sono organizzati in sessioni.
- Il leader della sessione è il processo che ha creato la sessione.
- L'ID della sessione è uguale al pid del processo che ha creato la sessione tramite la chiamata di sistema setsid ().
  - La funzione setsid () non accetta argomenti e restituisce il nuovo ID di sessione., cioè il PID del processo leader.
- Tutti i discendenti di quel processo sono quindi membri di quella sessione a meno che non si rimuovano specificamente da essa.

# Terminale di controllo (Controlling Terminal) di una sessione

- Ogni sessione è legata a un terminale da cui i processi nella sessione ricevono il loro input e ai quali inviano il loro output.
- Quel terminale può essere la console locale della macchina, un terminale connesso su una linea seriale o uno pseudo terminale che si collega a una finestra del window manager locale o attraverso una rete.
- Il terminale a cui è correlata una sessione è chiamato terminale di controllo (o control tty) della sessione.
- **Un terminale può essere il terminale di controllo per una sola sessione alla volta.**
- Sebbene il terminale di controllo per una sessione possa essere modificato, solitamente l'operazione di stabilire il terminale di controllo di una sessione viene eseguita solo dal processo che gestiscono l'accesso iniziale di un utente a un sistema o ad una finestra del window manager.

# Chiusura del Terminale e conseguente Terminazione dei processi della sessione

- Quando viene chiuso il terminale di una sessione, i processi che appartengono a quella sessione, non possono più continuare l'esecuzione e vengono terminati.
- L'operazione di terminazione viene realizzata dal sistema operativo mandando ad ogni processo un segnale di terminazione detto SIGHUP ("signal hang up").
- Ricevendo questo segnale, ogni processo termina.
- In tal modo si liberano le risorse del sistema operativo legate ai processi legati alla sessione terminata a causa della chiusura (voluta o inaspettata) del terminale di controllo della sessione.
- Nota Bene: un processo può essere configurato, da programma, per reagire diversamente all'arrivo di un segnale.

# Processi in background e in foreground (1)

## • Processi in **foreground**

- Processi che “controllano” il terminale dal quale sono stati lanciati, nel senso che hanno il loro standard input collegato al terminale e impegnano il terminale non permettendo l'esecuzione di altri programmi collegati a quel terminale, fino alla loro terminazione
- In ogni istante, un solo processo è in foreground

## • Processi in **background**

- Vengono eseguiti in parallelo rispetto all'esecuzione della bash, nel senso che permettono alla bash che li ha lanciati di leggere ed eseguire altri comandi e di lanciare altri programmi. Usano una copia dei fd della bash che li ha lanciati, quindi condividono con questa stdin/stdout/stderr. Poiché lo standard input rimane collegato al terminale della bash che li ha lanciati, quando terminiamo l'esecuzione della finestra del terminale, il terminale chiude lo stdin ed i processi vengono terminati. Per far proseguire l'esecuzione dei processi in background dopo la terminazione del terminale occorre sganciare i processi dal terminale col comando disown (vedi piu' avanti).

## • **Jobs** di una shell

- Processi in background o sospesi **solo figli** di quella shell (vedi jobs).

## • Job control

- Permette di portare i processi da background a foreground e viceversa

# Processi in background e in foreground (2)

- & lancia un processo direttamente in background (in \$! trovero' il pid)  
**Esempio:** `prova &`
- `^Z` sospende un processo in foreground
- `^C` termina un processo in foreground
- `bg` riprende l'esecuzione in background di un processo sospeso
- `jobs` produce una lista numerata dei processi in background o sospesi nella shell corrente
  - il numero tra parentesi quadre che indica ciascun processo **non e' il pid** bensì **un indice del job** che si usa per gestire il job, premettendo il carattere %

- `fg %n` porta in foreground un processo sospeso
- `kill` elimina il processo specificato dal proprio identificatore pid oppure specificato dal numero del job

**Esempio:**

`kill 6152` dove 6152 e' il pid del processo  
`kill %2` dove 2 e' l'indice del processo nella lista visualizzata dal comando `jobs`

- `disown -[ar] jobs` sgancia il job dalla shell interattiva che lo ha lanciato i jobs sono specificati con pid o **%indice**
- **Nota:** `jobs` si applica ai soli processi attualmente in esecuzione (o sospesi) nella shell, mentre la lista completa dei processi in esecuzione nel sistema può essere ottenuta con i comandi `ps -ax` oppure con `top`.

## Precisazione:

# \$! PID dell'ultimo processo lanciato in background

Quando lancio un processo direttamente in background, mediante l'operatore & allora il Process Identifier PID del processo appena lanciato viene messo nella variabile \$! della shell che ha lanciato quel processo.

La variabile \$! della shell mantiene quel valore fino a che la stessa shell non lancia in background un altro processo.

```
program.exe arg1 arg2 arg3 .... argN &  
echo il PID di program.exe e\' $!
```

Anche quando lancio il programma in background, sganciandolo dalla shell mediante l'utility nohup (vedi dopo), nella variabile \$! trovo il PID del processo appena lanciato in background

```
nohup program.exe arg1 arg2 arg3 .... argN &  
echo il PID di program.exe e\' $!
```

Nota Bene

Al contrario, se metto in background con l'utility bg un processo che era stato sospeso con CTRL+Z, allora dentro la variabile \$! non viene messo il PID di quel processo, cioe' la variabile \$! non viene modificata.

# Processi in background e in foreground (3)

- **Nota:** l'operatore & inserito nella riga di comando serve anche a indicare la fine degli argomenti passati al comando, cosi' come fanno gli operatori ; && || etc etc.
- Se si usa l'operatore & bisogna omettere il ;  
Es:  
./fai.sh 3 & ; ./fai.sh 2 &  
la presenza del ; produce **errore**  
-bash: syntax error near unexpected token `;'  
Il comando va lanciato senza il ;  
./fai.sh 3 & ./fai.sh 2 &

## ----- Prova chiarificatrice

Provare a lanciare la sequenza di comandi

sleep 23 & sleep 20

e immediatamente digitare

CTRL+Z

poi lanciare il comando

jobs

poi lanciare il comando

bg

e nuovamente lanciare il comando

jobs

# Processi in background e in foreground (3bis)

## Precisazione per Tarlo3 (andrea)

### Concetto di current job e simbolo %% per usarlo

- Tratto da `man bash`, nella parte relativa a Job Control

The symbols `%%` and `%+` refer to the shell's notion of the **current job**, which is the last job stopped while it was in the foreground or started in the background.

The previous job may be referenced using `%-`. If there is only a single job, `%+` and `%-` can both be used to refer to that job.

In output pertaining to jobs (e.g., the output of the **jobs command**), the **current job is always flagged with a +**, and the **previous job with a -**.

A single `%` (with no accompanying job specification) also refers to the current job.

(sleep 50 ; echo UNO )

`^Z`

`bg`

(sleep 50 ; echo DUE) &

**disown %%** (o **disown %** o anche solo **disown**) sgancia quello con DUE

Se invece lanciassi

`disown %-` sgancerei quello con UNO

Nota bene: man mano che i job terminano o che li sgancio, cambiano il job corrente e il job precedente.

# Processi in background e in foreground (4)



**Vedere esempi slide successiva**

# Processi in background e in foreground (5)

**Verifichiamo che i jobs possono anche essere delle subshell lanciate per eseguire dei comandi raggruppati:**

Lanciare una nuova shell interattiva, eseguire i seguente comando e osservare:

```
( sleep 50 ; echo finito > merda.txt ) &  
jobs
```

```
ps          (notare che esiste una shell che esegue sleep)
```

Dopo 50 secondi verificare che esiste il file merda.txt e poi eliminarlo.

**Verifichiamo che i jobs muoiono con la shell:**

Lanciare una nuova shell interattiva, eseguire i seguente comando e osservare:

```
( sleep 50 ; echo finito ; echo scrivo > merda.txt ) &  
jobs ; ps  
exit
```

Da una nuova shell lanciare jobs ; ps

Aspettare 51 secondi e poi verificare se esiste il file merda.txt. **Non c'e'.**

Attenzione: **il segnale viene processato solo quando il processo è attivo, quindi solo al termine della sleep. probabilmente esegue anche echo finito**  
Se elimino "echo finito" vedrò ugualmente il file merda.txt

**Controprova Verifichiamo che i jobs sganciati sopravvivono alla morte della shell**

Lanciare una nuova shell interattiva, eseguire i seguente comando e osservare:

```
( sleep 50 ; echo finito ; echo scrivo > merda.txt ) &
```

```
jobs ; ps
```

```
disown
```

o disown %1 se il job ha indice 1

```
jobs ; ps
```

```
exit
```

Da una nuova shell lanciare jobs ; ps

Aspettare 50 secondi e poi verificare se esiste il file merda.txt. **C'e'.**

# Processi in background e in foreground (6)

## Lanciare processo già “sganciato” dalla shell

Esiste un comando esterno alla shell che puo' essere utile per sganciare un processo dalla shell che lo ha lanciato il tutto in una sola istruzione. Puo' essere comodo per non doversi occupare di reperire il pid del processo creato o l'indice del job creato.

In pratica, lanciando il comando:

**nohup** comando arg1 arg2 .... argN &

Ottengo lo stesso effetto che avrei lanciando la sequenza di comandi

**comando** arg1 arg2 .... argN &

**disown** *sgancio dalla shell l'ultimo processo mandato in background*

nohup e' poco comodo perche' non permette, se non con dei trucchi, di lanciare una sequenza di comandi ma solo un comando singolo (con i suoi argomenti).

# Segnali - kill (1)

Interruzioni software mandati ai processi per notificare eventi asincroni)

Un segnale è una interruzione software, provocata in un processo destinazione, per notificare un evento asincrono.

Il comando `kill` invia segnali a processi.

Il tipo di segnale viene specificato con un simbolo oppure con il valore numerico.

Il processi destinazione vengono specificati mediante il loro pid.

Supponiamo che 7777 sia il pid di un processo.

I seguenti comandi inviano il segnale SIGTERM al processo destinazione, con ciò ordinandogli di terminare. Il segnale viene accettato solo se proviene dall'utente che esegue il processo (effective user). Il processo può intercettare il segnale e gestirlo diversamente o addirittura ignorarlo. Come si vede, se non si specifica un segnale, **per default** viene inviato il segnale **SIGTERM** (valore 15) di terminazione del processo.

kill	7777
kill	<b>-15</b> 7777
kill	<b>-SIGTERM</b> 7777

Esiste un altro segnale di terminazione del processo, SIGKILL o KILL che però il processo non può ignorare.

kill	<b>-9</b> 7777
kill	<b>-SIGKILL</b> 7777
kill	<b>-KILL</b> 7777

E' possibile inviare un segnale di terminazione a tutti i processi che il processo bash corrente può far terminare (cioè tutti i suoi figli diretti, non i nipoti)

kill	<b>-9</b> -1
------	--------------

# Segnali - kill (2)

Interruzioni software mandati ai processi per notificare eventi asincroni)

Altri possibili segnali sono:

kill	<b>-SIGTSTP</b>	pid	(è il segnale lanciato con CTRL Z )
kill	<b>-SIGCONT</b>	pid	(riprende processo sospeso, usato da fg e bg)
kill	<b>-SIGINT</b>	pid	(è il segnale lanciato con CTRL C)

ed altri ancora.

E' possibile visualizzare l'elenco dei segnali gestiti eseguendo il comando

```
kill      -l
```

**NOTA BENE: RISPOSTA DILAZIONATA AI SEGNALI.**

**Se un processo è bloccato in attesa di input da rete oppure fermo in una sleep (cioè in stato waiting), riceverà e gestirà il segnale solo al termine dell'I/O o della sleep.**

# Segnali - trap (3)

Ricezione di signal ed esecuzione di azione

Il comando trap definisce l'azione da svolgere al ricevimento di un elenco di segnali, esplicitando il nome di una funzione oppure una stringa di codice bash da eseguire.

**trap    action    lista\_di\_segnali**

ESEMPIO:        eseguire così:        ./lancia\_riceviSIGUSR1e2.sh

## **riceviSIGUSR1e2.sh**

```
#!/bin/bash
trap "echo \"ricevuto SIGUSR1 !!! Termino !!!\"; exit 99" SIGUSR1

ricevutoSIGUSR2() {
    echo "ricevuto SIGUSR2, continuo";
}
trap ricevutoSIGUSR2 SIGUSR2

while true ; do echo -n "."; sleep 1; done
```

## **lancia\_riceviSIGUSR1e2.sh**

```
#!/bin/bash
./riceviSIGUSR1e2.sh &
CHILDPID=$!
sleep 5 ; echo "mando SIGUSR2"; kill -s SIGUSR2 ${CHILDPID}
sleep 5 ; echo "mando SIGUSR2"; kill -s SIGUSR2 ${CHILDPID}
sleep 5; echo "mando SIGUSR1"; kill -s SIGUSR1 ${CHILDPID}
sleep 4;
```

# Segnali - trap (4)

La configurazione dell'azione si mantiene-  
Annullare l'esecuzione dell'azione

## riceviSIGUSR1e2.sh

```
#!/bin/bash
trap "echo \"ricevuto SIGUSR1 !!! Termino !!!\"; exit 99" SIGUSR1

NUMRICEVUTISIGUSR2=0
ricevutoSIGUSR2() {
    ((NUMRICEVUTISIGUSR2=${NUMRICEVUTISIGUSR2}+1))
    if ((${NUMRICEVUTISIGUSR2}==2)) ; then
        echo "ricevuto 2° SIGUSR2, disabilito gestione SIGUSR2";
        trap ":" SIGUSR2                                # non faccio fare piu' niente
    else echo "ricevuto ${NUMRICEVUTISIGUSR2}-esimo SIGUSR2, continuo";
    fi
}
trap ricevutoSIGUSR2 SIGUSR2
while true ; do echo -n "."; sleep 1; done
```

-Mando il primo SIGUSR2 per dimostrare che il trap setta la funzione da lanciare alla ricezione del signal.

-Mando il secondo SIGUSR2 per dimostrare che il trap mantiene il settaggio anche dopo l'arrivo di un primo segnale.

-Mando il terzo SIGUSR2 per dimostrare che posso cambiare la routine di gestione anche da DENTRO la routine stessa.

## lancia\_riceviSIGUSR1e2.sh

```
#!/bin/bash
./riceviSIGUSR1e2.sh &
CHILDPID=$!
for (( i=0; ${i}<3; i=${i}+1 )) ; do
    sleep 3; echo "mando SIGUSR2"; kill -s SIGUSR2 ${CHILDPID} ;
done
sleep 3; echo "mando SIGUSR1"; kill -s SIGUSR1 ${CHILDPID};
wait ${CHILDPID}
```

# Attesa terminazione di processo figlio di shell: **wait** (1)

Supponiamo che una shell bash lanci in esecuzione un processo e lo metta in background, poi la shell può fare qualcosa mentre il programma è in esecuzione, e infine la shell vuole aspettare che il programma lanciato termini.

Per fare questo devo utilizzare il comando built-in **wait** a cui passo come argomento il process identifier del processo di cui attendere la terminazione. Il comando wait termina quando termina il processo di cui è stato passato il PID.

```
program.exe arg1 arg2 arg3 .... argN &  
PIDsalvato=$!  
echo "il PID di program.exe e\' ${PIDsalvato}"  
... faccio qualcosa d'altro ...  
wait ${PIDsalvato}           <-- attende terminazione di program.exe
```

**NB: il comando wait può essere invocato SOLO dalla shell che ha lanciato il processo di cui vogliamo attendere la terminazione. Se l'attesa per la terminazione viene invocata da una shell diversa, il comando wait termina subito e restituisce 127.**

**NB: il comando wait restituisce come exit status l'exit status restituito dal processo figlio specificato dal PID. Se il PID specificato non corrisponde ad un processo figlio in esecuzione, il comando wait termina subito e restituisce 127.** esempio:

```
sleep 20 &  
wait $!    <-- attende fine di sleep 20 e restituisce risultato di sleep
```

# Attesa terminazione di processo figlio di shell: **wait** (2)

Il comando wait può prendere diversi argomenti a riga di comando:

- **un elenco di PID** : in tal caso wait aspetta la terminazione di tutti i processi indicati e restituisce come risultato il risultato dell'ultimo processo nella lista di PID, indipendentemente dall'ordine in cui terminano
- **un elenco di jobs** : in tal caso wait aspetta la terminazione di tutti i jobs indicati
- **nessun argomento** : in tal caso wait aspetta la terminazione di tutti i processi figli della shell in cui il comando wait è stato lanciato e restituisce exit status 0 non essendo indicato uno specifico figlio di cui restituire l'exit status.

```
(sleep 20 ; exit 3 ) &
```

```
wait $!
```

```
echo "il valore restituito da wait è: " $?
```

<-- attende terminazione di exit 3  
<-- visualizza 3

```
(sleep 20 ; false ) &
```

```
wait $!
```

```
echo "il valore restituito da false è: " $?
```

<-- attende terminazione di false  
<-- visualizza 1

```
progr &
```

```
pid1=$!
```

```
prog2 &
```

```
pid2=$!
```

```
prog3 &
```

```
pid3=$!
```

```
wait ${pid1} ${pid3} ${pid2} <-- attende terminazione dei 3 prog e restituisce l' exit status  
di prog2 cioè del programma il cui pid compare per ultimo nell'elenco 200
```

# **wait, processi Zombie, processi Orfani, processo init (1)**

Un processo (padre) genera un processo figlio e lo esegue in background.

Il processo figlio prima o poi **termina** e restituisce un valore intero.

Il processo padre vuole sapere quale è il valore restituito dal figlio per sapere se tutto è andato bene o no. A questo scopo, il processo padre esegue il comando **wait pidfiglio** che attende la terminazione del processo figlio avente pid pidfiglio e restituisce il risultato del processo figlio.

**1.Se il processo figlio termina prima del processo padre**, il sistema operativo rilascia le risorse occupate dal processo figlio **ma mantiene nelle sue tabelle una struttura pcb (process control block) con una descrizione del processo terminato**. Questa struttura conserva anche il **pid** e il **risultato** del processo figlio. In questo momento il processo figlio è uno **zombie** poiché è terminato ma la sua struttura descrittiva è ancora presente nelle tabelle del sistema operativo.

- **La struttura pcb viene eliminata solo quando il padre invoca il comando wait** (o una system call waitpid che fa la stessa cosa) per attendere la terminazione del figlio. A quel punto il processo figlio sparisce dalle tabelle e il suo pid può essere riutilizzato per altri processi.

**2.Se invece il processo padre termina senza fare la wait per il figlio, il processo figlio diventa orfano.** Quando un processo orfano termina, oppure quando uno zombie diventa orfano perché termina il padre, **l'orfano viene adottato dal processo init**, quello con pid 1 che ha originato tutti i processi al boot. Gli orfani diventano figli di init. **Ogni tanto il processo init chiama la wait sui propri figli**, anche quelli adottati ovviamente, e così fa rilasciare i pcb degli orfani.

- Quindi, **morto il padre, i figli che terminano vengono eliminati (no zombie)** 201

# Processi Zombie, Processi Orfani, processo init (2)

Per quale motivo un processo padre non fa una wait per attendere la terminazione di un processo figlio?

1. o per sbaglio, perché il programmatore se ne è dimenticato,
2. oppure appositamente, per impedire che un altro suo nuovo figlio prenda dal sistema operativo proprio il pid del processo figlio terminato.

In entrambi i casi, si rischia di esaurire i pid disponibili nel sistema operativo.

# killall - Terminazione di tutti i processi con un dato nome

Il comando **killall** viene usato, solitamente, per terminare l'esecuzione di tutti i processi che hanno lo stesso nome; quel nome viene passato come argomento al comando killall. Il comando killall per default invia a quei processi il segnale SIGTERM, a meno che non si specifichi un diverso segnale.

In realtà, il comando killall può servire più genericamente ad inviare ai processi un segnale specificato mediante un argomento a riga di comando.

Inoltre, alcuni parametri permettono di individuare in modo diverso i processi a cui inviare il segnale.

Esempio:

Supponiamo che, **nella directory corrente** esistano i file binari eseguibili di nome **attendiA.exe** e **attendiC.exe** e che esista uno script di comandi **attendiB.sh**, e che l'esecuzione di ciascuno di questi duri qualche minuto.

Posso lanciare in background più istanze di ciascun eseguibile/script così:

```
for (( i=1; $i < 10 ; i=$i+1 )) ; do ./attendiA.exe & ./attendiB.sh & done
```

Se voglio, posso terminarli tutti i processi attendiA.exe ed attendiB.sh usando il seguente comando:

```
killall -r 'attendi[[:upper:]]*'
```

Il comando ordina di usare l'espressione regolare (che segue l'opzione -r) per selezionare il nome dei processi tra attualmente in esecuzione da eliminare.

**Notare che gli apici semplici impediscono che sia la bash a interpretare i metacaratteri. L'interpretazione viene così fatta dalla killall con i nomi dei processi in memoria e non con quelli della directory corrente.**

# killall - Interpretazione del nome dei processi in memoria

Verifichiamo che la killall interpreta i metacaratteri cercando di **associarli ai nomi dei processi in memoria e non al nome dei file nel filesystem.**

Supponiamo che, **nella directory corrente** esistano i file binari eseguibili di nome **attendiA.exe** e **attendiC.exe** e che esista uno script di comandi **attendiB.sh**, e che l'esecuzione di ciascuno di questi duri qualche minuto.

Posso lanciare in background più istanze di ciascun eseguibile/script così:

```
for (( i=1; $i < 10 ; i=$i+1 )) ; do ./attendiA.exe & ./attendiB.sh & done
```

Ora lanciamo il seguente comando, SI NOTI CHE NON CI SONO APICI SINGOLI:

```
killall -r attendi[[:upper:]]*
```

**Senza gli apici semplici**, che impedirebbero alla bash di interpretare i metacaratteri, **l'interpretazione viene PRIMA effettuata dalla bash con i nomi dei file della directory corrente e, SOLO IN UN SECONDO MOMENTO, viene effettuata dalla killall con i nomi dei processi in memoria.**

la bash interpreta i metacaratteri e, in pratica lancerei

```
killall -r attendiA.exe attendiB.sh attendiC.exe
```

Allora, la killall mostra un output che fa capire che ha cercato in memoria il processo attendiC.exe ma non l'ha trovato

**attendiC.sh: no process found**

# Precedenze degli operatori

## Separatori di comando, condizionali e non

Gli operatori che delimitano la fine di una riga di comando sono:

; & e l'andata a capo **newline**

Gli operatori che connettono due comandi sono:

&& || ; & e l'operatore speciale |

Gli operatori && e || hanno la stessa precedenza.

Gli operatori & e ; hanno la stessa precedenza.

Gli operatori && e || hanno maggior precedenza degli operatori & e ;

L'operatore speciale | ha la precedenza maggiore di tutti.

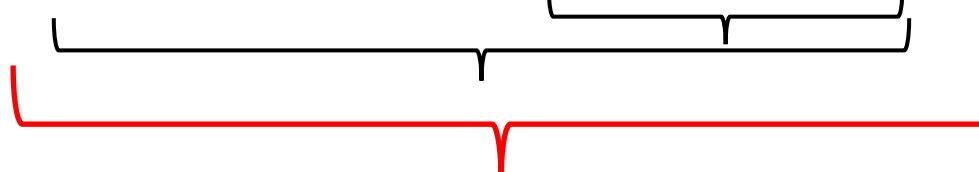
Che significa questo?

Significa che, se scrivo una sequenza di comandi connessi da alcuni separatori,

l'esecuzione dei comandi precede da sinistra verso destra, ma

- Ciascun insieme di comandi connessi da separatori a maggior precedenza va visto come un blocco unico,
- A ciascuno di questi blocchi “connessi da maggior precedenza” va applicato l'effetto dei separatori a minor precedenza presenti sulla destra del blocco.

Esempio: progA ; progB && progC && progD | progE & progF



# Per i puristi

A rigore, l'operatore `|` non dovrebbe essere considerato un operatore come gli altri, poiché l'esecuzione dei comandi che esso connette non è separabile, quindi i due o più comandi connessi dalle `|` dovrebbero essere trattati come un unico comando.

Per semplicità, consideriamo la `|` un operatore a priorità maggiore di `;` e `&` ed anche di `||` e `&&`

# Esempi di Precedenze degli operatori (1)

```
$ echo A && sleep 10 && echo B & echo C
```

```
[1] 30472
```

```
A
```

```
C
```

*qui termina il comando echo C*

```
$
```

*qui passano 10 secondi*

```
$ B
```

*messaggio di echo B*

```
[1]+ Done
```

```
$ echo A && sleep 10 && echo B
```

Notare che avendo l'operatore & minore precedenza di && accade che l'operatore & viene applicato a tutta la sequenza di comandi

```
$ echo A && sleep 10 && echo B & echo C
```

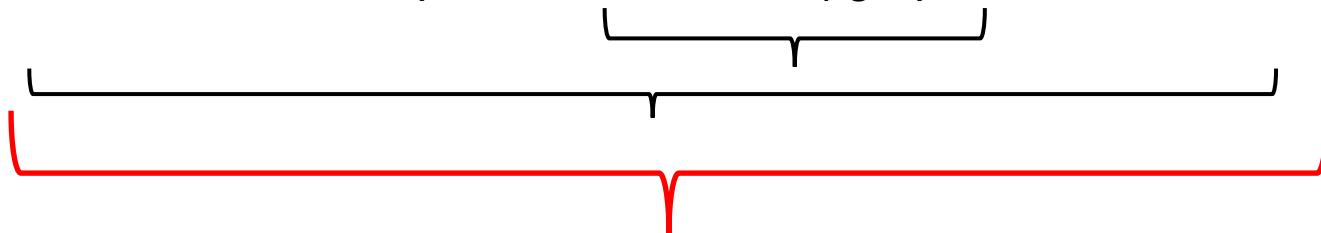
Quindi tutta la sequenza di tre comandi qui sopra viene messa in background mentre l'eseguibile echo C viene eseguito immediatamente.

NB: il \$ che compare a inizio riga e' il prompt della shell.

# Esempi di Precedenze degli operatori (2)

Esempio:

```
$ echo aaA ; echo abB && sleep 10 && echo abC | grep C && echo aaF & echo aaG
```



Ricordando che echo restituisce 0 (cioe' ok),

Allora a video si vedra':

```
aaA
```

```
[1] 42388
```

```
aaG
```

```
abB abB non e' stato "greppato"
```

qui passano 10 secondi prima di vedere qualcosa ....

```
$ abC abC e' passato dal grep
```

```
aaF aaF non e' stato greppato
```

```
[1]+ Done echo abB && sleep 10 && echo abC | grep C && echo aaF  
da qui si capisce cosa e' stato lanciato in background
```

```
$
```

# Modifica di Precedenze degli operatori mediante raggruppamento con { }

```
$ ps ; echo A && sleep 10 && { ps ; echo B & echo C ; }
```

PID	PPID	PGID	WINPID	TTY	UID	STIME	COMMAND
22652	40532	22652	41208	pty1	1001	12:45:12	/usr/bin/ps
40532	41172	40532	40384	pty1	1001	Oct 6	/usr/bin/bash
41172		1	41172	41172	?	1001	Oct 6 /usr/bin/mintty

A

PID	PPID	PGID	WINPID	TTY	UID	STIME	COMMAND
22548	40532	22548	22560	pty1	1001	12:45:22	/usr/bin/ps
40532	41172	40532	40384	pty1	1001	Oct 6	/usr/bin/bash
41172		1	41172	41172	?	1001	Oct 6 /usr/bin/mintty

[1] 29540

B

C

[1]+ Done

echo B

\$

Notare che nell'output del secondo **ps** rimane la sola shell bash con pid 40532 dovuto al fatto che eseguo il gruppo di comandi nella stessa shell (quella che legge le parentesi graffe) poiche' li racchiudo tra **parentesi graffe**.

NB: prima della graffa chiusa SERVE il ;

NB: il \$ a inizio riga e' il prompt

# Modifica di Precedenze degli operatori mediante raggruppamento con { }

Evidenziamo, con un esempio, che serve il ; prima della graffa chiusa.  
Invece, se uso parentesi tonde, il ; finale prima della tonda chiusa non e' necessario.

```
$ $ ps ; echo A && sleep 10 && { ps ; echo B & echo C }
```

```
>
```

```
$
```

Poiche' manca il punto e virgola prima della parentesi graffa chiusa, la shell non capisce dove finisce la riga di comando e chiede all'utente di digitare il resto della riga di comando, visualizzando il prompt |

# Modifica di Precedenze degli operatori mediante raggruppamento con ( )

```
$ ps ; echo A && sleep 10 && ( ps ; echo B & echo C )
  PID  PPID  PGID  WINPID  TTY   UID  STIME COMMAND
40532  41172  40532  40384  pty1  1001 Oct  6 /usr/bin/bash
23792  40532  23792  22456  pty1  1001 12:46:05 /usr/bin/ps
41172      1  41172  41172 ?    1001 Oct  6 /usr/bin/mintty

A
  PID  PPID  PGID  WINPID  TTY   UID  STIME COMMAND
21968  41428  41428  21804  pty1  1001 12:46:15 /usr/bin/ps
40532  41172  40532  40384  pty1  1001 Oct  6 /usr/bin/bash
41172      1  41172  41172 ?    1001 Oct  6 /usr/bin/mintty
41428  40532  41428  41428  pty1  1001 12:46:15 /usr/bin/bash
```

B

C

\$

**Notare** nell'output del secondo **ps** il processo aggiuntivo **/usr/bin/bash** con pid 41428 dovuto al fatto che eseguo un gruppo di comandi in una sottoshell poiche' li racchiudo tra **parentesi tonde**

Notare che dopo l'ultimo comando dentro le parentesi tonde, posso omettere il ; finale che infatti nell'esempio non compare.

# Occhio al significato di “eseguito nella stessa shell” quando uso { }

Supponiamo che lo script **chiamaps.sh** contenga solo la chiamata a **ps**

```
#!/bin/bash
```

```
ps
```

```
$ ps ; echo A && sleep 10 && { ./chiamaps.sh ; echo C ; }
```

PID	PPID	PGID	WINPID	TTY	UID	STIME	COMMAND
40532	41172	40532	40384	pty1	1001	Oct 6	/usr/bin/bash
41172		1	41172	41172	?	1001	Oct 6 /usr/bin/mintty
17500	40532	17500	44100	pty1	1001	13:19:53	/usr/bin/ps

A

PID	PPID	PGID	WINPID	TTY	UID	STIME	COMMAND
40532	41172	40532	40384	pty1	1001	Oct 6	/usr/bin/bash
41172		1	41172	41172	?	1001	Oct 6 /usr/bin/mintty
<b>17368</b>	40532	17368	44104	pty1	1001	13:20:03	<b>/usr/bin/bash</b>
17424	17368	17368	44064	pty1	1001	13:20:03	/usr/bin/ps

C

\$

**Notare**, nell'output del comando **ps** contenuto nello script **./chiamaps.sh** , il processo aggiuntivo **/usr/bin/bash** con pid **17368** dovuto al fatto che eseguo uno script (per cui serve una subshell) anche se il gruppo di comandi e' racchiuso tra **parentesi graffe****213**

# Occhio ancora al significato di “eseguito nella stessa shell” quando uso { source ... }

```
$ ps ; echo A && sleep 10 && { source ./chiamaps.sh ; echo C ; }
```

PID	PPID	PGID	WINPID	TTY	UID	STIME	COMMAND
40532	41172	40532	40384	pty1	1001	Oct 6	/usr/bin/bash
19072	40532	19072	17380	pty1	1001	13:25:59	/usr/bin/ps
41172		1	41172	41172	?	1001	Oct 6 /usr/bin/mintty

A

PID	PPID	PGID	WINPID	TTY	UID	STIME	COMMAND
18132	40532	18132	17288	pty1	1001	13:26:09	/usr/bin/ps
40532	41172	40532	40384	pty1	1001	Oct 6	/usr/bin/bash
41172		1	41172	41172	?	1001	Oct 6 /usr/bin/mintty

C

\$

**Notare**, nell'output del comando **ps** contenuto nello script **./chiamaps.sh** , non compare una shell aggiuntiva poiche' ho eseguito lo script **./chiamaps.sh** mediante il comando **source**

# Parameter Expansion – Uso di stringhe (1)

## Estrazione di sottostringhe da variabili

La bash fornisce alcuni operatori che vengono specificati all'interno dei simboli che vengono utilizzati per ottenere il contenuto di una variabile, la variable expansion.

**Tali operatori forniscono una stringa che e' una parte del contenuto della variabile oppure una parte modificata del contenuto della variabile.**

Il contenuto originale della variabile non viene modificato, a meno che io non effettui un assegnamento alla variabile originale.

**Se l'estrazione di parte del contenuto o la sostituzione non sono possibili, gli operatori restituiscono l'intero contenuto della variabile, senza modifiche.**

Gli operatori che effettuano una sostituzione, normalmente ne effettuano una soltanto, anche se fossero possibili piu' sostituzioni. Però qualche operatore consente di effettuare più sostituzioni.

Per effettuare piu' sostituzioni complesse si può però invocare piu' volte il comando salvando di volta in volta il risultato ottenuto.

Anticipiamo alcune definizioni:

definiamo      suffisso=che sta alla fine      prefisso=che sta all'inizio.

# Parameter Expansion – Uso di stringhe (2)

## Estrazione di sottostringhe da variabili

Esempio di uso: estrarre numero tra [] in VAR="13 qualcosa con [ o ] fine"

Definiamo suffisso=che sta alla fine prefisso=che sta all'inizio.

**pattern** puo' contenere wildcard che cercano di matchare con sottostringhe in VAR  
**pattern** puo' contenere anche variabili

`${VAR%%pattern}`

`$ echo ${VAR%]*}`

Rimuovo il piu' **lungo suffisso** che fa match con stringa orig

[13

Rimuovo fino alla fine a destra

la sottostringa **piu' lunga** che inizia con ]

`${VAR%pattern}`

`$ echo ${VAR%]*}`

Rimuovo il piu' **corto suffisso** che fa match con stringa orig

[13] qualcosa con [ o

Rimuovo fino alla fine della stringa originale

la sottostringa **piu' corta** che inizia con ]

`${VAR##pattern}`

`$ echo ${VAR##*[}`

Rimuovo il piu' **lungo prefisso** che fa match con stringa orig

o ] fine

Rimuovo, dall'inizio dell'originale, la sottostringa piu' lunga

che finisce con [

`${VAR#pattern}`

`$ echo ${VAR#*[}`

Rimuovo il piu' **corto prefisso** che fa match con stringa orig

13] qualcosa con [ o ] fine

Rimuovo, dall'inizio dell'originale, la sottostringa piu' corta

che finisce con [

# Parameter Expansion – Uso di stringhe (3) sottostringhe da variabili

es: VAR="alfabetagamma"

`${#VAR}` viene espansa nella stringa che esprime la lunghezza in byte del contenuto di VAR. Con la variabile VAR di esempio produce la stringa "17". Produce la stringa "0" se la variabile VAR non esiste o se è vuota.

`${VAR/pattern/string}` cerca nel contenuto di VAR la sottostringa piu' lunga che fa match con il pattern specificato (con wildcard) e lo **sostituisce** con string. Se sono possibili piu' sostituzioni viene sostituita solo la sottostringa piu' vicina all'inizio.  
ALTRA="vaf"; echo "\${VAR/b\*a/k\${ALTRA}p}"  
produce in output: alfakvafp

`${VAR:offset}` sottostringa che parte dal offset-esimo carattere del contenuto di VAR  
L'offset del primo carattere e' zero. Gli argomenti vengono valutati aritmeticamente. Lo stesso per il prossimo operatore

`${VAR:offset:length}` sottostringa lunga length che parte dal offset-esimo carattere del contenuto di VAR  
es: VAR="alfabetagamma" ; DA="2" ; FINOA="5" ;  
echo "\${VAR:\$DA}: \${FINOA}+3" ;  
produce in output: fabetaga

# Parameter Expansion – Uso di stringhe (4) estrazione con sostituzione da variabili

esempio: come effettuare piu' sostituzioni nel contenuto di una variabile

```
#!/bin/bash
VAR="a1BDaxxx2BaDxxx3BbDxx4BcDxxx5BDxxx6BdD"
PREVIOUS=${VAR}
while true ; do
    VAR=${VAR/B?D/ZZZ}
    if [ ${VAR} == ${PREVIOUS} ] ; then
        break ;
    else
        PREVIOUS=${VAR}
    fi
done
echo "VAR=${VAR}"
```

Lo script visualizza

VAR=a1BDaxxx2ZZZxxx3ZZZxx4ZZZxxx5BDxxx6ZZZ

---

NB: più semplicemente si poteva usare:

VAR=\${VAR//B?D/ZZZ}

(vedi dopo)

# Parameter Expansion – Uso di stringhe (4bis)

## ulteriori dettagli su sostituzione in variabili

L'operatore di sostituzione varia il suo comportamento se inserisco uno dei 3 caratteri speciali subito dopo il primo / dopo il nome di variabile, in particolare:

`${VAR//pattern/string}` quando dopo il primo / c'e' un altro / allora TUTTE le sottostringhe che fanno match con il pattern specificato vengono sostituite, non solo la prima.  
esempio: sostituisce tutti i cane con gatto {VAR//cane/gatto}  
esempio: sostituisce tutti gli asterischi \* con \\* per impedire che il contenuto della variabile possa essere interpretato.  
 `${VAR/\^*\^\\*}`

`${VAR/#pattern/string}` quando dopo il primo / c'e' un # allora il pattern viene sostituito SOLO SE si trova all' INIZIO della variabile.

`${VAR/%pattern/string}` quando dopo il primo / c'e' un % allora il pattern viene sostituito SOLO SE si trova alla FINE della variabile.

# Parameter Expansion – Uso di stringhe (5) operatori vari su variabili

Espansione verso **nomi** di variabili corrispondenti ad un prefisso pattern

`${!VarNamePrefix*}` restituisce un elenco con tutti i nomi delle variabili il cui nome inizia con il prefisso specificato VarNamePrefix

Esempio: se esistono le seguenti variabili

BASH=/bin/bash  
BASH\_ALIASES=()  
BASH\_ARGC=()  
BASH\_ARGV=()  
BASH\_CMDS=()  
BASH\_LINENO=()  
BASH\_SOURCE=()  
BASH\_VERSION='4.1.17(9)-release'  
CYG\_SYS\_BASHRC=1

ed eseguo il comando

`echo ${!BASH_AR*}`

vedro' in output

BASH\_ARGC BASH\_ARGV

# APPUNTI DA RISISTEMARE: escludere directory da ricerca con find

escludo da find la ricerca nella directory ./BUTTA

```
find ./ -path ./BUTTA -prune -o -type f -name "*.c" -exec grep -H rand '{}' \; |  
more
```

escludo da find la ricerca nella directory ./ESAMI e anche nella ./BUTTA

```
find ./ -path ./ESAMI -prune -o -path ./BUTTA -prune -o -type f -name "*.c" -  
exec grep -H rand '{}' \;
```

# APPUNTI DA RISISTEMARE: Follie bash ovvero Scorciatoie

**!!** riesegue l'ultimo comando appena eseguito

**!n** riesegue l'ennesimo comando presente nella storia, dove 'n' è il numero del comando da rieseguire

**!stringa** riesegue l'ultimo comando che inizia con i caratteri specificati in 'stringa'

**!stringa:p** visualizza l'ultimo comando che inizia con i caratteri specificati in 'stringa'

**!?comando?** ricerca il comando specificato tra punti interrogativi

**fc 4** permette di modificare in comando numero 4 con l'editor predefinito (solitamente vi)

**fc -e 'nome' 4** permette di modificare in comando numero 4 con l'editor 'nome' specificato

**^comando1^comando2** riesegue l'ultimo comando eseguito che contiene la parola 'comando1' sostituendola con 'comando2'.

**history** visualizza l'elenco di tutti i comandi eseguiti

**CTRL-U** cancella tutta la riga dalla posizione del cursore all'inizio della riga

**CTRL-K** cancella tutta la riga dalla posizione del cursore alla fine della riga

**CTRL-W** cancella una parola dalla posizione del cursore all'inizio della riga

**ALT-D** cancella una parola dalla posizione del cursore alla fine della riga

**freccia sinistra** sposta il cursore di un carattere a sinistra

**freccia destra** sposta il cursore di un carattere a destra

**freccia su** scorre la storia dei comandi a ritroso

**freccia giu'** scorre la storia dei comandi in avanti

**tasto home** sposta il cursore all'inizio della riga

**CTRL-A** sposta il cursore all'inizio della riga

**tasto fine** sposta il cursore alla fine della riga

**CTRL-E** sposta il cursore alla fine della riga

**ALT-F** sposta il cursore alla fine della parola successiva (F sta per forward, successivo)

**CTRL-B** sposta il cursore all'inizio della parola precedente (B sta per backward, precedente)

**CTRL-T** inverte gli ultimi due caratteri a sinistra del cursore, cioè ab diventa ba (T sta per transpose)

**ALT-T** inverte le ultime due parole a sinistra del cursore, cioè cp pippo pluto diventa cp pluto pippo

**ALT-U** trasforma in maiuscolo la parola su cui si trova il cursore (U sta per uppercase, cioè maiuscolo)

**ALT-L** trasforma in minuscolo la parola su cui si trova il cursore (L sta per lowercase, cioè minuscolo)

**tasto TAB** espande il nome di un file o di un comando

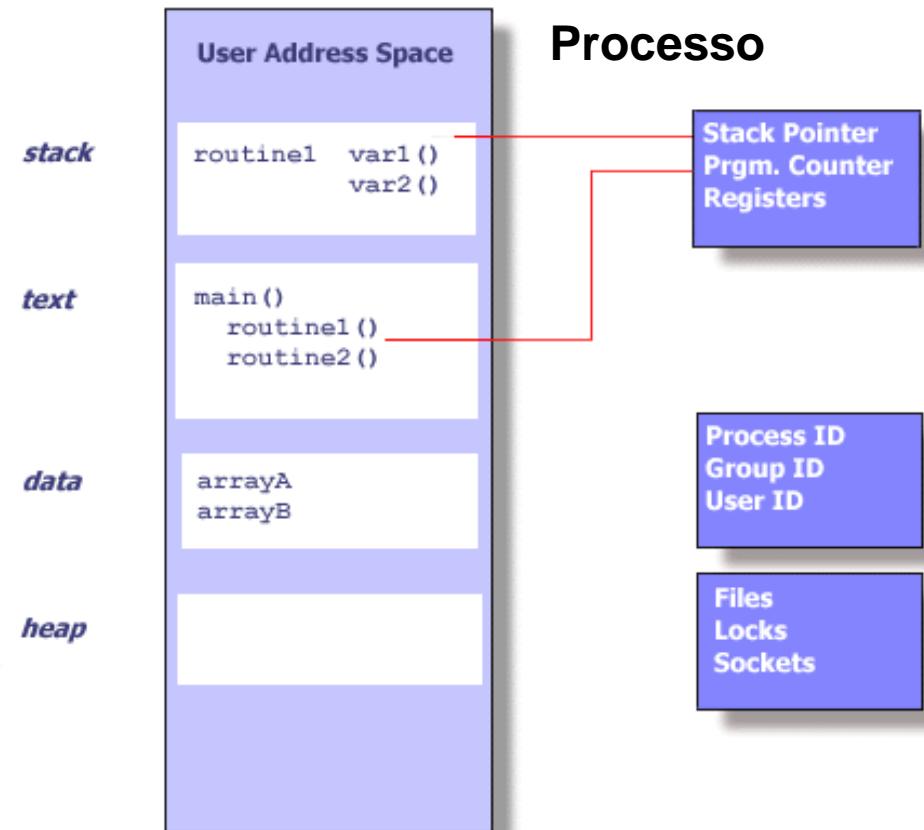
# Thread e POSIX Thread

Introduzione alla  
programmazione concorrente  
in linguaggio C  
in ambito POSIX

...

# I THREAD

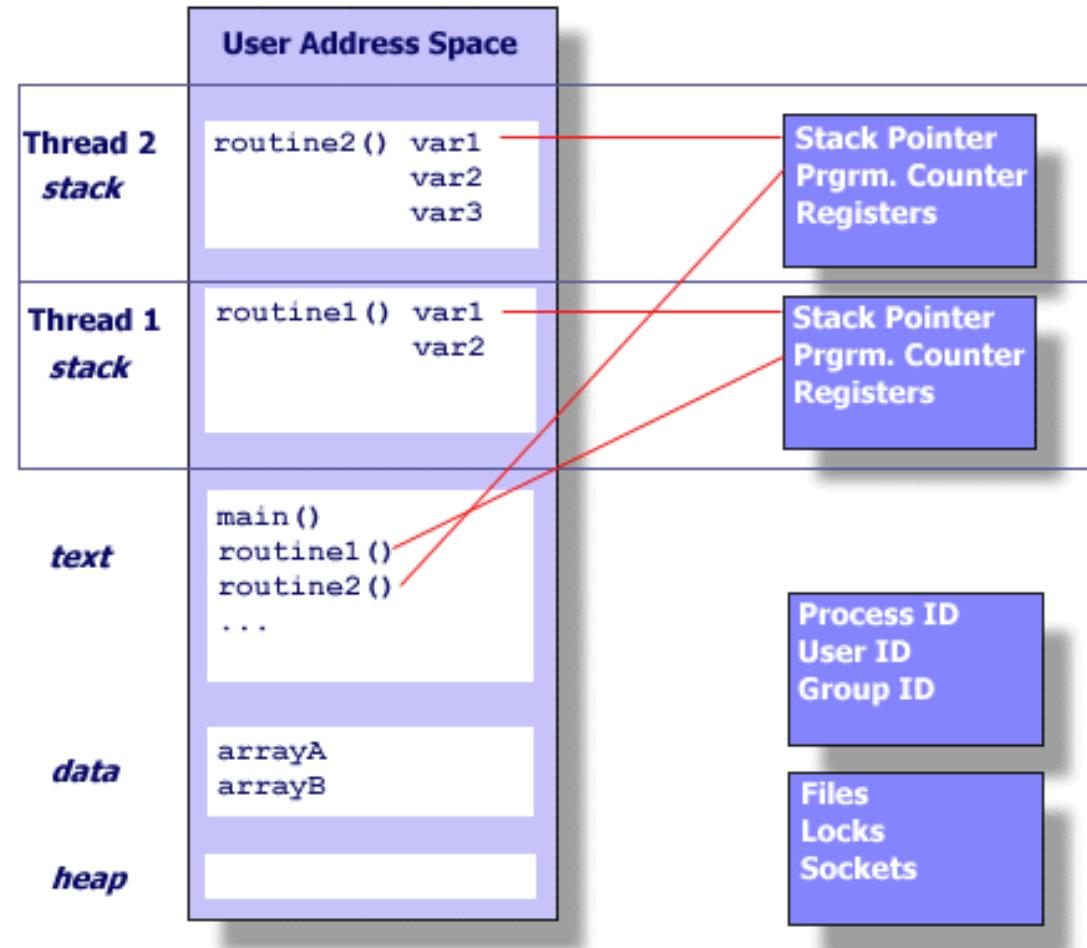
- **Un thread è un singolo flusso di istruzioni, all'interno di un processo, che lo scheduler può fare eseguire separatamente e concorrentemente con il resto del processo.**
- Un thread può essere pensato come una procedura che lavora in parallelo con altre procedure all'interno di un processo
- Per eseguire in parallelo con il resto del processo, un thread deve possedere delle strutture dati (un proprio contesto) cioè un proprio ambiente di esecuzione, per realizzare il proprio flusso di controllo.
- **Ogni processo ha il proprio contesto**, ovvero il proprio Process ID, Program Counter, Stato dei Registri, Stack, Codice, Dati, File Descriptors, Entità IPC, Azioni dei segnali.
- Il Codice del processo è pensato per eseguire procedure sequenzialmente.
- L'astrazione dei thread vuole consentire di eseguire procedure in parallelo (concorrentemente), ovviamente scrivendo tali procedure in modo opportuno.
- **Ciascuna procedura da eseguire in parallelo sarà un thread.**



# Il contesto di esecuzione di ciascun Thread

- Un thread è un singolo flusso di istruzioni, all'interno di un processo, che lo scheduler può fare eseguire separatamente e concorrentemente con il resto del processo. Per fare questo uno thread deve possedere un proprio contesto di esecuzione.
- Un Processo può avere più thread.
- Tutti i thread di uno stesso processo condividono le risorse del processo (dati globali e CPU) ed eseguono nello stesso spazio utente.
- Ciascun Thread può usare tutte le **variabili globali** del processo, e condivide **la tabella dei descrittori di file** del processo.
- Ciascun thread in più potrà avere anche dei **propri dati locali**, e sicuramente avrà un proprio **Stack**, un proprio **Program Counter**, un proprio **Stato dei Registri** ed una propria variabile **errno**.
- Dati globali ed entità del Thread (Dati, Stack, Codice, Program Counter, Stato dei Registri) rappresentano lo **stato di esecuzione del singolo thread**.

Processo con 2 thread



# Vantaggi e Svantaggi nell'uso di Thread

## □ **Vantaggi:**

- Visibilità dei dati globali: condivisione di oggetti semplificata.
- Più flussi di esecuzione.
- gestione semplice di eventi asincroni (I/O per esempio)
- Comunicazioni veloci. Tutti i thread di un processo condividono lo stesso spazio di indirizzamento, quindi le comunicazioni tra thread sono più semplici delle comunicazioni tra processi.
- Context switch veloce. Nel passaggio da un thread ad un altro di uno stesso processo viene mantenuto buona parte dell'ambiente.

## □ **Svantaggi:**

- Concorrenza invece di parallelismo:
  - occorre gestire la mutua esclusione per evitare che più thread utilizzino in maniera scoordinata i dati condivisi, modificandoli in momenti sbagliati.
- La concorrenza deve essere gestita
  - sia da **chi scrive il programma** che usa i thread.
  - sia dal **sistema operativo che implementa le funzioni di libreria e le system calls utilizzate "contemporaneamente" da più thread di uno stesso processo.**
  - Le funzioni delle librerie di sistema e le system calls devono essere **rientranti (thread safe call)**.

# Operazioni Atomiche: definizione

il termine operazione qui è volutamente generico

- **In generale**, un'operazione che usa dei dati condivisi è **atomica** se è indivisibile, ovvero **se nessun'altra operazione**, che usa quegli stessi dati condivisi, **può cominciare prima che la prima sia finita**, e quindi non può esserci interleaving tra le diverse operazioni. Il risultato di quella operazione è sempre lo stesso se parte dalle stesse condizioni iniziali.
- Quando parleremo di istruzioni macchina che accedono alla memoria e introdurremo la paginazione e il page fault, vedremo che la parte **verde** di questa affermazione dovrà essere modificata e meglio precisata, ottenendo l'affermazione **blu** qui sotto:
- **un'operazione, che usa dati condivisi, è atomica, rispetto alle operazioni che usano gli stessi dati condivisi, se viene eseguita in modo indivisibile.**
  - **Può però capitare che una operazione indivisibile debba essere interrotta per permettere l'esecuzione di una operazione più urgente.**
  - **In caso di interruzione, un modo per rendere comunque l'operazione atomica consiste nell'attendere la fine dell'interruzione e far ripartire dall'inizio l'operazione interrotta che si voleva fosse eseguita atomicamente.**
  - **Poiché in caso di interruzione riparto da capo, le condizioni iniziali da cui l'operazione riparte potrebbero essere nel frattempo cambiate.**
  - **Ma, a parità di condizioni di partenza, il risultato di una operazione atomica sarà sempre lo stesso.**

# Le istruzioni in linguaggio C sono Atomiche ?

- **Le istruzioni in linguaggio C sono atomiche? NO.**
  - in generale le istruzioni in linguaggio di alto livello non sono atomiche.
- **Le istruzioni di solo assegnamento di una costante ad una variabile e le istruzioni di sola lettura di una variabile, sono atomiche? NO**
  - **Sono atomiche solo se la dimensione della variabile è minore dell'ampiezza del bus dati.**
  - Ad esempio, in un processore i386, con bus dati a 32 bit, l'assegnamento seguente viene addirittura tradotto in DUE istruzioni assembly.  
(vedere test\_assegnamento\_var\_grande.c)

```
uint64_t G;  
int main()  
{  
    G=2034573288479;  
}
```



```
mov    DWORD PTR G, -1241209825  
mov    DWORD PTR G+4, 473
```

NB: Se non disponete di un processore con bus dati avente ampiezza a 32 bit, potete comunque generare il codice così se compilate con il flag `-m32` ed aggiungete il flag `-S` per generare l'assembly.

# Le istruzioni assembly sono Atomiche ?

- **Le istruzioni di un programma in assembly sono atomiche? NO, non tutte.**
  - Il linguaggio assembly mette a disposizione anche delle specie di macro che vengono tradotte dall'assembler in una sequenza di istruzioni macchina. Si pensi alle istruzioni call che invoca una funzione e che deve salvare alcuni dati sullo stack, Ovviamente, le traduzione in linguaggio macchina di quelle macro non sono eseguibili atomicamente.
- Restringiamo il campo, allora, alle sole istruzioni assembly che non siano delle macro assembly.
  - **Alcune istruzioni assembly elementari non sono atomiche.** L'istruzione inc incrementa di 1 il valore di un byte in memoria, ma non è atomica perche deve:
    - ▶ fare una lettura tramite bus, del dato in memoria per portarlo in un registro,
    - ▶ incrementare di 1 il contenuto di quel registro,
    - ▶ portare il nuovo contenuto nella locazione di memoria.
- **La sola copia di un dato da registro a memoria (o in senso contrario, da memoria a registro) è atomica? In generale si, se l'ampiezza del bus dati è maggiore o uguale alla dimensione del registro.**
  - In generale, **se un'istruzione richiede più di un accesso al bus, non è atomica.**
  - Inoltre, parlando di paginazione (e in particolare di page fault), vedremo che in qualche caso sarà necessario far ripartire l'istruzione da capo.

# Cosa c'è di Atomico?

## Supporto ISA alla Mutua Esclusione: istruzioni compare-exchange o compare-and-swap (1)

I processori, nel loro livello ISA, mettono a disposizione delle istruzioni macchina basiche e atomiche per consentire l'implementazione di flussi di esecuzione atomici più complessi che si basano sul valore di una variabile «di guardia». Queste istruzioni sono diverse da processore a processore-

Nei processori Intel delle famiglie x86 (IA-32) e x64 (EM64T, Intel 64) esiste un'istruzione **cmpxchg** ed un prefisso **lock** che modifica il comportamento di questa istruzione, rendendolo atomico. In altre famiglie di processori si parla di istruzioni compare-and-swap.

L'istruzione **lock cmpxchg** vuole due argomenti esplicativi ed uno implicito. Il primo argomento esplicito è l'indirizzo di una **variabile intera** in memoria, il secondo argomento esplicito è il **nome di un registro** in cui c'è già il valore da assegnare alla variabile. L'argomento隐式 è il **registro eax** in cui deve essere posto il **valore da confrontare** col valore della variabile.

L'istruzione **lock cmpxchg** preleva il valore della variabile puntata dall'indirizzo, lo confronta col valore contenuto nel registro eax, se i due valori sono uguali assegna alla variabile il nuovo valore (contenuto nel registro passato come secondo argomento). In pratica, atomicamente, se la variabile ha il valore cercato allora le viene assegnato il nuovo valore, altrimenti mantiene il suo vecchio valore.

# Cosa c'è di Atomico?

## Supporto ISA alla Mutua Esclusione: istruzioni compare-exchange o compare-and-swap (2)

Le istruzioni simili a compare-exchange servono a realizzare, in modo atomico, la verifica del valore di una variabile globale, la quale indica se la risorsa è occupata o no. Se la variabile vale 0 viene settata ad 1. Confronto ed assegnamento vengono eseguiti assieme ed atomicamente.

```
int occupato = 0; /* variabile globale */
```

### compare-exchange

```
while( 1 ) {  
    if ( occupato == 0 ) {  
        occupato =1;  
        Operazioni eseguite atomicamente;  
        occupato = 0;  
    }  
    break;  
}
```

```
while( 1 ) {  
    if ( occupato == 0 ) {  
        occupato =1;  
        Operazioni eseguite atomicamente;  
        occupato = 0;  
    }  
}
```

# System Call (e funzioni) NON RIENTRANTI

- i thread di un processo usano il s.o. mediante system call che usano dati e tabelle di sistema dedicate al processo.
- **Le syscall dovrebbero essere costruite in modo da poter essere utilizzate da più thread contemporaneamente.**
- **Alcune** syscall invece non sono costruite per essere usate da più thread contemporaneamente.
- Ad es: la funzione `char *inet_ntoa()` scrive il proprio risultato in una variabile (un buffer) di sistema dedicata al processo (che è visibile al processo) e restituisce al chiamante un puntatore a tale variabile. Se due thread di uno stesso processo eseguono "nello stesso istante" la chiamata a due `inet_ntoa()` ognuno provoca la scrittura di un valore nella variabile condivisa. Cosa leggono i due chiamanti dopo che le chiamate sono terminate?

- thread1 chiama `inet_ntoa`  
- `inet_ntoa` scrive dentro var  
- thread1 legge da var

- thread2 chiama `inet_ntoa`  
- `inet_ntoa` scrive dentro var  
- thread2 legge da var

buffer **var** della libc  
(libreria standard del C)  
condivisa dai thread  
del processo

130.136.1.1

# Thread Safe Call

- Le implementazioni dei **thread** per soddisfare gli **standard POSIX** offrono delle **funzioni thread safe**, cioè che non causano problemi nella scrittura/lettura di strutture dati interne al s.o e condivise dai thread di uno stesso processo.
- Il termine **Rientrante (Reentrant)** è sinonimo di **thread safe**.
- In particolare tutte le funzioni dello standard ANSI C e le funzioni degli standard POSIX.1, sono thread safe, ad eccezione di alcune: strerror, inet\_ntoa, asctime, ctime, getlogin, rand, readdir, strtok, ttyname, gethostXXX, getprotoXXX, getservXXX
- Per ovviare al problema delle funzioni di libreria non rientranti, sono state rese disponibili altre funzioni, che invece sono implementate in modo rientrante. Solitamente, il nome delle funzioni rientranti finisce con **\_r**
- Ad esempio, la funzione `char *strerror(int errnum);` fa cose diverse ma restituisce il risultato nello stesso modo della `inet_ntoa` e infatti **non è rientrante**.
  - Abbiamo visto che esiste una funzione alternativa, rientrante, **strerror\_r**, disponibile se definiamo il simbolo `_POSIX_C_SOURCE` con un valore  $\geq 200112L$
  - `int strerror_r(int errnum, char *buf, size_t buflen);`

- thread1 chiama `strerror_r` passandogli l'indirizzo di un proprio buffer
- `strerror_r` scrive nel buffer **del** thread1
- thread1 legge il proprio buffer

*No such file or directory*

- thread2 chiama `strerror_r` passandogli l'indirizzo di un proprio buffer
- `strerror_r` scrive nel buffer **del** thread2
- thread2 legge il proprio buffer

*Cannot allocate memory*

# POSIX Thread

- I Thread sono stati standardizzati. IEEE POSIX 1003.1c (1995) specifica l'interfaccia di programmazione (Application Program Interface - API) dei thread. I thread POSIX sono noti come **Pthread**.
- Le API per Pthread distinguono le funzioni in 3 gruppi:
  - **Thread management:** funzioni per creare, eliminare, attendere la fine dei pthread
  - **Mutexes:** funzioni per supportare un tipo di sincronizzazione semplice chiamata "mutex" (abbreviazione di **mutua esclusione**). Comprende funzioni per creare e eliminare la struttura per mutua esclusione di una risorsa, **acquisire** e **rilasciare** tale risorsa.
  - **Condition variables:** funzioni a supporto di una **sincronizzazione** più complessa, **dipendente dal valore** di **variabili**, secondo i modi definite dal programmatore. Comprende funzioni per creare e eliminare la struttura per la sincronizzazione, per **attendere** e **segnalare** le modifiche delle variabili.

# POSIX Thread API

Convenzione sui nomi delle funzioni:

Gli identificatori della libreria dei Pthread iniziano con **pthread\_**

<b>pthread_</b>	indica gestione dei pthread in generale
<b>pthread_attr_</b>	funzioni per gestione proprietà dei thread
<b>pthread_mutex_</b>	gestione mutua esclusione
<b>pthread_mutexattr_</b>	proprietà delle strutture per mutua esclusione
<b>pthread_cond_</b>	gestione delle variabili di condizione
<b>pthread_condattr_</b>	proprietà delle variabili di condizione
<b>pthread_key_</b>	dati speciali dei thread

il file **pthread.h** contiene le definizioni dei pthread

# Compilazione di programmi che usano Pthread

- Il file **pthread.h** contiene le definizioni dei pthread
- Normalmente si puo' compilare secondo il dialetto **-ansi**
- Per aderire anche allo standard POSIX, nella sua prima versione originaria (IEEE Std 1003.1), occorre anche definire il simbolo `-D_POSIX_SOURCE=1` oppure `-D_POSIX_C_SOURCE=1`
- Il dialetto **-ansi** però non comprende alcune funzioni messe a disposizione recentemente dalle librerie pthread, in particolare le API relative ai semafori per distinguere letture e scritture su variabili (le funzioni che operano sul tipo di dato **pthread\_rwlock\_t**). Quindi compilando con il dialetto **-ansi**, le parti del file `pthread.h` relative a queste funzioni `pthread_rwlock_*` vengono escluse dalla compilazione. Qualora occorra utilizzare la funzione **strerror\_r** oppure le funzioni di tipo `pthread_rwlock_*` occorre invece compilare secondo un dialetto piu' recente, ad esempio secondo lo standard `-std=gnu99` oppure occorre definire il simbolo **\_POSIX\_C\_SOURCE** con un valore  $\geq 200112L$
- In un programma che usa i pthread, è bene definire, all'inizio di ciascun file C, e **prima** delle inclusioni degli header di libreria standard, il simbolo **#define \_THREAD\_SAFE**  
Ciò consente al preprocessore di selezionare, quando esistono, le implementazioni thread safe delle funzioni di libreria.

Analogamente, invece di **\_THREAD\_SAFE** (di cui si parla nel file `/usr/include/features.h`) si puo' definire **\_REENTRANT**.

- **Nota Bene:** le funzioni `inet_ntoa()` `strerror()` sono intrinsecamente **NON** thread safe. Anche se definite il simbolo **\_THREAD\_SAFE** non potete usare con tranquillità quelle funzioni perché potrebbero darvi problemi.

# Linking di programmi che usano Pthread

- Durante la fase di **linking**, usando il *gcc*, aggiungere il flag **-Ipthread** per usare la libreria dei pthread **libpthread.so**.
- Inserire il flag **-Ipthread** alla fine della riga di comando assieme agli altri -l

Ad es:            `gcc -ansi -o thr1 thr1.o -Ipthread`

- Esiste anche la possibilità di usare un equivalente flag apposito **-pthread** (senza la l).
- Ve lo sconsiglio, usate il tradizionale -l mettendolo alla fine.

# API per creazione ed esecuzione di Pthread

```
int pthread_create( pthread_t * thread, pthread_attr_t *attr,  
                      void* (*start_routine)(void *), void * arg );
```

- crea una thread e lo rende eseguibile, cioè lo mette a disposizione dello scheduler che prima o poi lo farà partire.
- Il primo parametro **thread** è un puntatore ad un identificatore di thread in cui verrà scritto l'identificatore del thread creato.
- Il terzo parametro **start\_routine** è il nome (indirizzo) della procedura da fare eseguire dal thread. Deve avere come unico argomento un puntatore.
- Il secondo parametro seleziona caratteristiche particolari: può essere posto a NULL per ottenere il comportamento di default.
- Il quarto parametro è un puntatore che viene passato come argomento a **start\_routine**. Tale puntatore solitamente punta ad una area di memoria allocata dinamicamente.

```
void pthread_exit (void *retval);
```

- termina l'esecuzione del thread da cui viene chiamata, immagazzina l'indirizzo **retval**, restituendolo ad un altro thread che attende la sua fine.
- Il sistema libera le risorse allocate al thread.
- Il caso del programma principale (**main**) è particolare.
- Se il **main** termina prima che i thread da lui creati siano terminati e non chiama la funzione **pthread\_exit**, allora tutti i thread sono terminati. se invece il **main** chiama **pthread\_exit** allora i thread possono continuare a vivere fino alla loro teminazione.

# Identifieri dei Pthread

Il tipo di dato **pthread\_t** è il tipo di dato che contiene l'identificatore univoco di un pthread.

Due funzioni utili a maneggiare gli identifieri di pthread sono :

`pthread_t pthread_self(void);`

restituisce l'identificatore del thread che la chiama.

`int pthread_equal( pthread_t pthread1, pthread_t pthread2 );`

restituisce 1 se i due identifieri di pthread sono uguali

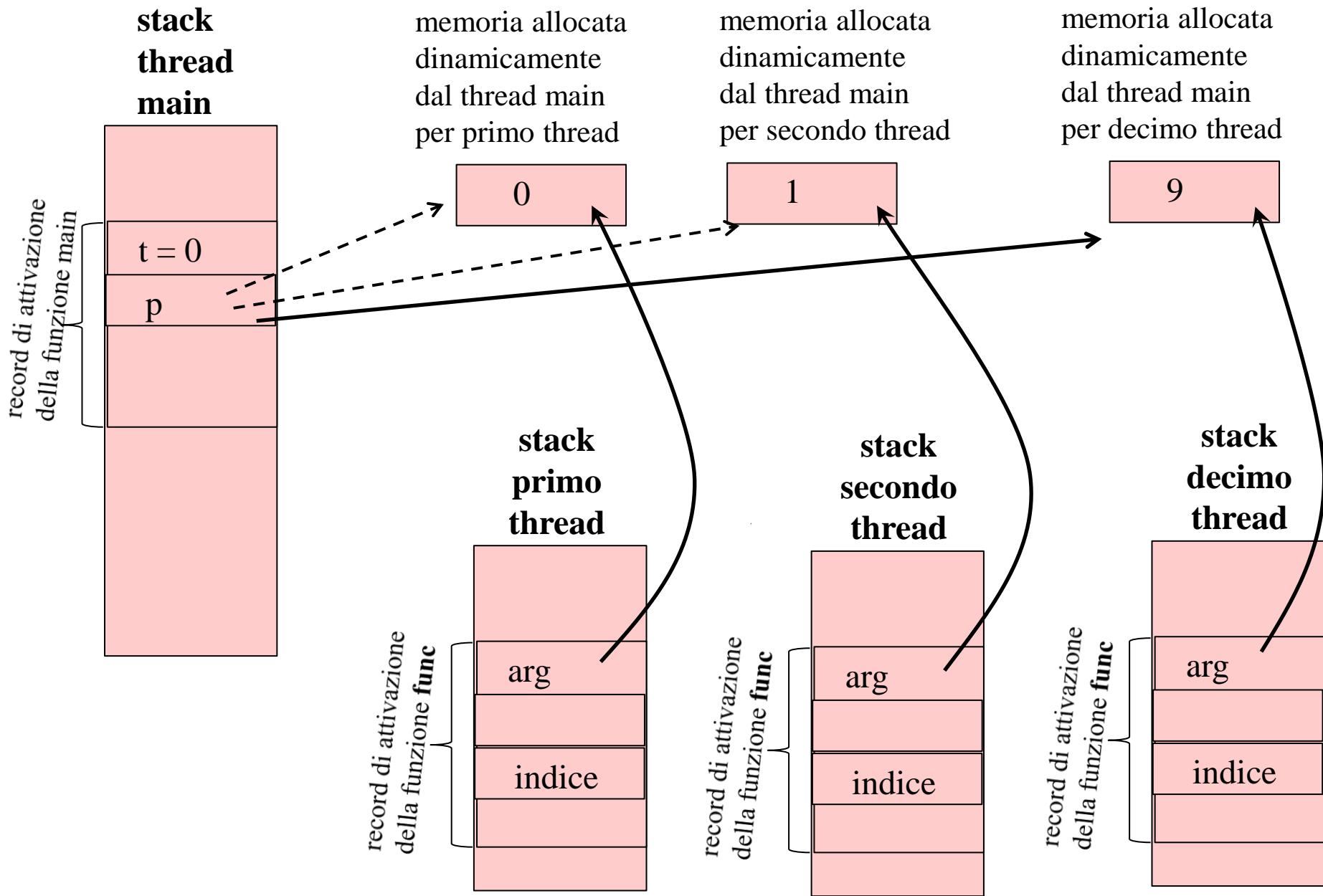
# Creazione di un Pthread

La creazione di un Pthread viene effettuata chiamando la funzione:

```
int pthread_create( pthread_t *threadId , const pthread_attr_t *attr,  
                    void *(*start_routine) (void *), void *arg );
```

- threadId è l'indirizzo di una variabile di tipo *identificatore di Pthread* in cui verrà messo l'identificatore del Pthread creato.
- attr è l'indirizzo di una variabile di tipo pthread\_attr\_t in cui posso specificare alcune caratteristiche del Pthread da creare. Il parametro attr può essere NULL per usare le impostazioni di default.
- start routine è il nome della funzione che implementa il Pthread da creare. Tale funzione formalmente deve prendere come argomento un puntatore generico void\* e deve restituire un puntatore generico void\*
- arg è un puntatore generico void\* che punta ad un'area di memoria in cui sono stati messi gli argomenti da passare alla funzione start\_routine da eseguire. Il formato di tale area di memoria è user defined, cioè è concordato tra chi implementa il Pthread e chi implementa la chiamata al Pthread. Il parametro arg può essere NULL se voglio creare un Pthread senza passargli alcun argomento.
- Il risultato restituito dalla funzione pthread\_create è un intero. Vale 0 se la funzione è riuscita a creare il Pthread. Vale !=0 se non è stato possibile creare il Pthread.
- Se diverso da 0, il valore restituito identifica il tipo di errore avvenuto.

# Schema di Passaggio di argomenti a Pthread



# Passaggio degli argomenti ad un Pthread

La funzione **pthread\_create** richiede un puntatore per il passaggio dei parametri al Pthread che sta creando. Nel momento in cui il Pthread comincerà l'esecuzione avrà a disposizione questo puntatore.

Chi chiama la pthread\_create deve allocare dinamicamente una struttura dati in cui collocare i parametri da passare al pthread. Il Pthread creato userà quest'area di memoria e poi la deallocherà.

Formalmente, la funzione che implementa il Pthread prende come argomento un puntatore generico void\* e restituisce un puntatore generico.

*Nell'esempio che segue, il main crea 10 Pthread passando a ciascuno un valore intero, ciascun pthread legge il valore intero ricevuto ricevuto e lo mette in una propria variabile indice.*

## codice del main

```
#define NUM_THREADS 10
pthread_t tid;
int t, rc;
int *p;

CORRETTO
for(t=0;t<NUM_THREADS;t++) {
    p = (int *) malloc( sizeof(int) );
    *p = t;
    rc = pthread_create( & tid , NULL, func, (void *) p );
}
```

## SBAGLIATO

```
for(t=0;t<NUM_THREADS;t++) {
    rc = pthread_create( & tid , NULL, func, (void *) & t );
}
```

## codice dei Pthread

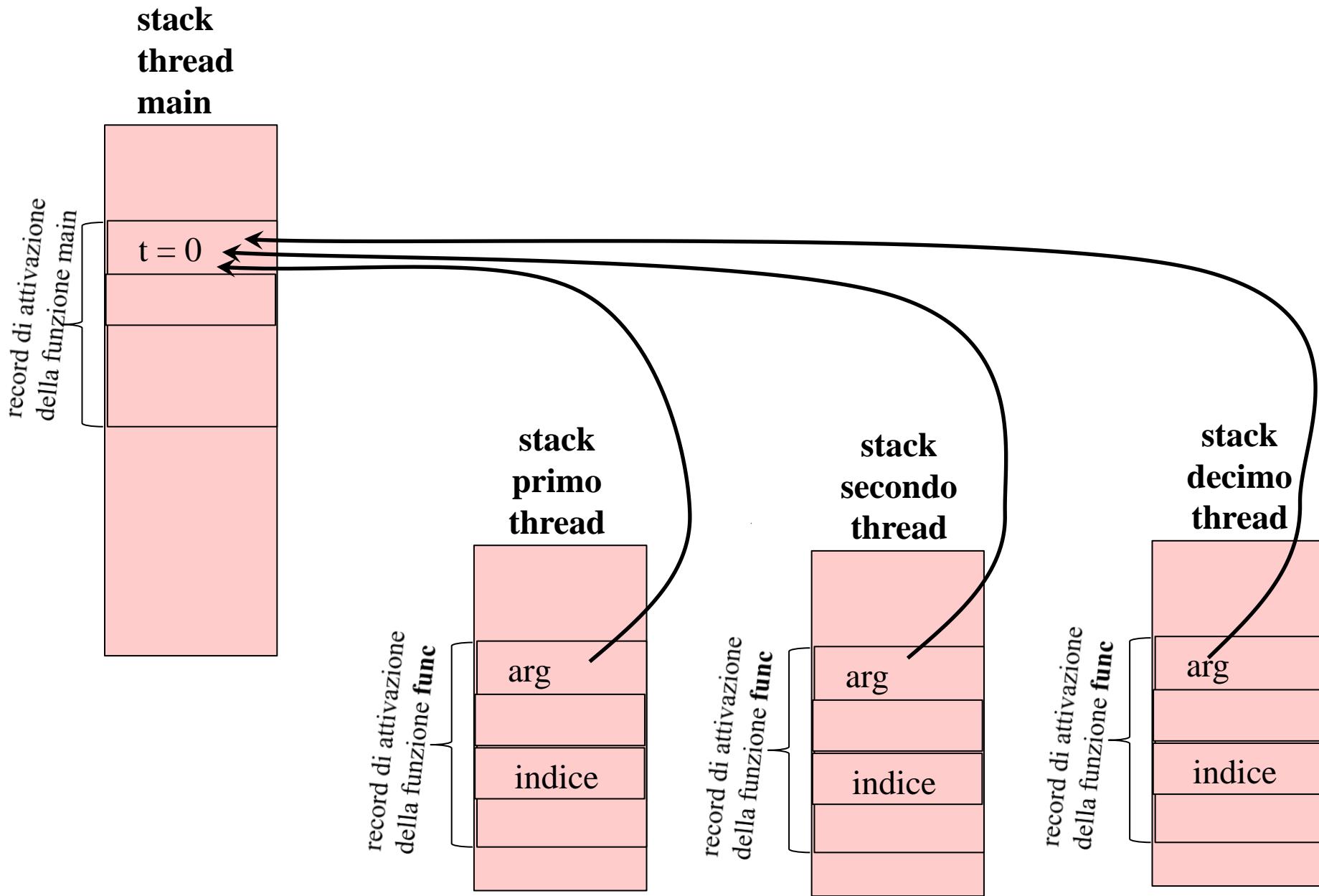
```
void * func( void *arg ) {
    int indice;
    /* uso arg come puntatore a int */
    indice = * ((int*)arg);

    /* rilascio memoria */
    free( arg ); /* non fare in caso sbagliato */

    printf(" ho ricevuto %i \n", indice );

    pthread_exit( NULL );
}
```

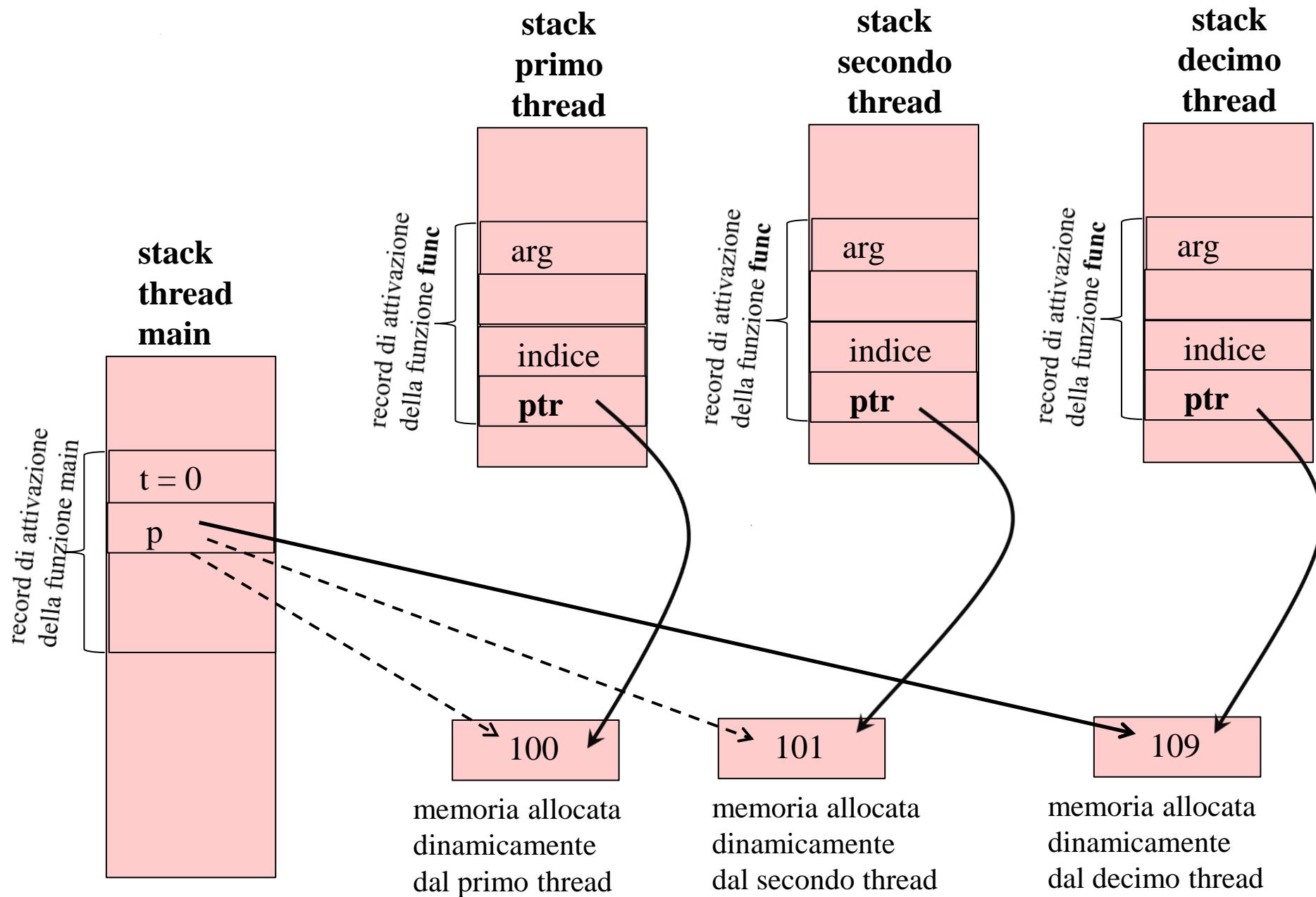
# Errore nel Passaggio di argomenti a Pthread



# Terminazione di Pthread e processo

- Il main di un processo è un Pthread come gli altri, tranne per quanto riguarda la terminazione.
- Quando un Pthread qualunque chiama l'istruzione exit() provoca la terminazione di tutto il processo con tutti i suoi Pthread.
- Quando il main (solo il main, non gli altri Pthread) chiama l'istruzione return, provoca la terminazione di tutto il processo con tutti i suoi Pthread.
- La funzione pthread\_exit() viene chiamata da un Pthread per terminare se stesso (inteso come Pthread) e restituire un risultato.
  - Se ci sono altri Pthread in esecuzione, il processo continua l'esecuzione degli altri Pthread.
  - Se invece il Pthread che ha chiamato la pthread\_exit era l'ultimo Pthread ancora in esecuzione in quel processo, allora il processo viene terminato.

# Schema di Passaggio di risultato di un Pthread



# Terminazione e Risultato di un Pthread

Quando un Pthread termina, può voler far conoscere a qualche altro Pthread il risultato del suo lavoro. Occorre un meccanismo con cui **un Pthread può restituire** un risultato (o, più in generale, **un'area di memoria** in cui potrebbe stare anche una struttura dati) a qualche altro Pthread.

La funzione **pthread\_exit** permette ad un Pthread di stabilire quale area di memoria deve essere restituita come risultato al termine del Pthread.

Formalmente, ogni Pthread deve restituire come risultato un puntatore generico **void\***. Da questo deriva che la funzione pthread\_exit prevede come argomento un puntatore generico void\* che sarà consegnato a chi vuole sapere il risultato del pthread.

```
void pthread_exit ( void* ptr );
```

Il puntatore ptr può essere NULL se il Pthread non vuole restituire un qualche risultato. Il Pthread che invece intende restituire un risultato, deve allocare dinamicamente una struttura dati in cui collocare i dati che intende restituire come risultato.

Nota Bene:

Spiegare **dove** viene inserito il puntatore da restituire, quando si parlerà dell'esempio relativo alla funzione pthread\_join.

# Dove viene mantenuto il Puntatore che funge da risultato di un Pthread

- Il risultato restituito da un Pthread mediante la chiamata a `pthread_exit()` è un puntatore ad un'area di memoria allocata dal Pthread stesso.
- **Il valore di questo puntatore viene mantenuto nello stack del Pthread anche dopo la terminazione del Pthread stesso, e fino a che un altro Pthread non richiede quel risultato mediante la chiamata alla funzione `pthread_join`.**
- **La memoria occupata dallo stack del Pthread già terminato viene rilasciata**
  - **solo dopo che un altro Pthread ha chiamato la `pthread_join` per conoscere il risultato del Pthread terminato.**
  - **oppure ovviamente quando termina il processo.**
- Se nessun Pthread chiede il risultato di un Pthread già terminato, la parte di memoria occupata dallo stack di quel Pthread terminato rimane occupata fino alla terminazione del processo.
  - Però, se un processo gira a lungo e continua a creare nuovi Pthread senza far rilasciare la memoria dello stack dei suoi Pthread che terminano, prima o poi la memoria disponibile si riempie e il processo smette di funzionare.
- E' però possibile configurare i Pthread, al momento della loro creazione, per consentire che **il loro stack possa essere liberato immediatamente dopo la loro terminazione, senza aspettare la `pthread_join`**. Questi Pthread vengono detti **detached**.
  - C'è uno svantaggio, però: i Pthread detached non possono far sapere a nessun altro Pthread il loro risultato.

# Attesa di terminazione di un Pthread

E' possibile per un Pthread attendere la terminazione di un altro Pthread dello stesso processo. Occorre conoscere l'identificatore del Pthread di cui vogliamo attendere la terminazione. La funzione **pthread\_join** vuole come argomento l'indirizzo di un puntatore generico, in cui verrà collocato l'indirizzo restituito dal Pthread il cui identificatore è passato come primo argomento.

Nello scheletro di esempio che segue, il main crea 10 Pthread, poi aspetta la terminazione dei 10 Pthread, da ciascuno riceve un puntatore ad intero e lo usa per stampare il valore intero lì contenuto. Poi rilascia la memoria allocata dal Pthread terminato

```
codice del main
#define NUM_THREADS 10
pthread_t tid [NUM_THREADS];
int t, rc; int *p;
/* creo i pthread */
for(t=0;t < NUM_THREADS;t++) {
    p = (int *) malloc( sizeof(int) );           *p = t;
    rc = pthread_create( & tid[t] , NULL, func, (void*) p );
}
/* attendo terminazione dei pthread */
for(t=0;t < NUM_THREADS;t++) {
    int ris;

    rc = pthread_join( tid[t] , (void**) & p );
    ris = *p ;
    printf( " pthread restituisce %i \n", ris );
    free (p);
}
```

```
codice del pthread
void * func( void *arg ) {
    int *ptr;
    int indice = *((int*) arg); free(arg);
    /* qui il pthread fa qualcosa ... */

    ptr = (int *) malloc( sizeof(int));
    /* pthread vuole passare un valore
       intero, ad es 100+indice */

    *ptr = 100+indice;
    pthread_exit( (void*) ptr );
}
```

# Preliminare informaticamente osceno (1): usare un intero con dimensioni di un puntatore

Può capitare di volere usare un puntatore (chiamiamolo p) per conservare un valore intero, e non un indirizzo. Voglio cioè mettere un valore intero dentro un puntatore. Ovviamente devo ricordarmi di non usare quel puntatore come puntatore, cioè non devo fare accessi tipo `*p` `p->`

Questa operazione può essere fatta senza perdita di informazioni solo se l'intero ha le stesse dimensioni di un puntatore.

Purtroppo, le dimensioni dei puntatori variano al variare del processore, poiché varia la dimensione del BUS degli indirizzi, che determina la dimensione dei puntatori.

POSIX definisce un tipo di dato intero che ha le stesse dimensioni di un puntatore.

Tale definizione è contenuta nel file **stdint.h**

I due tipi di interi disponibili, rispettivamente interi con segno e senza segno, sono  
**intptr\_t**      e      **uintptr\_t**

**Diventa possibile fare le seguenti operazioni senza warning :**

```
void *p;                intptr_t t;  
p = (void*) t;  
t = (intptr_t) p;
```

# Preliminare informaticamente osceno (2) : stampare un intero con dimensioni di un puntatore

- A questo punto si pone il problema di come stampare tali valori con una printf, poiché usare gli specicatori di formato per gli int o i long int %i o %u provoca problemi.
- Sono a tal scopo definite delle macro che inseriscono l'adatto specifikatore di formato nelle printf e nelle scanf a seconda che vogliamo stampare l'intero come signed unsigned esadecimale etc.
- Le macro sono contenute nel file inttypes.h

Gli specicatori di formato per i tipi intptr, corrispondenti sono:

ottale

specifikatore per tipo intero

sia in printf che in scanf

%d

%i

%o

%u

%x

%X

specifikatore per tipo intptr in printf

PRIIdPTR

PRIiPTR

PRIoPTR

PRIuPTR

PRIxPTR

PRIXPTR

specifikatore per tipo intptr in scanf

SCNdPTR

SCNiPTR

SCNoPTR

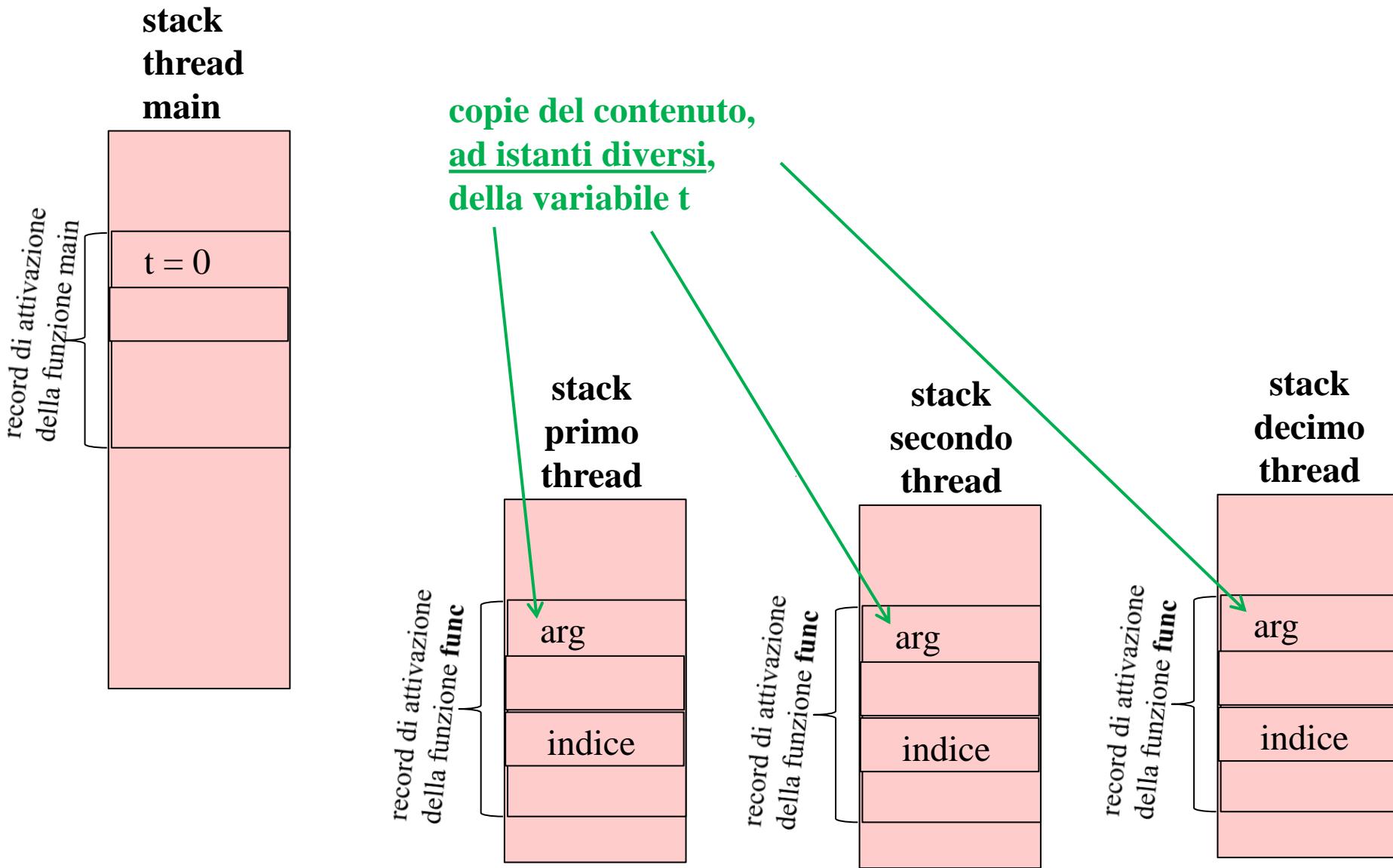
SCNuPTR

SCNxPTR

SCNXPTR

```
#include <stdio.h>
#include <stdint.h>
#include <inttypes.h>
intptr_t t = 13;    void *p=NULL;
p = (void*) t;
t = (intptr_t) p;
printf ( " stampo t che vale %" PRIiPTR " \n", t );
```

# Trucco osceno (informaticamente parlando) per passare un intero a un Pthread



# Trucco osceno per passare un intero a un Pthread

Se, quando creo un Pthread, devo passare SOLAMENTE un intero al Pthread, allora posso sfruttare un trucco osceno per evitare di allocare e deallocaare memoria.

Quando creo il Pthread mediante la funzione `pthread_create`, utilizzo **come se fosse un intero**, il puntatore arg da passare come ultimo argomento alla funzione `pthread_create`.

Metto in quel puntatore non un indirizzo bensì il valore intero da passare al Pthread.

Occorre che l'intero che voglio passare abbia esattamente le stesse dimensioni di un puntatore.

Per tale motivo utilizzo un particolare tipo di intero definito in POSIX, le cui dimensioni sono esattamente le dimensioni di un puntatore: ovviamente, tali dimensioni cambiano a seconda del processore e del s.o. Tale tipo è **intptr\_t** o **uintptr\_t** ed è definito in **stdint.h**

Le macro per stampare con `printf` tali tipi di dato sono in **inttypes.h**

## codice del main

```
#define NUM_THREADS 10
pthread_t tid;
int rc;
intptr_t t;

for(t=0;t < NUM_THREADS; t++) {
    rc = pthread_create( & tid , NULL,
                        func, (void *) t );
}
```

notare che qui **NON** c'è l' &  
cioè non passo l'indirizzo di t  
bensì proprio il contenuto di t

## codice dei Pthread

```
void * func( void *arg ) {
    intptr_t indice;

    indice = (( intptr_t ) arg );

    /* NON DEVO rilasciare memoria
     NOOO!!!!!! free( arg );
     */

    printf(" ho ricevuto %" PRIiPTR " \n",
          indice );

    pthread_exit( NULL );
}
```

# Mutua Esclusione e Sincronizzazione

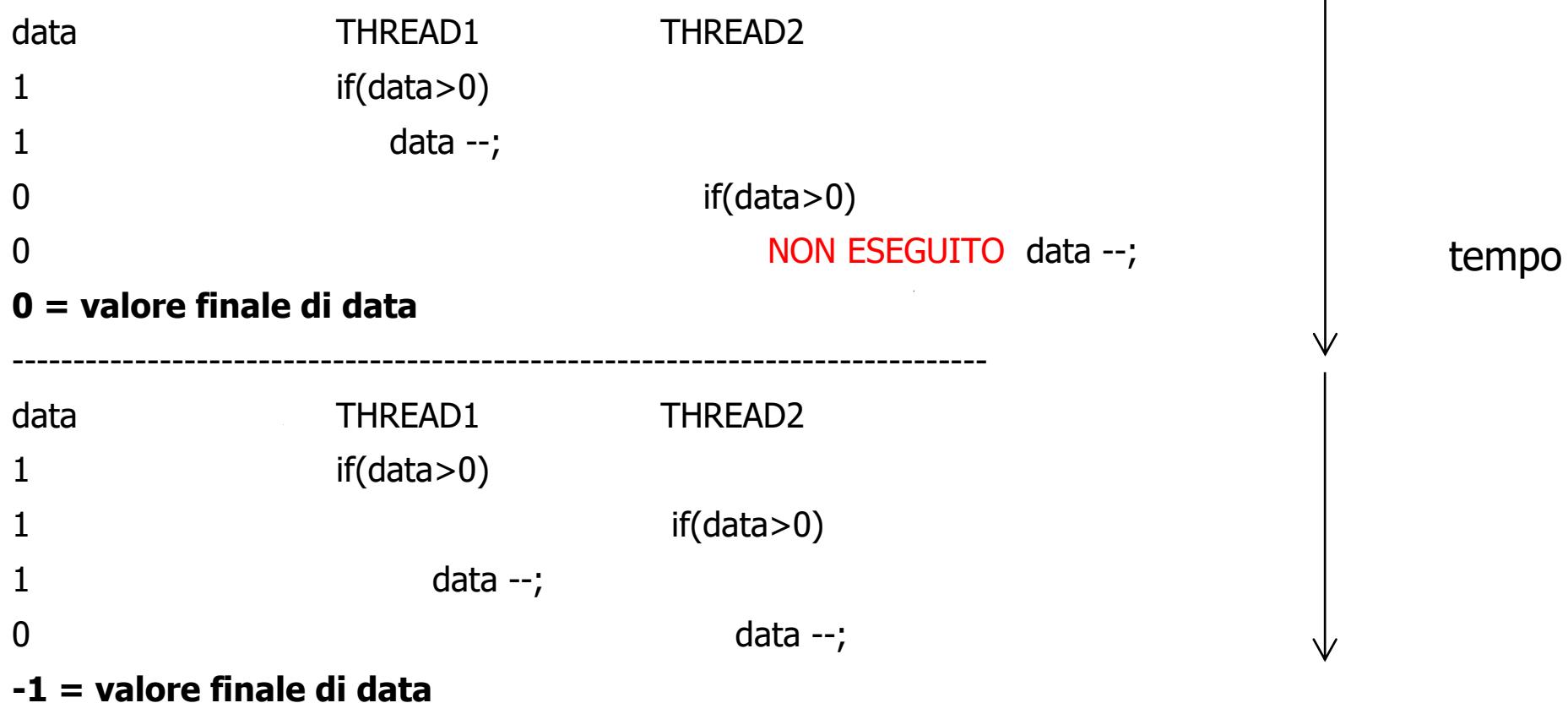
# Perché Garantire la Mutua Esclusione - race condition

Esempio: Due thread devono decrementare il valore di una variabile globale data, ma solo se questa è maggiore di zero. Inizialmente data vale 1.

THREAD1  
if(data>0)  
    data --;

THREAD2  
if(data>0)  
    data --;

A seconda del tempo di esecuzione dei due thread, la variabile data assume valori diversi (race condition).



# Mutex Variables

- **Mutex** è l'abbreviazione di “**mutua esclusione**”.
- Una variabile mutex (formalmente di tipo **pthread\_mutex\_t**) serve per regolare l'accesso a dei dati che debbono essere protetti dall'accesso contemporaneo da parte di più thread.
- Noi usiamo le cosiddette FAST mutex. Ne esistono altri tipi più evoluti che vengono determinati in fase di inizializzazione, **ma noi NON le usiamo e non le potrete usare all'esame**.
- Ogni thread, prima di accedere a tali dati, deve effettuare una operazione di **pthread\_mutex\_lock** su una stessa variabile mutex. L'operazione detta “lock” di una variabile mutex blocca l'accesso da parte di altri thread.
- Infatti, se più thread eseguono l'operazione di lock **su una stessa variabile mutex**, solo uno dei thread termina la lock() e prosegue l'esecuzione, gli altri rimangono bloccati nella lock. In tal modo, il processo che continua l'esecuzione può accedere ai dati (protetti mediante la mutex).
- Finito l'accesso, il thread effettua un'operazione detta **pthread\_mutex\_unlock** che libera la variabile mutex. Un'altro thread che ha precedentemente eseguito la lock della mutex potrà allora terminare la lock ed accedere a sua volta ai dati.
- La tipica sequenza d'uso di una mutex è quindi:
  - creare ed inizializzare la mutex
  - più thread cercano di accedere alla mutex chiamando ciascuno la **pthread\_mutex\_lock**
  - un solo thread termina la lock e diviene proprietario della mutex, gli altri sono bloccati.
  - il thread proprietario accede ai dati, o esegue funzioni.
  - il thread proprietario libera la mutex eseguendo la **pthread\_mutex\_unlock**
  - un'altro thread termina la lock e diventa proprietario di mutex
  - .... e così via
  - al termine del programma, o quando non serve più, la mutex viene distrutta.

# Operazioni con Mutex (1)

## Creare e Distruggere variabili Mutex (per FAST Mutex)

- Le variabili Mutex devono essere create usando il tipo di dato `pthread_mutex_t` e devono essere inizializzate prima di poter essere usate.

- **Inizializzazione statica**, all'atto della dichiarazione;

```
pthread_mutex_t mymutex = PTHREAD_MUTEX_INITIALIZER;
```

- **Inizializzazione dinamica**, mediante invocazione di funzione, in un momento successivo alla dichiarazione, nel caso si voglia specificare proprietà aggiuntive; Se il puntatore agli attributi è `NULL` si utilizzano gli attributi di default.

```
pthread_mutex_t mymutex;
```

```
pthread_mutex_init( &mymutex , &attribute);
```

attribute può essere `NULL`

- Finito l'uso delle variabili mutex, bisognerebbe rilasciarle.

```
pthread_mutex_destroy (&mymutex);
```

# Operazioni con Mutex (2)

## Attesa per Mutua Esclusione (per Fast Mutex)

- **int pthread\_mutex\_lock (pthread\_mutex\_t \*mutex);** blocca la variabile mutex passata come argomento.
  - Se la variabile mutex è attualmente sbloccata, diventa bloccata e di proprietà del thread chiamante e immediatamente la funzione pthread\_mutex\_lock termina e restituisce il controllo al chiamante, con risultato 0. In caso di problemi viene restituito un risultato diverso da zero che identifica il tipo di errore.
  - Se invece la variabile mutex è già bloccata da un altro thread, allora la funzione pthread\_mutex\_lock sospende il thread chiamante finché la mutex non viene sbloccata.
  - **Attenzione**, se la mutex è già bloccata dal thread chiamante (perché lo stesso pthread ha già fatto una lock senza fare una successiva unlock) allora, chiamando ancora la pthread\_mutex\_lock il thread va in stallo e si blocca per sempre. In altri tipi di mutex NON FAST, invece, il comportamento è differente.
- **int pthread\_mutex\_unlock (pthread\_mutex\_t \*mutex);** sblocca la variabile mutex.
  - La funzione DEVE ESSERE CHIAMATA su una variabile mutex che sia già bloccata e di proprietà del thread chiamante. In tal caso la funzione pthread\_mutex\_unlock sblocca la variabile mutex e termina restituendo 0. In caso di problemi viene restituito un risultato diverso da zero che identifica il tipo di errore.
  - Attenzione: Se la funzione pthread\_mutex\_unlock viene chiamata da un thread che NON È PROPRIETARIO della variabile mutex (cioè non ha fatto una precedente lock su quella variabile) allora si genera un comportamento impredicibile, poiché la mutex viene sbloccata anche se è di proprietà di un thread diverso. Questo è un comportamento su cui non si deve fare affidamento.
  - Nelle mutex di tipo NON FAST, invece, vengono effettuati controlli aggiuntivi ed il comportamento è diverso.

# Operazioni con Mutex (3)

## Attesa per Mutua Esclusione (per Fast Mutex)

### Evitare il blocco

```
int pthread_mutex_trylock (pthread_mutex_t *mutex);
```

- questa funzione è come la lock(), ma **se** si accorge che la mutex è già in possesso di altro thread ( e quindi si rimarrebbe bloccati ) restituisce immediatamente il controllo al chiamante con risultato EBUSY
- Se, invece, si ottiene la proprietà della mutex, restituisce 0.
  
- **Attenzione**, questa funzione porta a creare codice che causa busy waiting.

# Esempio di protezione con Mutex Variable

```
#define NUM_THREADS 10
pthread_t tid [NUM_THREADS ];
pthread_mutex_t mutexdata;
int data=4;

int main (void) {
int rc , t;
int *p;

pthread_mutex_init (&mutexdata, NULL);

/* creo i pthread */
for(t=0;t < NUM_THREADS;t++) {
    rc = pthread_create( & tid[t] , NULL, func, NULL ) ;
}

/* attendo terminazione dei pthread */
for(t=0;t < NUM_THREADS;t++) {

    rc = pthread_join( tid[t] , (void**) & p ) ;
}
printf ("data = %d \n", data);

pthread_mutex_destroy (&mutexdata);

pthread_exit(NULL);
}
```

codice del pthread

```
void * func( void *arg ) {

    pthread_mutex_lock (&mutexdata);

    if(data>0)
        data--;

    pthread_mutex_unlock (&mutexdata);

    pthread_exit( NULL );
}
```

# Condition Variables

- Le Mutex consentono di effettuare sincronizzazioni tra pthreads nel momento in cui ciascun pthread tenta l'accesso in mutua esclusione. L'accesso viene consentito senza poter valutare a priori il valore delle variabili condivise.
- Al contrario, le condition variables sono delle variabili che consentono di effettuare delle sincronizzazioni tra pthreads mentre questi già detengono la mutua esclusione, bloccandoli o facendoli continuare in base a condizioni definite dal programmatore e dipendenti dal valore attuale delle variabili condivise.
- Senza le condition variables, il programmatore dovrebbe scrivere dei pthread che effettuano un loop continuo in cui prima viene presa la mutua esclusione, poi viene controllato il valore delle variabili condivise. Se il valore corrisponde alle condizioni richieste allora il pthread esegue le operazioni richieste e poi rilascia la mutua esclusione. Se invece il valore NON corrisponde alle condizioni richieste allora il pthread rilascia immediatamente la mutua esclusione e poi la riprende e ricontrolla i valori delle variabili condivise e così via all'infinito, **effettuando busy waiting e sprecando così tempo di CPU**.
- Le condition variables devono sempre essere utilizzate assieme ad una mutex per consentire di accedere in mutua esclusione alle variabili condivise.
- Ci sono tre principali funzioni per sincronizzare con le condition variables:
  - **pthread\_cond\_wait:** blocca un thread fino a che un altro thread lo risveglia e può prendere la mutua esclusione.
  - **pthread\_cond\_signal:** sveglia un altro thread bloccato sulla pthread\_cond\_wait, ma l'altro thread prima di ripartire deve ottenere la mutua esclusione.
  - **pthread\_cond\_broadcast:** sveglia tutti i threads bloccati sulla pthread\_cond\_wait, ma ciascuno di questi, prima di ripartire uno alla volta, deve ottenere la mutua esclusione.

## ESEMPIO di SINCRONIZZAZIONE

Volpe mangia uova deposte da gallina. La volpe aspetta che la gallina abbia deposto un uovo per poi mangiarselo, poi aspetta di nuovo e così via all'infinito.

- Una prima implementazione (Orrenda) senza Condition variables, provoca busy waiting.
- Una seconda implementazione corretta con Condition variables, efficiente.
  - Stessa soluzione può essere usata avendo contemporaneamente più volpi e più galline, se si considera che solo una gallina alla volta può deporre l'uovo e che solo una volpe per volta può mangiare un uovo.

# Volpe mangia uova

## SENZA CONDITION VARIABLES - BUSY WAITING ☹ ☹ ☹

```
int uova = 0;
pthread_mutex_t mutex = PTHREAD_MUTEX_INITIALIZER;

void *gallina_produce_uova(void *)
{   while(1) {
        sleep(3); /* gallina produce uova impiegando tempo ....*/
        pthread_mutex_lock(&mutex);
        uova++;
                           /* gallina depone uovo */
        pthread_mutex_unlock(&mutex);
    }
}

void *volpe_mangia_uova(void *)
{   while(1) {
        pthread_mutex_lock(&mutex);
        if( uova > 0 ) {
            mangia(); /* volpe mangia uovo impiegando poco tempo ....*/
            uova--;
            pthread_mutex_unlock(&mutex);
            burp(); /* volpe digerisce impiegando tempo */
        } else {
            ; /* do nothing, ma la valutazione di condizione if l'hai fatta
               e la fai in continuazione usando CPU .... */
            pthread_mutex_unlock(&mutex);
        }
    }
}

int main(void)
{   pthread_t tid;
    pthread_create( &tid, NULL, gallina_produce_uova, NULL )
    pthread_create( &tid, NULL, volpe_mangia_uova, NULL )
    pthread_exit(NULL);
}
```

# CON CONDITION VARIABLES - NO BUSY WAITING



```
int uova = 0;
pthread_mutex_t mutex = PTHREAD_MUTEX_INITIALIZER;
pthread_cond_t cond = PTHREAD_COND_INITIALIZER;

void *gallina_produce_uova(void *arg)
{   while(1) /* gallina produce uova impiegando tempo ....*/
    /* poi gallina depone uovo e fa coccodè' */
    pthread_mutex_lock(&mutex);
    uova++;
    pthread_cond_signal(&cond); /* coccodè' avvisa volpe che c'è uovo */
    pthread_mutex_unlock(&mutex);
}

void *volpe_mangia_uova(void *arg)
{   while(1) {
        pthread_mutex_lock(&mutex);
        while( uova==0 ) { /* attendi che venga prodotto uovo, attendi signal */
            pthread_cond_wait(&cond, &mutex);
        }
        /* quando arrivo qui c'è almeno un uovo */
        mangia();           /* volpe mangia uovo impiegando tempo ....*/
        uova--;
        pthread_mutex_unlock(&mutex);

        burp(); /* volpe digerisce impiegando tempo */
    }
}

int main(void)
{   pthread_t tid;
    pthread_create( &tid, NULL, gallina_produce_uova, NULL )
    pthread_create( &tid, NULL, volpe_mangia_uova, NULL )
    pthread_exit(NULL);
}
```

# Più attori, stesso codice, NO BUSY WAITING ☺

```
int uova = 0;
pthread_mutex_t mutex = PTHREAD_MUTEX_INITIALIZER;
pthread_cond_t cond = PTHREAD_COND_INITIALIZER;

void *gallina_produce_uova(void *arg)
{   while(1) /* gallina produce uova impiegando tempo ....*/
    /* poi gallina depone uovo e fa coccodè' */
    pthread_mutex_lock(&mutex);
    uova++;
    pthread_cond_signal(&cond); /* coccodè' avvisa volpe che c'è uovo */
    pthread_mutex_unlock(&mutex);
}

void *volpe_mangia_uova(void *arg)
{   while(1) {
    pthread_mutex_lock(&mutex);
    while( uova==0 ) { /* attendi che venga prodotto uovo, attendi signal */
        pthread_cond_wait(&cond, &mutex);
    }
    /* quando arrivo qui c'è almeno un uovo */
    mangia();           /* volpe mangia uovo impiegando tempo ....*/
    uova--;
    pthread_mutex_unlock(&mutex);

    burp(); /* volpe digerisce impiegando tempo */
}

int main(void)
{   pthread_t tid; int i;
    for (i=0,i<10;i++) pthread_create( &tid, NULL, gallina_produce_uova, NULL )
    for (i=0,i<30;i++) pthread_create( &tid, NULL, volpe_mangia_uova, NULL )
    pthread_exit(NULL);
}
```

# Operazioni con Condition Variables (1)

## Creare e distruggere Condition Variables

- Le Condition variables devono essere create usando il tipo di dato pthread\_cond\_t e devono essere inizializzate prima di poter essere usate.

- **Inizializzazione statica**, all'atto della dichiarazione;

```
pthread_cond_t mycond = PTHREAD_COND_INITIALIZER;
```

- **Inizializzazione dinamica**, mediante invocazione di funzione, quando si vuole specificare proprietà aggiuntive;

```
pthread_cond_t mycond;
```

```
pthread_cond_init( & mycond , &attribute);
```

- Finito l'uso delle condition variable, bisognerebbe rilasciarle.

```
pthread_cond_destroy(&mycond);
```

# Operazioni con Condition Variables (2)

## Attesa

- **`pthread_cond_wait ( pthread_cond_t *cond, pthread_mutex_t *mutex)`** è eseguita da un pthread quando questo vuole bloccarsi ed aspettare che una condizione sia vera.
- Prima di chiamare la wait il pthread deve prendere la mutua esclusione sulla mutex specificata nel secondo parametro della wait.
- Quando la wait blocca il pthread, automaticamente la wait rilascia la mutua esclusione e poi si mette in attesa di essere abilitata al risveglio da una `pthread_cond_signal()` chiamata da qualche altro pthread.
- La wait continua e termina solo dopo che si verificano due condizioni
  - 1) un altro pthread l'ha risvegliata con una chiamata a `pthread_cond_signal()` e che
  - 2) la wait ha potuto riprendere la mutua esclusione.
- Quando la wait termina, il pthread si trova a detenere la mutua esclusione sulla variabile mutex specificata nel secondo parametro della wait.

# Operazioni con Condition Variables (3)

## Abilitazione al risveglio

- **`pthread_cond_signal( pthread_cond_t *cond )`** controlla se c'è qualche thread in attesa con una wait sulla condition variable specificata nel parametro passato alla signal. Se c'è lo avvisa e lo abilita a risvegliarsi, ma per potersi risvegliare quel thread deve attendere di poter prendere la mutua esclusione.
- Dopo aver abilitato il thread a proseguire, la funzione signal termina.
- Se non c'è un thread in attesa da abilitare, la funzione semplicemente termina.
- Non è specificato qual' è l'ordine con cui le signal abilitano i thread in attesa su una wait. Non è affatto detto che l'ordine di risveglio sia lo stesso ordine in cui i threads sono entrati in wait.
- **IMPORTANTE:** Le chiamate alle `pthread_cond_signal()` e `pthread_cond_broadcast()` devono essere effettuate da un thread che detiene la mutua esclusione sulla mutex specificata nelle wait per quella condition variable. In tal modo si protegge l'accesso alla condition variable che è essa stessa una variabile condivisa.
- In pratica, prima di chiamare la `pthread_cond_signal()` o la `pthread_cond_broadcast()` occorre prima avere chiamato la `pthread_mutex_lock()`.
- Per abilitare tutti i thread in attesa su una wait per una data condition variable, posso fare una iterazione di chiamate alla signal, oppure posso chiamare la funzione `pthread_cond_broadcast( pthread_cond_t *cond )`.

# Riassumendo: Operazioni con Condition Variables

## □ Waiting and signaling on condition variables

## □ Routines

### □ `pthread_cond_wait(condition, mutex)`

- ▶ Blocks the thread until the specific condition is signalled.
- ▶ Should be called with mutex locked
- ▶ Automatically release the mutex lock while it waits
- ▶ When return (condition is signaled), mutex is locked again

### □ `pthread_cond_signal(condition)`

- ▶ Wake up a thread waiting on the condition variable.
- ▶ Called after mutex is locked, and must unlock mutex after

### □ `pthread_cond_broadcast(condition)`

- ▶ Used when multiple threads blocked in the condition

# *Concetti Generali sulla Gestione della memoria*

*Binding Address, Allocazione, Segmentazione, Paginazione  
Memoria Virtuale (swap)*

*Dispense estratte (e parzialmente modificate) dal documento:*

*Sistemi Operativi*

*Modulo 6: Gestione della memoria*

*A.A. 2009-2010*

**Renzo Davoli**

**Alberto Montresor**

Copyright © 2002-2005 Renzo Davoli, Alberto Montresor

Permission is granted to copy, distribute and/or modify this document under the terms of the GNU Free Documentation License, Version 1.2 or any later version published by the Free Software Foundation; with no Invariant Sections, no Front-Cover Texts, and no Back-Cover Texts. A copy of the license can be found at:  
<http://www.gnu.org/licenses/fdl.html#TOC1>

*Un sentito ringraziamento ai colleghi per aver concesso l'uso della loro opera.*

*Gli eventuali errori sono stati introdotti da me.*

# Sommario

- **Compiti del gestore della memoria del sistema operativo**
  - tenere traccia della memoria libera e occupata
  - allocare memoria ai processi e deallokarla quando non più necessaria
  - Il gestore può avere necessità di appoggiarsi alla memoria secondaria (disco), al fine di emulare memoria principale
- 
- 
- **Binding, loading, linking**
- **Allocazione contigua**
- **Paginazione**
- **Segmentazione**
- **Memoria virtuale**

# Introduzione

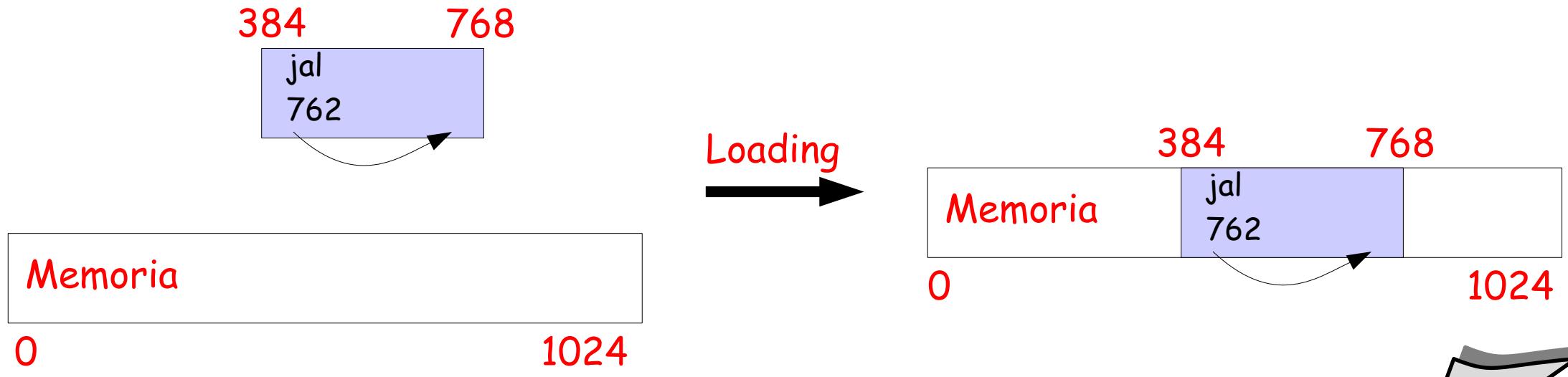
- **Prospettiva storica**
  - partiremo vedendo i meccanismi di gestione della memoria più semplici;
  - a volte possono sempre banali, ma...
- **... ma nell'informatica, la storia ripete se stessa:**
  - alcuni di questi meccanismi vengono ancora utilizzati in sistemi operativi speciali per palmari, sistemi embedded (microcontrollori), smart-card

# Binding Address

- **Definizione**
  - con il termine *binding address* o (*rilocazione*) si indica l'associazione di indirizzi di memoria fisica ai dati e alle istruzioni di un programma
- **Il binding può avvenire**
  - durante la compilazione
  - durante il caricamento del programma in memoria per l'esecuzione
  - durante l'esecuzione.

# Binding Address

- **Binding durante la compilazione del programma**
  - gli indirizzi vengono calcolati al momento della compilazione e resteranno gli stessi ad ogni esecuzione del programma
  - il codice generato viene detto codice *assoluto*
  - Esempi:
    - codice per microcontrollori, per il kernel, file COM in MS-DOS



# Binding Address

- **Binding durante la compilazione**
  - vantaggi
    - non richiede hardware speciale
    - semplice
    - molto veloce
  - svantaggi
    - non funziona con la multiprogrammazione

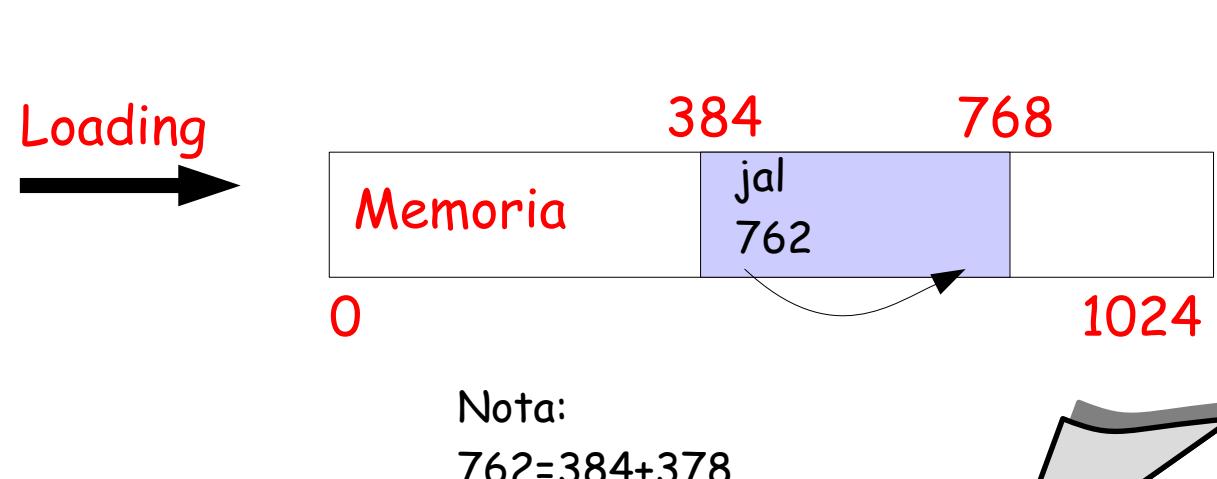
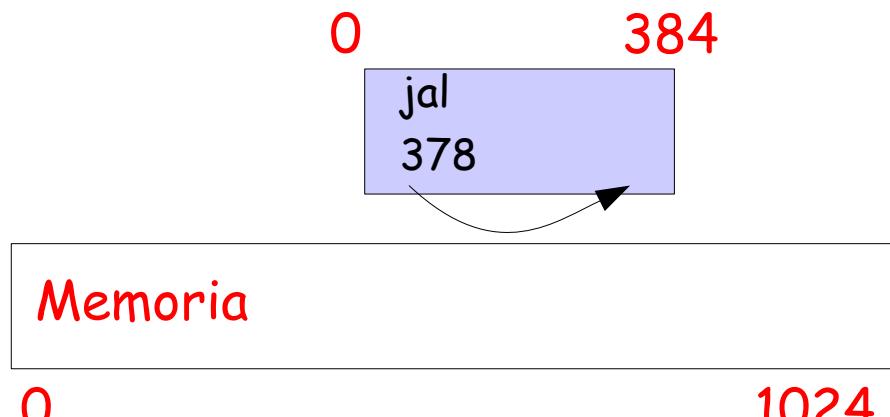
# Binding Address

- **Binding durante il caricamento**

- il codice generato dal compilatore non contiene indirizzi assoluti ma relativi (rispetto all' Instruction Pointer **oppure** rispetto ad un indirizzo base, **l'inizio del segmento**)
- questo tipo di codice viene detto *rilocabile*

- **Durante il caricamento**

- il loader si preoccupa di **aggiornare tutti i riferimenti agli indirizzi di memoria** coerentemente al punto iniziale di caricamento



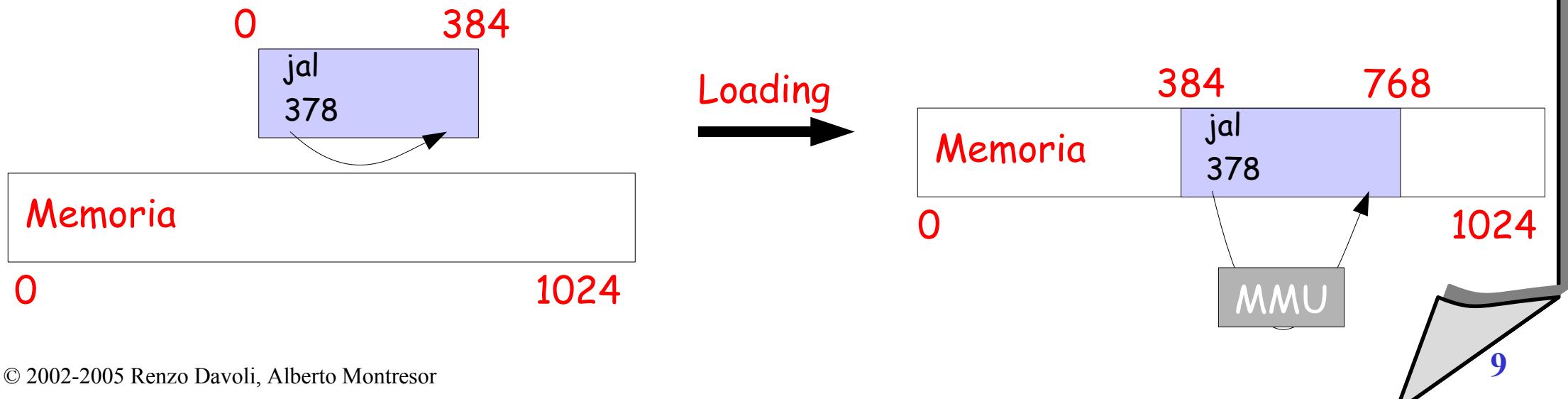
# Binding Address

- **Binding durante il caricamento**
  - vantaggi
    - permette di gestire multiprogrammazione
    - non richiede uso di hardware particolare
  - svantaggi
    - richiede una traduzione degli indirizzi da parte del loader, e quindi formati particolare dei file eseguibili

# Binding Address

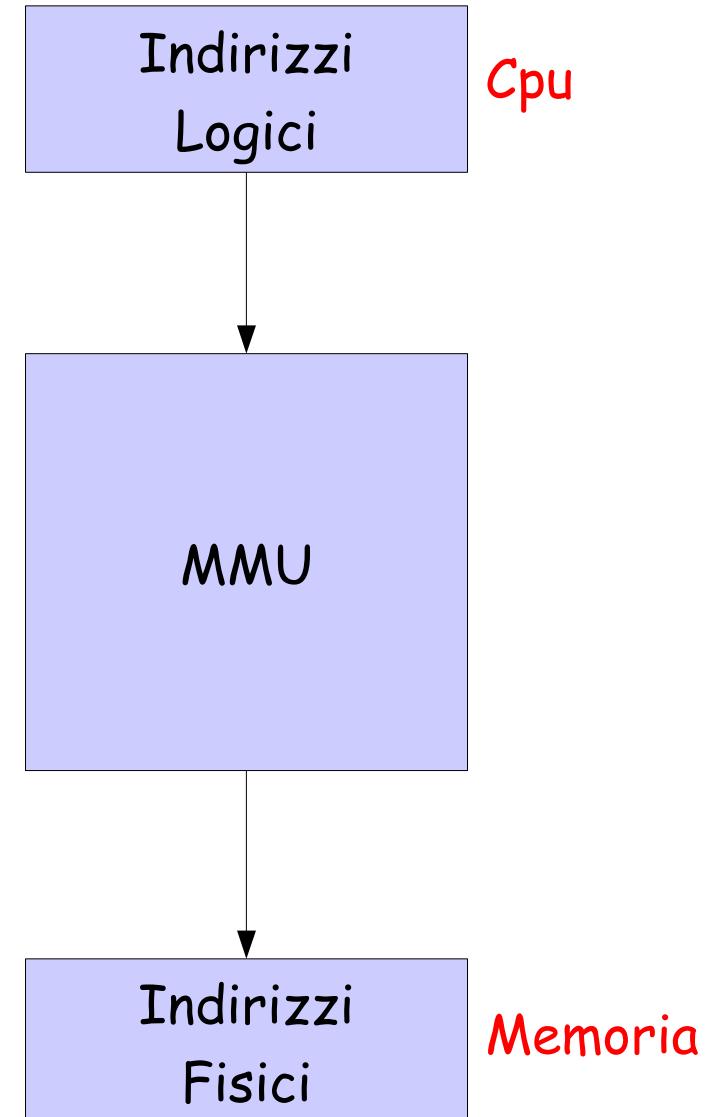
- **Binding durante l'esecuzione**

- l'individuazione dell'indirizzo di memoria effettivo viene effettuata durante l'esecuzione da un componente hardware apposito:  
la *memory management unit* (MMU)



# Indirizzi logici e indirizzi fisici

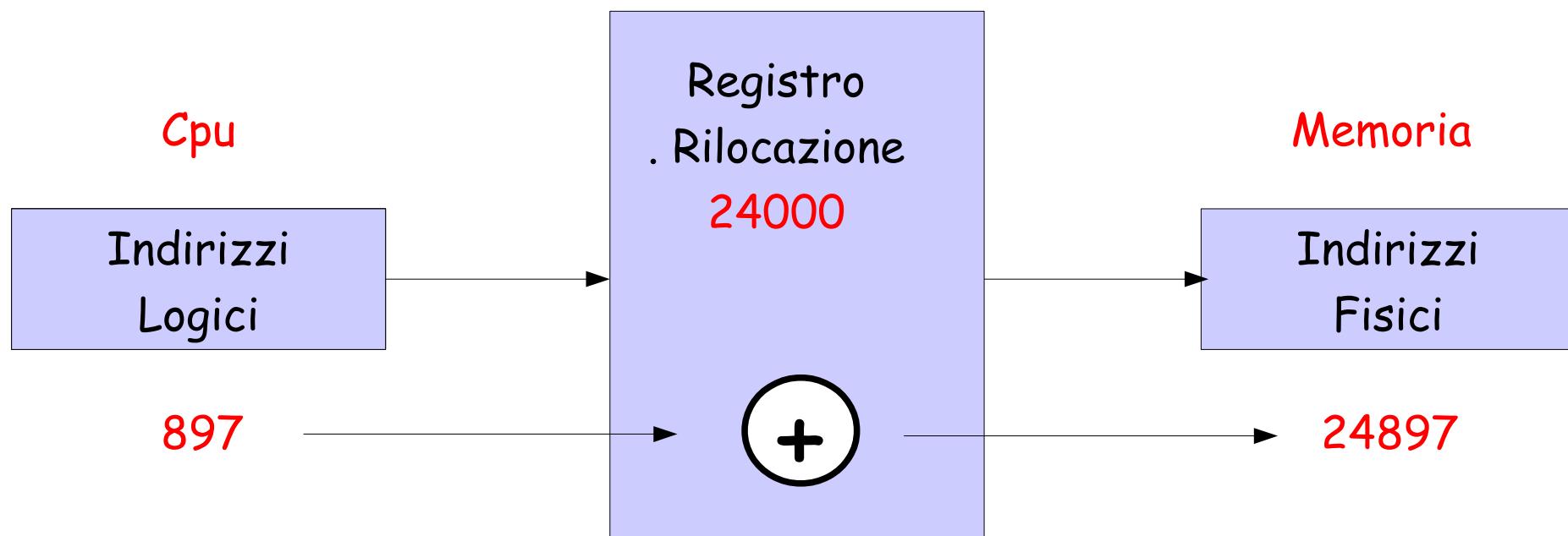
- **Spazio di indirizzamento logico**
  - ogni processo è associato ad uno spazio di indirizzamento logico
  - gli indirizzi usati in un processo sono indirizzi logici, ovvero riferimenti a questo spazio di indirizzamento
- **Spazio di indirizzamento fisico**
  - ad ogni indirizzo logico corrisponde un indirizzo fisico
  - la MMU opera come una funzione di traduzione da indirizzi logici a indirizzi fisici



# Esempi di MMU - Registro di rilocazione

- **Descrizione**

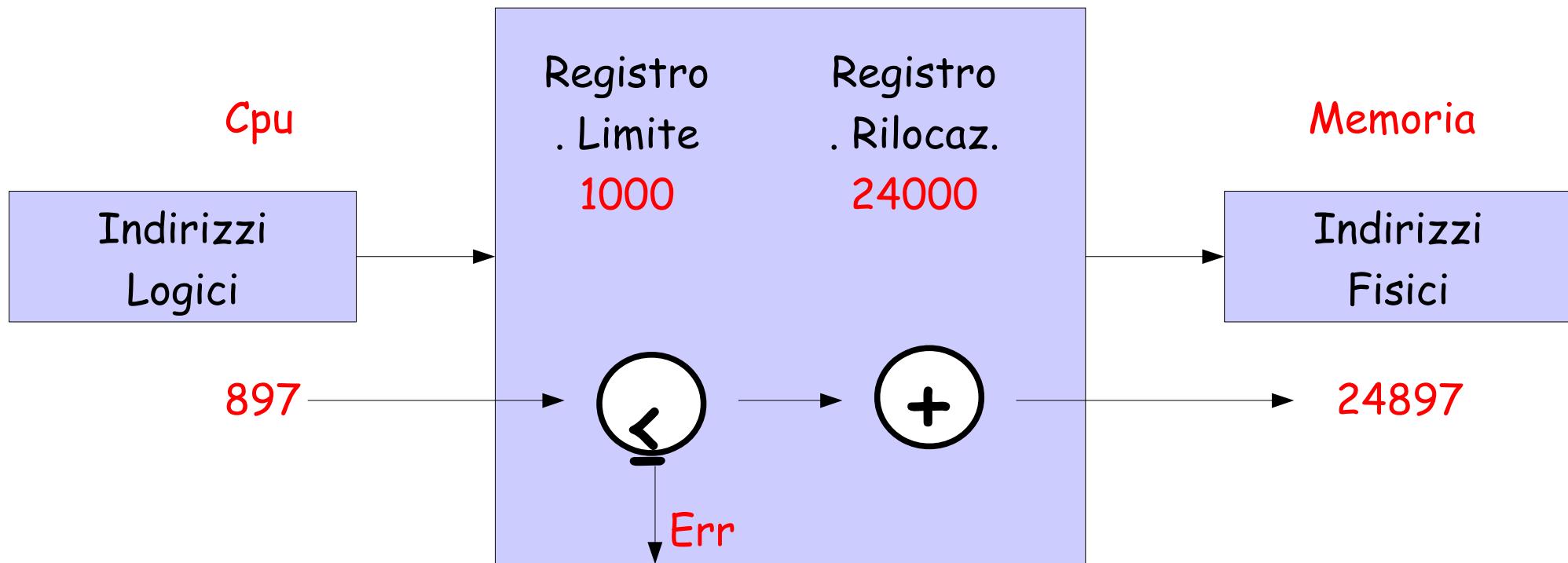
- se il valore del registro di rilocazione è R, uno spazio logico 0...Max viene tradotto in uno spazio fisico R...R+MAX
- esempio: nei processori Intel 80x86, esistono 4 registri base per il calcolo degli indirizzi (CS, DS, SS, ES)



# Esempi di MMU- Registro di rilocazione e limite

- **Descrizione**

- il registro limite viene utilizzato per implementare meccanismi di protezione della memoria



# Allocazione di memoria

- E' una delle funzioni principali del gestore di memoria
- Consiste nel reperire ed assegnare uno spazio di memoria fisica
  - a un programma che viene attivato
  - oppure per soddisfare ulteriori richieste effettuate dai programmi durante la loro esecuzione

# Allocazione: definizioni

- **Allocazione contigua**
  - tutto lo spazio assegnato ad un programma deve essere formato da celle consecutive
- **Allocazione non contigua**
  - è possibile assegnare a un programma aree di memorie separate
- **Nota**
  - la MMU deve essere in grado di gestire la conversione degli indirizzi in modo coerente alla allocazione
  - esempio: la MMU basata su rilocazione gestisce solo allocazione contigua (per uno stesso segmento, ma possono esistere più segmenti).

# Allocazione: statica o dinamica

- **Statica**
  - un programma deve mantenere la propria area di memoria dal caricamento alla terminazione
  - non è possibile rilocare il programma durante l'esecuzione
- **Dinamica**
  - durante l'esecuzione, un programma può essere spostato all'interno della memoria

# Allocazione a partizioni fisse

- **Descrizione**

- la memoria disponibile (quella non occupata dal s.o.) viene suddivisa in partizioni
- ogni processo viene caricato in una delle partizioni libere che ha dimensione sufficiente a contenerlo

- **Caratteristiche**

- statica e contigua
- vantaggi: molto semplice
- svantaggi: spreco di memoria, grado di parallelismo limitato dal numero di partizioni



# Allocazione a partizioni fisse

- **Gestione memoria**
  - è possibile utilizzare una coda di programmi da eseguire per partizione, oppure una coda comune per tutte le partizioni
- **Sistemi monoprogrammati**
  - esiste una sola partizione, dove viene caricato un unico programma utente
  - esempio:
    - MS-DOS
    - sistemi embedded



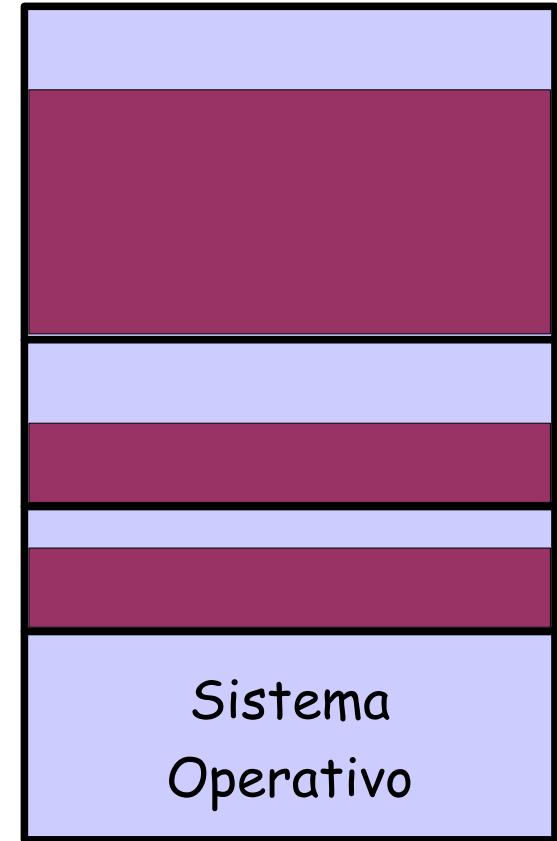
# Frammentazione interna

- **Nell'allocazione a partizione fisse**

- se un processo occupa una dimensione inferiore a quella della partizione che lo contiene, lo spazio non utilizzato è sprecato
- la presenza di spazio inutilizzato all'interno di un'unità di allocazione si chiama *frammentazione interna*

- **Nota:**

- il fenomeno della frammentazione interna non è limitata all'allocazione a partizioni fisse, ma è generale a tutti gli approcci in cui è possibile allocare più memoria di quanto richiesto (per motivi di organizzazione)



# Allocazione a partizioni dinamiche

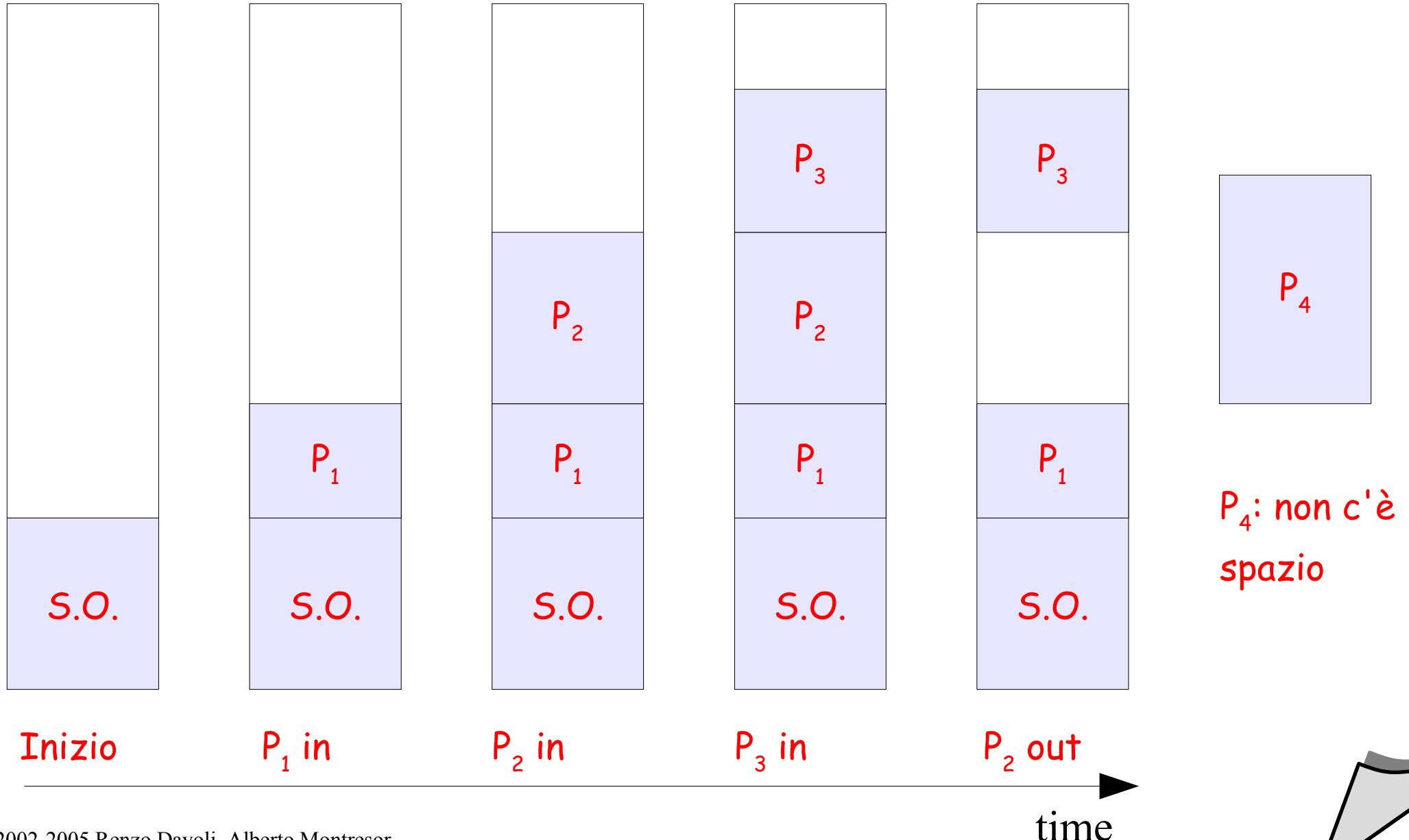
- **Descrizione**

- la memoria disponibile (nella quantità richiesta) viene assegnata ai processi che ne fanno richiesta
- nella memoria possono essere presenti diverse zone inutilizzate
  - per effetto della terminazione di processi
  - oppure per non completo utilizzo dell'area disponibile da parte dei processi attivi

- **Caratteristiche**

- statica e contigua
- esistono diverse politiche per la scelta dell'area da utilizzare

# Allocazione a partizioni dinamiche



# Frammentazione esterna

- **Problema**
  - dopo un certo numero di allocazioni e deallocazioni di memoria dovute all'attivazione e alla terminazione dei processi lo spazio libero appare suddiviso in piccole aree
  - è il fenomeno della *frammentazione esterna*
- **Nota**
  - la frammentazione *interna* dipende dall'uso di unità di allocazione di dimensione diversa da quella richiesta
  - la frammentazione *esterna* deriva dal susseguirsi di allocazioni e deallocazioni

# Compattazione

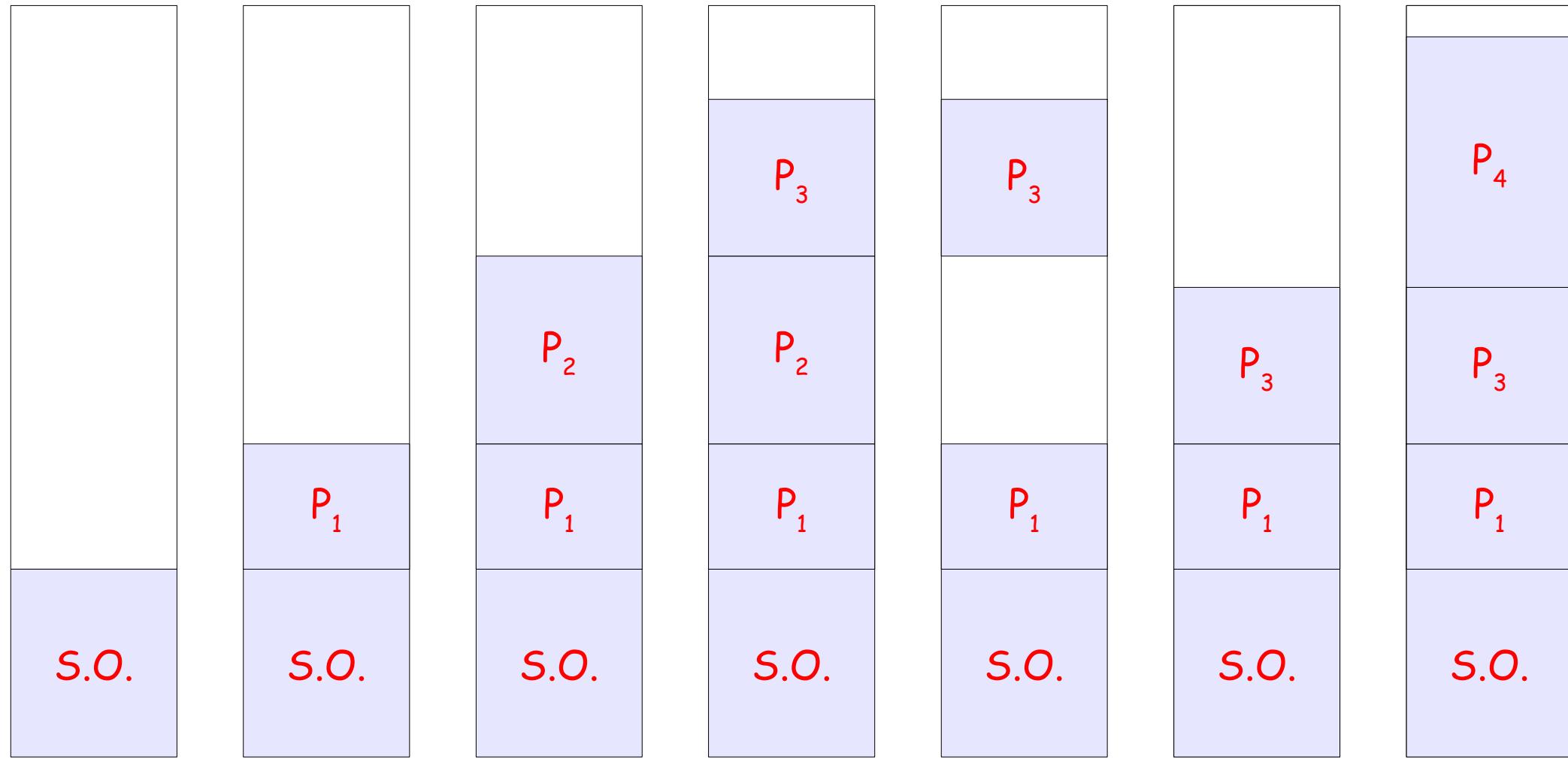
- **Compattazione**

- se è possibile rilocare i programmi durante la loro esecuzione, è allora possibile procedere alla *compattazione* della memoria
- compattare la memoria significa spostare in memoria tutti i programmi in modo da riunire tutte le aree inutilizzate
- è un'operazione volta a risolvere il problema della frammentazione esterna

- **Problemi**

- è un'operazione molto onerosa
  - occorre copiare (fisicamente) in memoria grandi quantità di dati
- non può essere utilizzata in sistemi interattivi
  - i processi devono essere fermi durante la compattazione

# Compattazione



# Allocazione dinamica - Selezione blocco libero

- L'operazione di selezione di un blocco libero è concettualmente indipendente dalla struttura dati
- **First Fit** 
  - scorre la lista dei blocchi liberi, partendo dall'inizio della lista, fino a quando non trova il primo segmento vuoto grande abbastanza da contenere il processo
- **Next Fit**
  - come First Fit, ma invece di ripartire sempre dall'inizio, parte dal punto dove si era fermato all'ultima allocazione
- **Commenti**
  - Next Fit è stato progettato per evitare di frammentare continuamente l'inizio della memoria
  - ma sorprendentemente, ha performance peggiori di First Fit

# Allocazione dinamica - Selezione blocco libero

- **Best Fit**
  - seleziona il più piccolo fra i blocchi liberi, sufficientemente grandi, presenti in memoria
- **Commenti**
  - più lento di First Fit, in quanto richiede di esaminare tutti i blocchi liberi presenti in memoria
  - genera più frammentazione di First Fit, in quanto tende a riempire la memoria di blocchi liberi troppo piccoli
- **Worst fit**
  - seleziona il più grande fra i blocchi liberi presenti in memoria
- **Commenti**
  - proposto per evitare i problemi di frammentazione di First/Best Fit
  - rende difficile l'allocazione di processi di grosse dimensioni

# Allocazione dinamica - Strutture dati (ancora)

- **Miglioramenti**

- è possibile ottimizzare il costo di allocazione
  - mantenendo una lista separata per i soli blocchi liberi
  - eventualmente, ordinando tale lista per dimensione

- **Dove mantenere queste informazioni**

- per i blocchi occupati
  - ad esempio, nella tabella dei processi
- per i blocchi liberi
  - nei blocchi stessi!
- è richiesta un'unità minima di allocazione

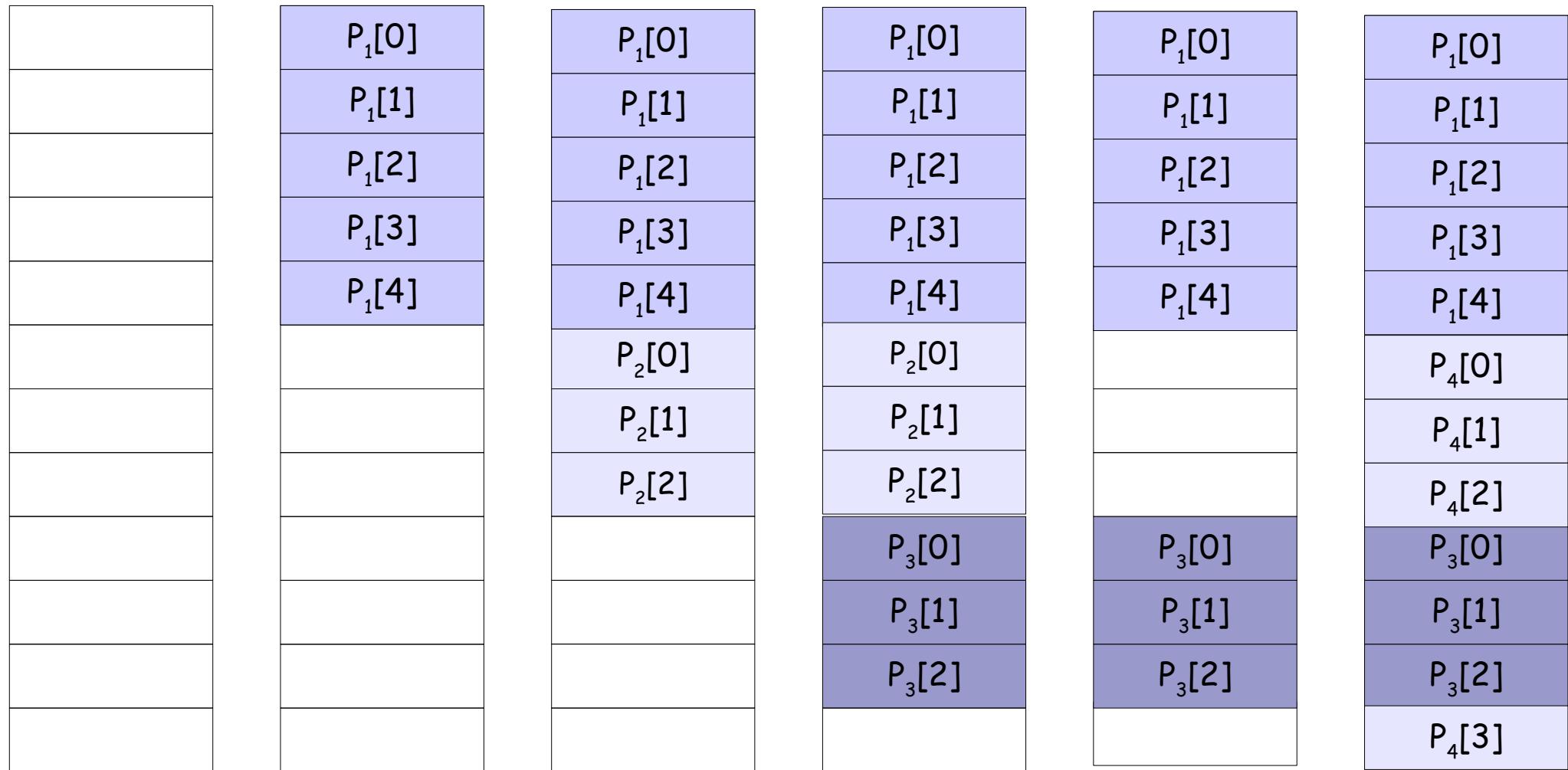
# Paginazione

- **Problema**
  - i meccanismi visti (partizioni fisse, partizioni dinamiche) non sono efficienti nell'uso della memoria
    - frammentazione interna
    - frammentazione esterna
- **Paginazione**
  - è l'approccio contemporaneo
    - riduce il fenomeno di frammentazione interna
    - minimizza (elimina) il fenomeno della frammentazione esterna
  - attenzione però: necessita di hardware adeguato

# Paginazione

- **Lo spazio di indirizzamento logico di un processo**
  - viene suddiviso in un insieme di blocchi di dimensione fissa chiamati *pagine*
- **La memoria fisica**
  - viene suddivisa in un insieme di blocchi della stessa dimensione delle pagine, chiamati *frame*
- **Quando un processo viene allocato in memoria:**
  - vengono reperiti ovunque in memoria un numero sufficiente di frame per contenere le pagine del processo

# **Paginazione - Esempio**



Tutto  
libero

P<sub>1</sub> in

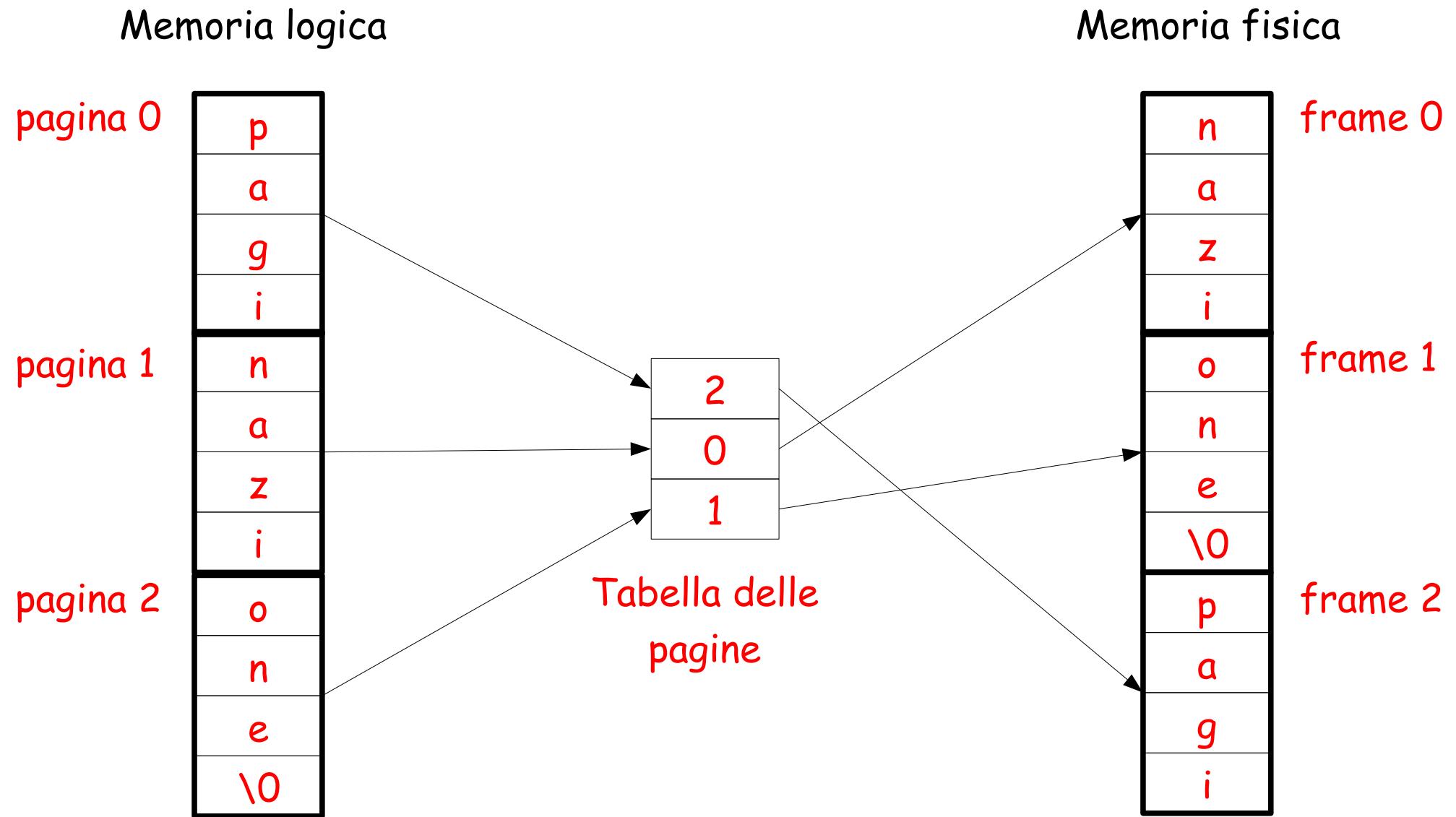
P<sub>2</sub> in

P<sub>3</sub> in

P<sub>2</sub> out

P<sub>4</sub> in

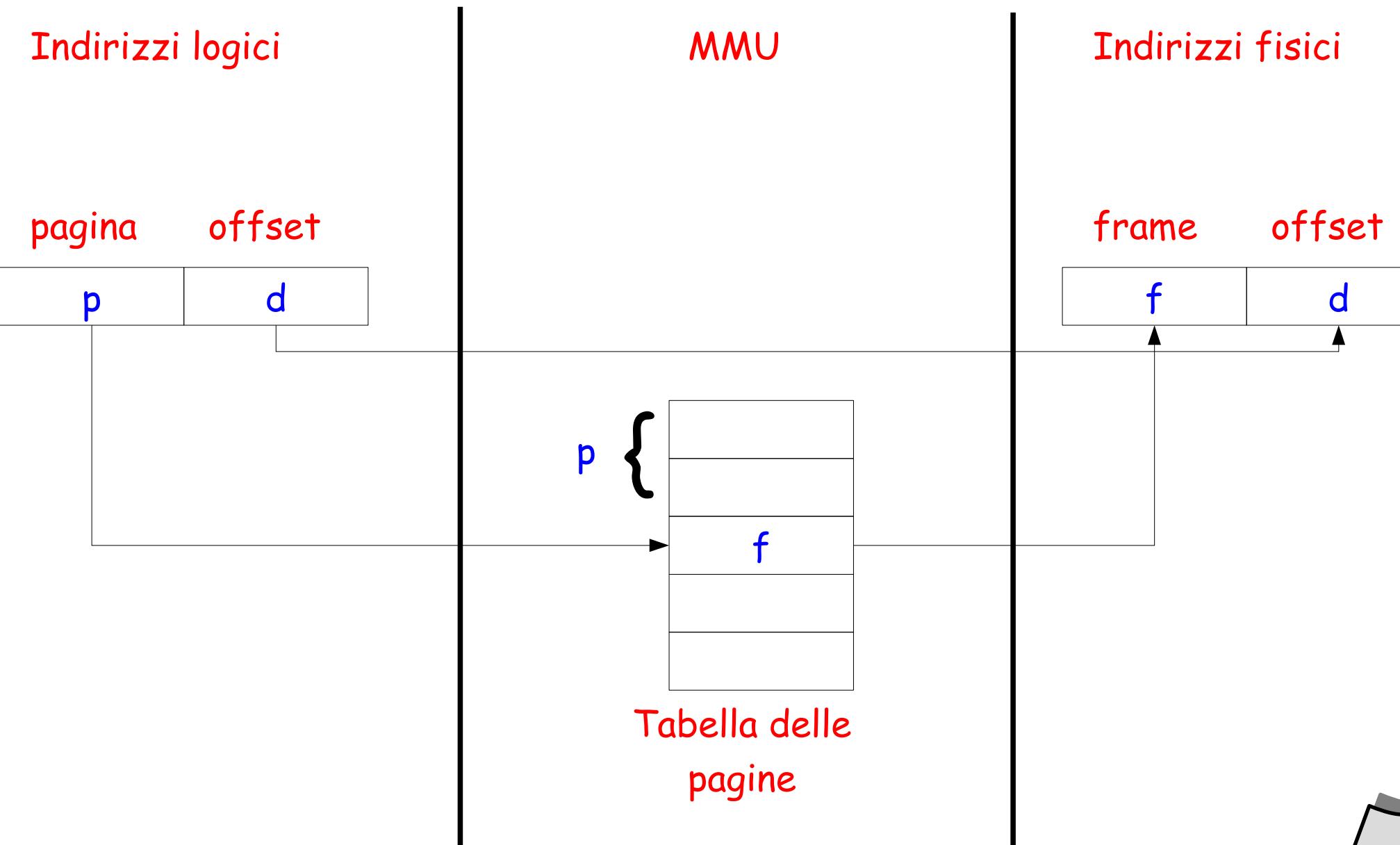
# Paginazione - Esempio



# Dimensione delle pagine

- **Come scegliere la dimensione delle pagine?**
  - la dimensione delle pagine deve essere una potenza di due, per semplificare la trasformazione da indirizzi logici a indirizzi fisici
  - la scelta della dimensione deriva da un trade-off
    - con pagine troppo piccole, la tabella delle pagine cresce di dimensioni
    - con pagine troppo grandi, lo spazio di memoria perso per frammentazione interna può essere considerevole
  - valori tipici: 1KB, 2KB, **4KB**, 4MB

# Supporto hardware (MMU) per paginazione



# Implementazione della page table

- **Dove mettere la tabella delle pagine?**
- **Soluzione 1: registri dedicati**
  - la tabella può essere contenuta in un insieme di registri ad alta velocità all'interno del modulo MMU (o della CPU)
  - problema: troppo costoso
  - esempio:
    - pagine di 4K, processore a 32 bit
    - numero di pagine nella page table: 1M (1.048.576)
- **Soluzione 2: totalmente in memoria**
  - problema: il numero di accessi in memoria verrebbe raddoppiato; ad ogni riferimento, bisognerebbe prima accedere alla tabella delle pagine, poi al dato
    - **Soluzione:** cache per tabella delle pagine: **Translation lookaside buffer (TLB)**

# Segmentazione

- **In un sistema con segmentazione**
  - la memoria associata ad un programma è suddivisa in aree differenti dal punto di vista funzionale
- **Esempio**
  - aree text:
    - contengono il codice eseguibile
    - sono normalmente in sola lettura (solo i virus cambiano il codice)
    - possono essere condivise tra più processi (codice reentrant)
  - aree dati
    - possono essere condivise oppure no
  - area stack
    - read/write, non può assolutamente essere condivisa

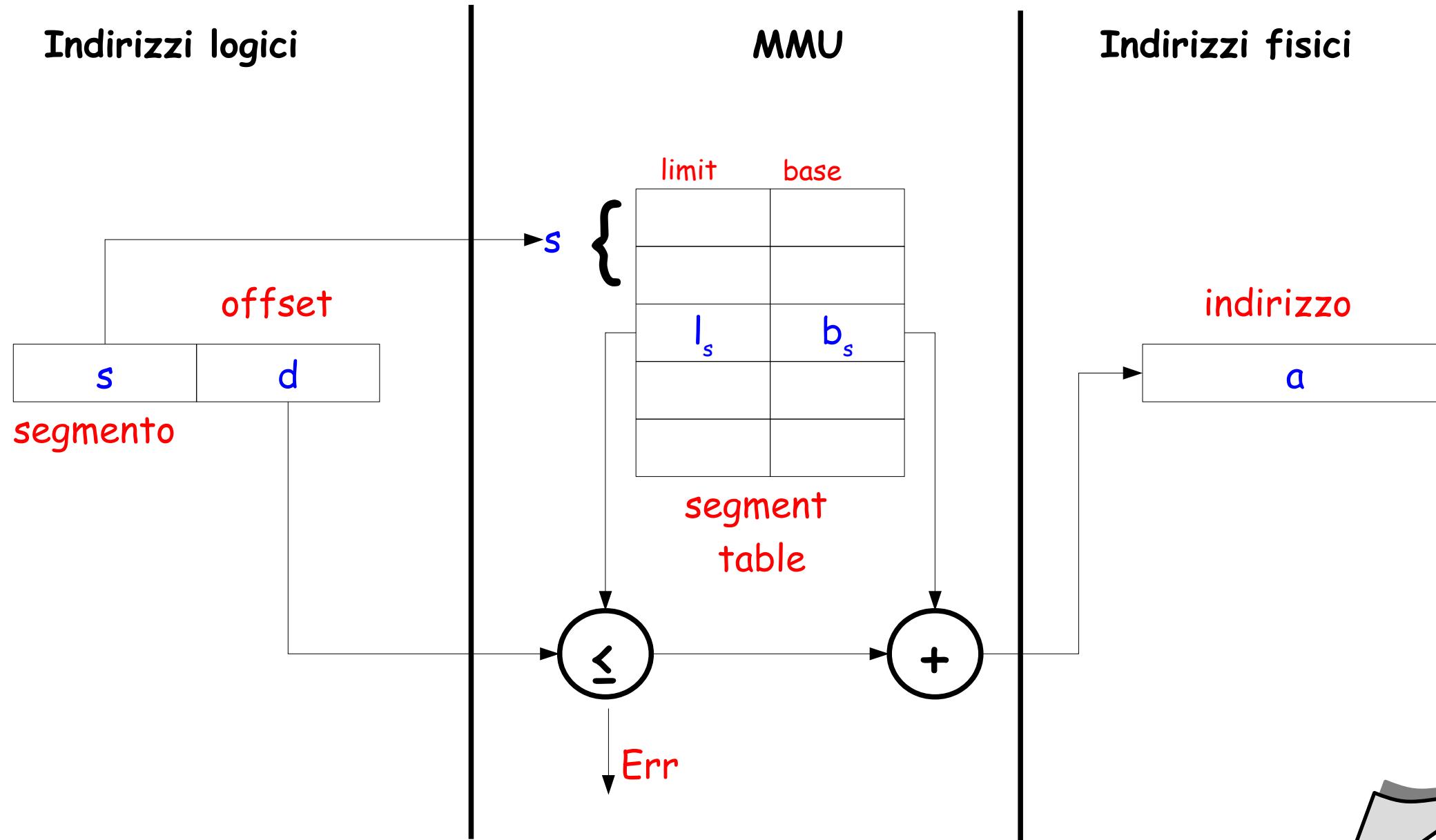
# Segmentazione

- **In un sistema basato su segmentazione**
  - uno spazio di indirizzamento logico è dato da un insieme di segmenti
  - un segmento è un'area di memoria (logicamente continua) contenente elementi tra loro affini
  - ogni segmento è caratterizzato da un *nome* (normalmente un indice) e da una *lunghezza*
  - ogni riferimento di memoria è dato da una coppia  
*<nome segmento, offset>*
- **Spetta al programmatore o al compilatore la suddivisione di un programma in segmenti**

# Segmentazione vs Paginazione

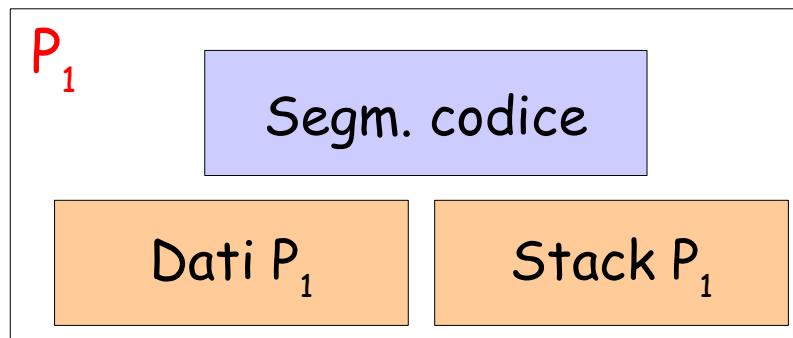
- **Paginazione**
  - la divisione in pagine è automatica.
  - le pagine hanno dimensione fissa
  - le pagine possono contenere informazioni disomogenee (ad es. sia codice sia dati)
  - una pagina ha un indirizzo
  - dimensione tipica della pagina: 1-4 KB
- **Segmentazione**
  - la divisione in segmenti spetta al programmatore.
  - i segmenti hanno dimensione variabile
  - un segmento contiene informazioni omogenee per tipo di accesso e permessi di condivisione
  - un segmento ha un nome.
  - dimensione tipica di un segmento: 64KB - 1MB

# Supporto hardware per segmentazione

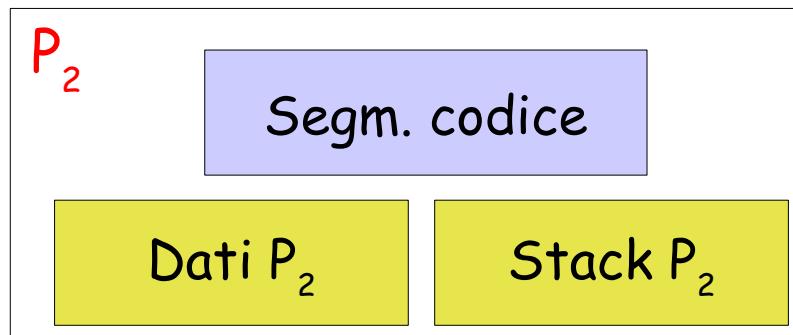


# Segmentazione e condivisione

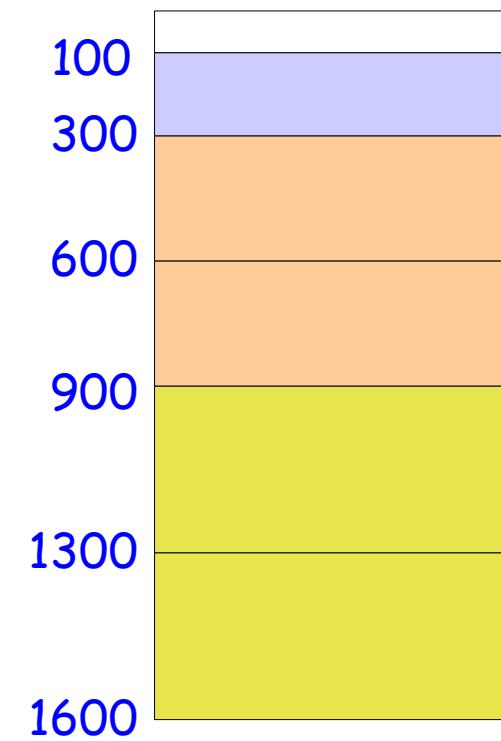
- La segmentazione consente la condivisione di codice e dati
- Esempio: editor condiviso



Code	100	200
Data	300	300
Stack	600	300



Code	100	200
Data	900	400
Stack	1300	400



# Segmentazione e frammentazione

- **Problema**
  - allocare segmenti di dimensione variabile è del tutto equivalente al problema di allocare in modo contiguo la memoria dei processi
  - è possibile utilizzare
    - tecniche di allocazione dinamica (e.g., First Fit)
    - compattazione
- **ma così torniamo ai problemi precedenti, quelli incontrati nella allocazione contigua di memoria per tutto un processo !**

# Segmentazione e paginazione

- **Segmentazione + paginazione**
  - è possibile utilizzare il metodo della paginazione combinato al metodo della segmentazione
  - ogni segmento viene suddiviso in pagine che vengono allocate in frame liberi della memoria (non necessariamente contigui)
- **Requisiti hardware**
  - la MMU deve avere sia il supporto per la segmentazione sia il supporto per la paginazione
- **Benefici**
  - sia quelli della segmentazione (condivisione, protezione)
  - sia quelli della paginazione (no frammentazione esterna)

# Memoria virtuale

- **Definizione**
  - è la tecnica che permette l'esecuzione di processi che non sono completamente in memoria
- **Considerazioni**
  - permette di eseguire in concorrenza processi che nel loro complesso (o anche singolarmente) hanno necessità di memoria maggiore di quella disponibile
  - la memoria virtuale può diminuire le prestazioni di un sistema se implementata (e usata) nel modo sbagliato

# Memoria virtuale

- **Requisiti di un'architettura di Von Neumann**
  - le istruzioni da eseguire e i dati su cui operano devono essere in memoria
- **ma....**
  - non è necessario che l'intero spazio di indirizzamento logico di un processo sia in memoria
  - i processi non utilizzano tutto il loro spazio di indirizzamento *contemporaneamente*
    - routine di gestione errore
    - strutture dati allocate con dimensioni massime ma utilizzate solo parzialmente
    - passi di avanzamento di un programma (e.g. compilatore a due fasi)

# Memoria virtuale

- ♦ **Implementazione**

- ♦ ogni processo ha accesso ad uno *spazio di indirizzamento virtuale* che può essere più grande di quello fisico
- ♦ gli indirizzi virtuali
  - possono essere mappati su indirizzi fisici della memoria principale
  - oppure, possono essere mappati su memoria secondaria (spazio su disco)
- ♦ in caso di accesso ad indirizzi virtuali mappati in memoria secondaria:
  - i dati associati vengono trasferiti in memoria principale
  - se la memoria è piena, si sposta in memoria secondaria i dati contenuti in memoria principale che sono considerati meno utili

# Memoria virtuale

- **Paginazione a richiesta (*demand paging*)**
  - si utilizza la tecnica della paginazione, ammettendo però che alcune pagine possano essere in memoria secondaria
- **Nella tabella delle pagine**
  - si utilizza un bit (*v*, per valid) che indica se la pagina è presente in memoria centrale oppure no
- **Quando un processo tenta di accedere ad un pagina non in memoria**
  - il processore genera una eccezione di tipo fault (*page fault*)
  - un componente del s.o. (*pager*) si occupa di caricare la pagina mancante in memoria, e di aggiornare di conseguenza la tabella delle pagine

# Memoria virtuale - Esempio

0	A
1	B
2	C
3	D
4	E
5	F
6	G
7	H

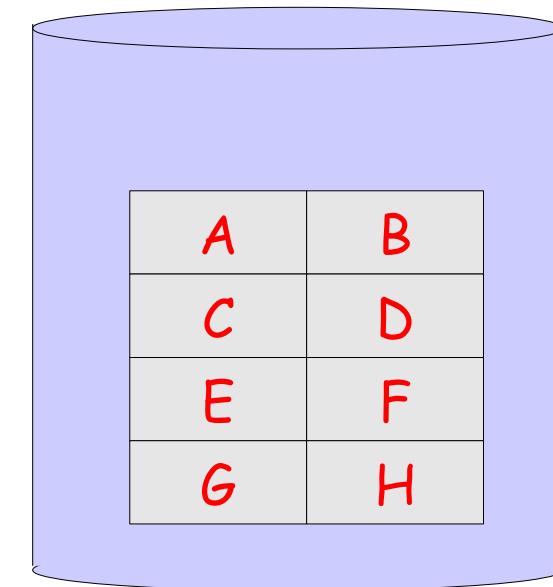
frame	bit valid/ invalid	
	4	v
0		i
1	6	v
2		i
3		i
4		i
5	1	v
6		i
7		i

0	
1	F
2	
3	
4	A
5	
6	C
7	
8	
9	
10	
11	

Memoria  
Logica

Page Table

Memoria  
principale



Memoria  
secondaria

# Pager/swapper

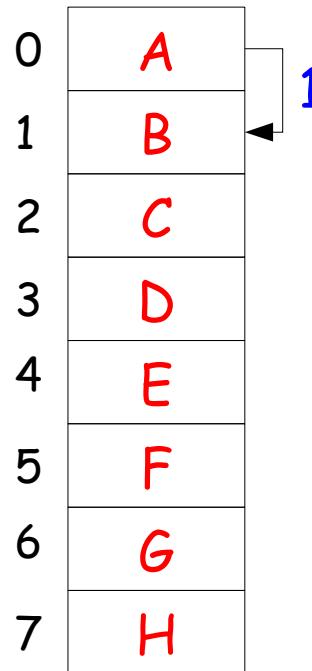
- **Swap**
  - con questo termine si intende l'azione di copiare l'intera area di memoria usata da un processo
    - dalla memoria secondaria alla memoria principale (*swap-in*)
    - dalla memoria principale alla memoria secondaria (*swap-out*)
  - era una tecnica utilizzata nel passato quando demand paging non esisteva
- **Paginazione su richiesta**
  - può essere vista come una tecnica di swap di tipo lazy (pigro)
  - viene caricato solo ciò che serve

# Pager/swapper

- **Per questo motivo**
  - alcuni sistemi operativi indicano il pager con il nome di *swapper*
  - è da considerarsi una terminologia obsoleta
- **Nota**
  - però utilizziamo il termine *swap area* per indicare l'area del disco utilizzata per ospitare le pagine in memoria secondaria

# Gestione dei page fault

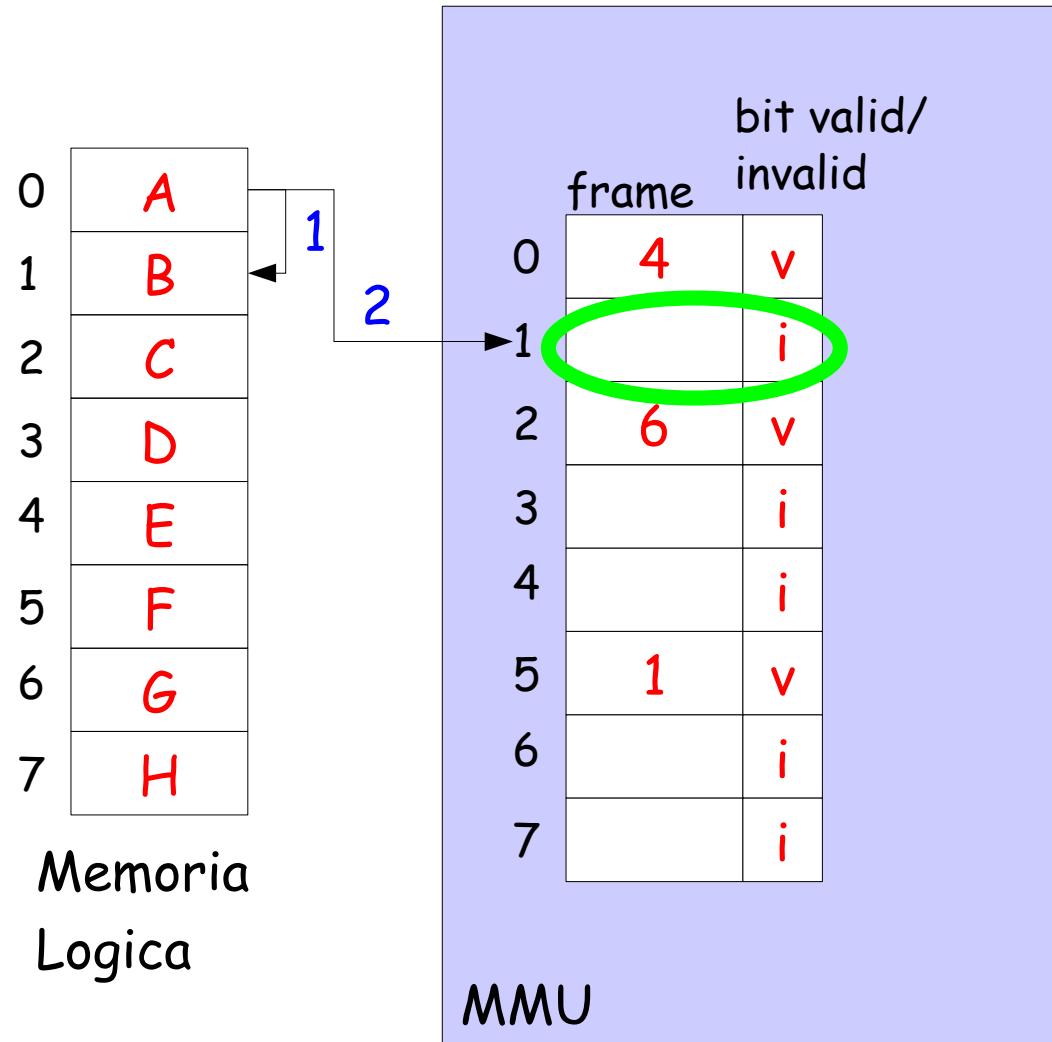
- Supponiamo che una istruzione macchina del codice in pagina 0 faccia riferimento alla pagina 1



Memoria  
Logica

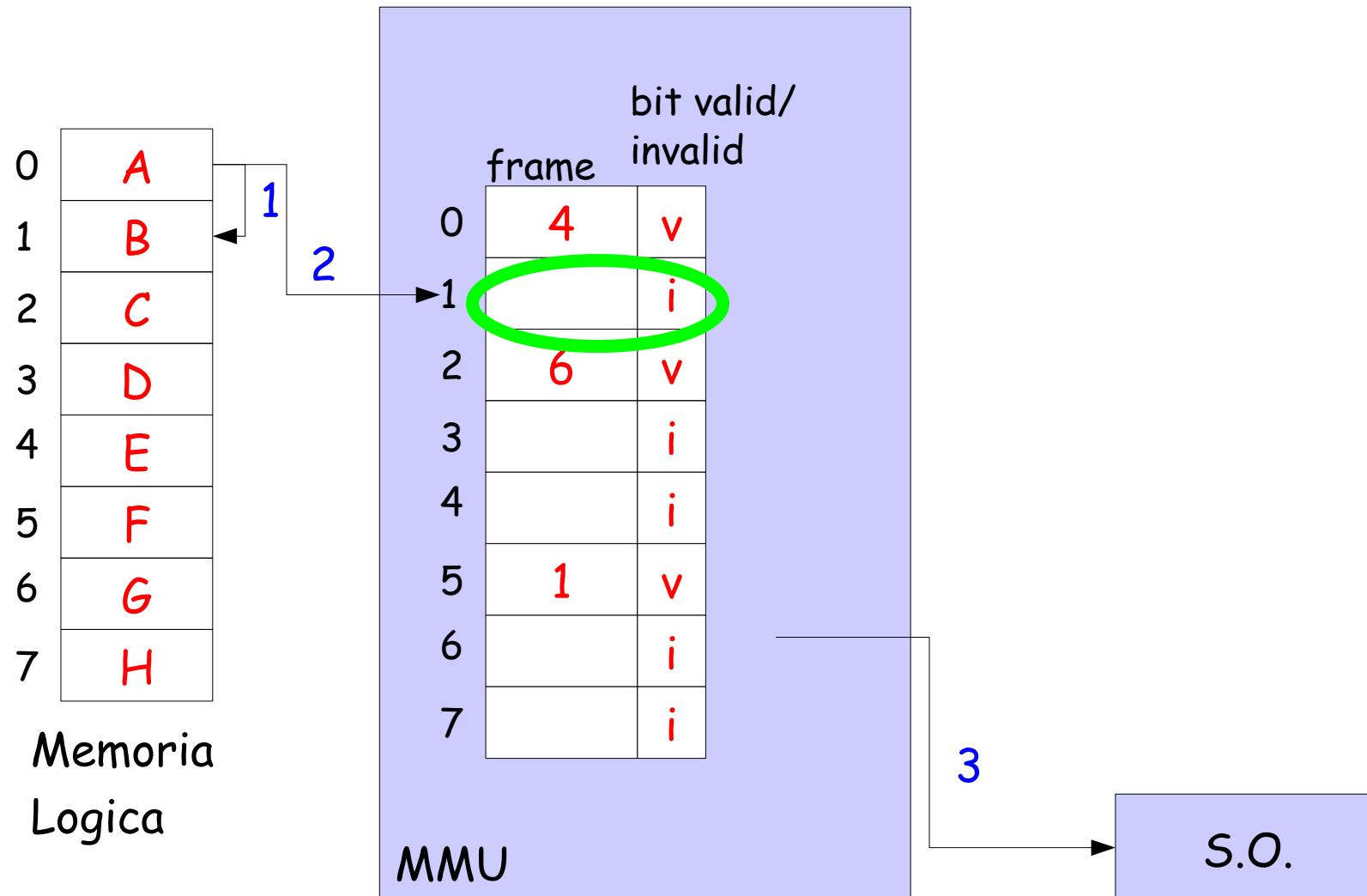
# Gestione dei page fault

- La MMU scopre che la pagina 1 non è in memoria principale



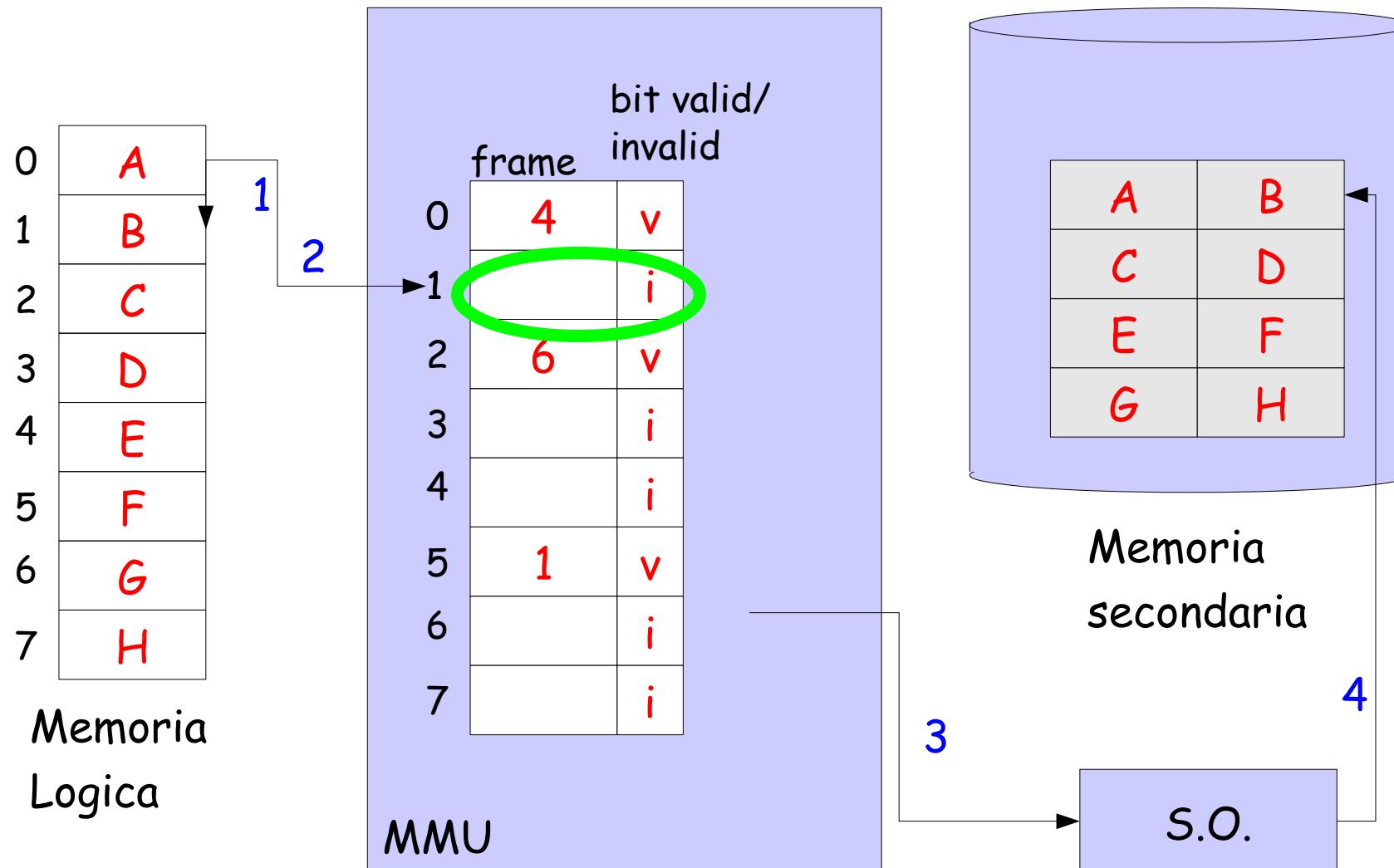
# Gestione dei page fault

- Viene generato una eccezione di tipo fault "page fault", che viene catturato dal s.o.



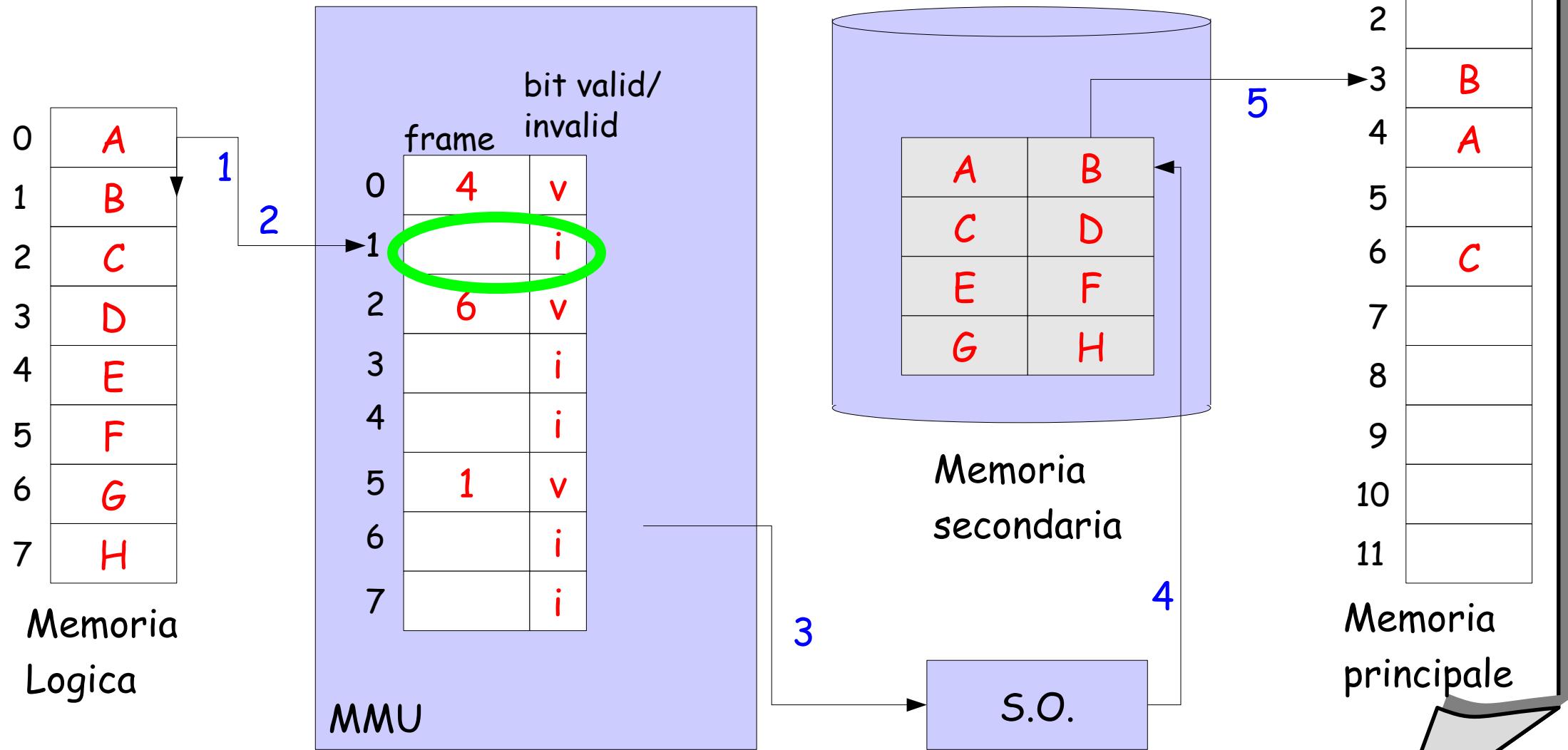
# Gestione dei page fault

- Il s.o. cerca in memoria secondaria la pagina da caricare



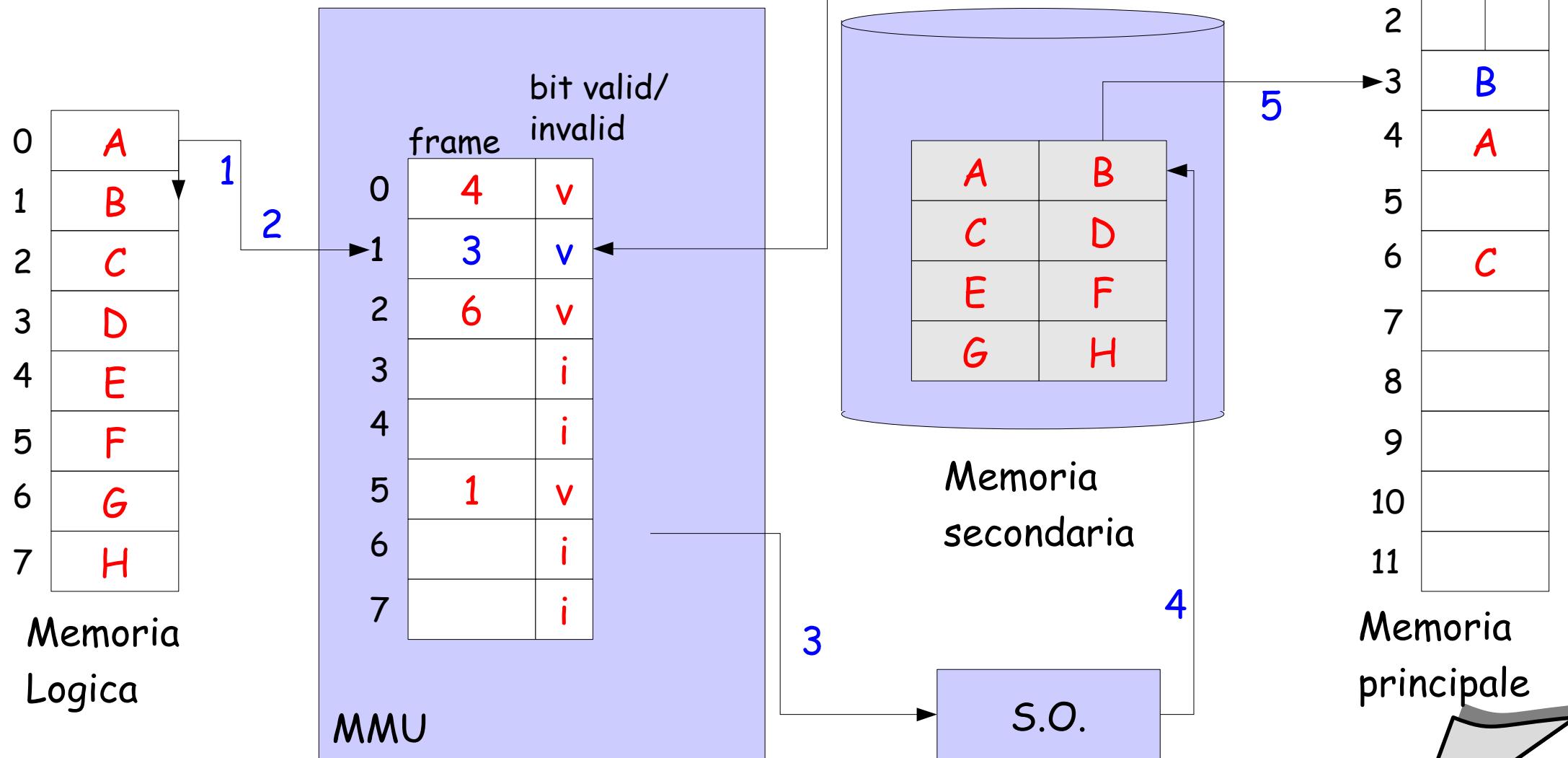
# Gestione dei page fault

- Il s.o. carica la memoria principale con il contenuto della pagina



# Gestione dei page fault

- Il s.o. aggiorna la page table in modo opportuno e riavvia l'esecuzione dell'istruzione



# Gestione dei page fault

- **Cosa succede in mancanza di frame liberi?**
  - occorre "liberarne" uno
  - la pagina vittima deve essere la meno "utile"
- **Algoritmi di sostituzione o rimpiazzamento**
  - la classe di algoritmi utilizzati per selezionare la pagina da sostituire

# Algoritmo del meccanismo di demand paging

- Individua la pagina in memoria secondaria (disco)
- Individua un frame libero
- Se non esiste un frame libero
  - richiama algoritmo di rimpiazzamento
  - aggiorna la tabella delle pagine (invalida pagina "vittima")
  - se la pagina "vittima" è stata variata, scrive la pagina sul disco
  - aggiorna la tabella dei frame (frame libero)
- Aggiorna la tabella dei frame (frame occupato)
- Leggi la pagina da disco (quella che ha provocato il fault)
- Aggiorna la tabella delle pagine
- Riattiva il processo

# On demand puro

---

- È possibile avviare l'esecuzione di un processo senza pagine in memoria:
  - Quando il SO carica nel program counter l'indirizzo della prima istruzione, genera un primo page fault
  - Una volta portata la prima pagina in memoria, le altre vengono caricate quando sono indirizzate perché contengono dati o codice.
- Questo schema di esecuzione è detta **paginazione su richiesta pura**

# Morale

---

- In un sistema con memoria virtuale basata su paginazione su richiesta è importante **tenere basso il numero dei page fault** altrimenti il tempo effettivo di accesso aumenta a dismisura e si rallenta notevolmente l'esecuzione dei processi.
- E' cruciale **scegliere bene il meccanismo di sostituzione** delle pagine!

# Sostituzione delle pagine

---

- Se nessun frame è libero è possibile liberarne uno occupato scaricando il suo contenuto dalla memoria centrale alla backing store.
- La **sostituzione delle pagine** (una è stata scaricata – **swap out** - e una è stata caricata – **swap in** -) deve poi essere registrata nelle tabella delle pagine.

# Dirty bit

---

- Lo scaricamento può essere evitato se la pagina da scaricare non è stata modificata.
- Per verificare questa condizione occorre aggiungere alla pagina un **bit di modifica (dirty bit)** che viene gestito via hardware:
  - Quando la pagina è caricata viene messo a 0
  - Quando la pagina è scritta viene messo a 1
  - Quando la pagina è scaricata viene fatta la scrittura su disco solo se il bit di modifica è a 1.

# Paginazione a richiesta

---

- Il meccanismo di sostituzione illustrato sino ad ora necessita della definizione di due componenti fondamentali:
  - L'algoritmo per l'**allocazione dei frame** che decide quanti frame devono essere allocati a ciascun processo.
  - L'algoritmo per la **sostituzione delle pagine** che decide quale pagina debba essere scaricata se non ci sono frame liberi.

# File System

## Concetti principali

# Sommario

---

- Concetto di File e directory
- Metodi di accesso
- Struttura del File system

# File system

---

- Per la maggior parte degli utenti il **file system** è l'aspetto più visibile del SO.
- Il file system rappresenta una astrazione del modo con cui i dati sono allocati e organizzati su un dispositivo memoria di massa.
- Attraverso il file system, il SO offre una visione **logica** uniforme della memorizzazione delle informazioni sui diversi supporti (dischi, nastri, CD, ecc.).
- Elemento di base nella gestione a livello logico della memoria di massa è il **file**.

# File

---

- Un **file** è un insieme di informazioni correlate e registrate nella memoria secondaria con un nome.
- Il file è la più piccola unità di memoria secondaria assegnabile all'utente che può scrivere sulla memoria secondaria solo registrando un file.
- Il file può avere una sua struttura interna, a seconda del formato o del tipo. Per esempio un file eseguibile è una sequenza di sezioni di codice che possono essere caricate ed eseguite.

# Attributi

---

- Principali attributi del file sono:
  - **Nome:** è l'unica informazione mantenuta in un formato simbolico leggibile da una persona.
  - **Tipo:** usato nei sistemi che supportano più tipi diversi di file.
  - **Locazione:** puntatore al dispositivo e alla locazione di quel file sul dispositivo.
  - **Dimensione.**

# Attributi

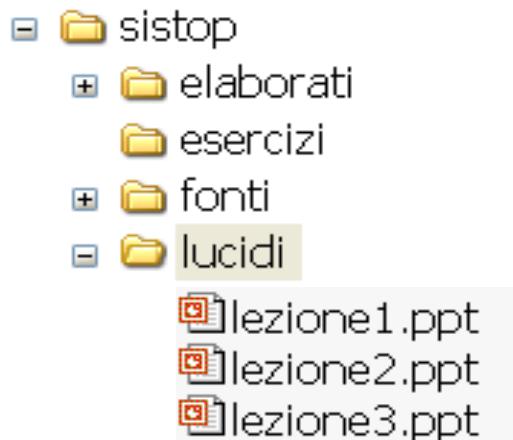
---

- Altri importanti attributi del file sono:
  - **Protezione:** informazioni di controllo che specificano chi può leggere, scrivere o eseguire il file.
  - **Ora, data e identificazione dell'utente:** informazioni usate per funzioni di protezione dei dati e di monitoring. Possono essere riferite a:
    - Creazione
    - Ultimo utilizzo
    - Ultima lettura

# Directory

---

- Il file system può essere molto ampio (contenere molte migliaia di file) e tipicamente è organizzato in una struttura gerarchica che mantiene gli elementi terminali (i file) all'interno di contenitori detti **directory**.



# File in uso

---

- Il sistema mantiene in memoria l'elenco dei file in uso in una apposita tabella detta **tabella dei file aperti**
- Quando viene iniziata una operazione sul file, il file viene inserito nella tabella in modo che ogni successiva operazione non comporti fasi di ricerca

# Informazioni sui file aperti

---

- A ciascun file aperto sono associate diverse informazioni:
  - **Puntatore alla posizione corrente nel file:** per il supporto a read e write. Se più processi operano sul file esistono più puntatori alla posizione corrente.
  - **Contatore delle aperture:** se più processi possono aprire il file, il SO deve tenere conto delle aperture avvenute e quando sono tutte chiuse, rimuovere il file dalla tabella dei file aperti.
  - **Posizione su disco del file:** quando il file è aperto viene memorizzata la sua posizione sul dispositivo per evitare di doverlo cercare nuovamente ad ogni operazione.

# Struttura dei file

---

- Tipicamente il SO non si occupa di gestire la **struttura interna** associata ai diversi tipi di file, ma lascia che siano le applicazioni a definirla e utilizzarla.
- Per il SO i file sono sostanzialmente insiemi ordinati di byte e le convenzioni che danno un significato specifico ai byte (cioè il formato dei file) sono gestiti a livello applicazione.
- I vantaggi nel delegare la gestione dei formati alle applicazioni sono diversi:
  - Dimensioni del codice del SO: per gestire tutti i formati il sistema dovrebbe essere enorme. Lasciando il controllo alle applicazioni si limita la dimensione del SO.
  - Flessibilità nella definizione di nuove strutture: quando occorre gestire nuovi formati non è necessario modificare il file system e il SO ma è sufficiente dotarsi delle applicazioni appropriate.
- Tutti i SO supportano almeno il formato dei file eseguibili, per poterli caricare in memoria ed eseguire.

# Struttura interna del file

---

- Si noti che :
  - lo spazio fisico è allocato per blocchi, è probabile che l'ultimo blocco di un file sia usato parzialmente, ovvero che una parte dell'ultimo blocco di un file vada sprecata.
  - Maggiore è la dimensione del blocco, maggiore è la frammentazione interna legata a questo fenomeno.

# Metodi di accesso

---

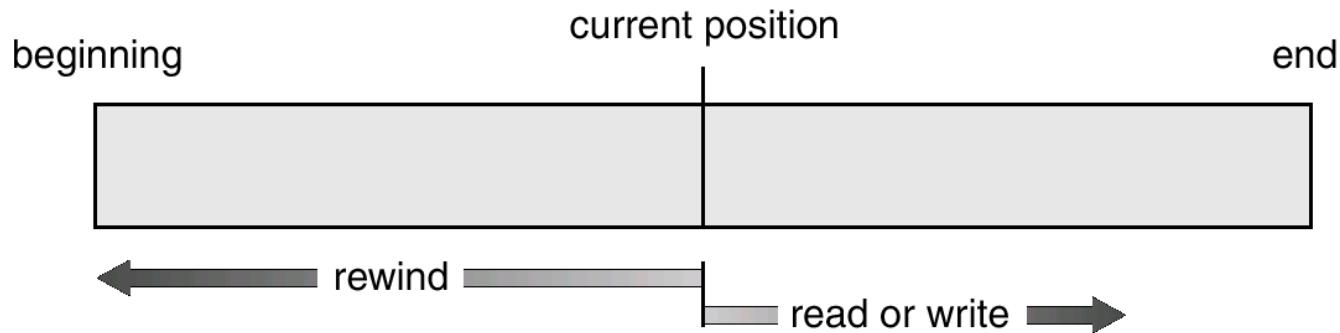
- Il SO può fornire diversi metodi di accesso ai file:
  - **Sequenziale**: le informazioni del file vengono elaborate in ordine, un record dopo l'altro.
    - nastri
  - **Diretto**: il file è costituito da un insieme ordinato di blocchi a cui si accede direttamente.
    - dischi
  - **Attraverso indice**: al file vero e proprio è associato un file indice con lo scopo di velocizzare le ricerche.
    - Database

# Accesso sequenziale

---

- Le informazioni del file vengono elaborate in ordine, un record dopo l'altro. E' il più utilizzato (ES: compilatori).
- Operazioni:
  - **Lettura:** **read**, legge la prossima porzione del file e avanza il puntatore di posizione.
  - **Scrittura:** **write**, scrive i nuovi dati in coda al file e avanza l'end of file.
  - **Reset:** riposiziona il puntatore di posizione a inizio file.

# Accesso sequenziale



# Accesso diretto

---

- Il modello i riferimento per l'accesso sequenziale sono i dispositivi come il nastro che consentono solo accessi in sequenza.
- I dispositivi ad accesso casuale (nel senso di non sequenziale) sono modello per un altro metodo di accesso al file: **l'accesso diretto** (o **accesso relativo**) in cui il file è costituito da record logici di lunghezza fissa e viene considerato come un insieme ordinato di blocchi (record) numerati che possono essere acceduti in modo arbitrario.
- Il **numero di blocco** è tipicamente assegnato in modo **relativo** (ciascun file inizia con il suo blocco 0).

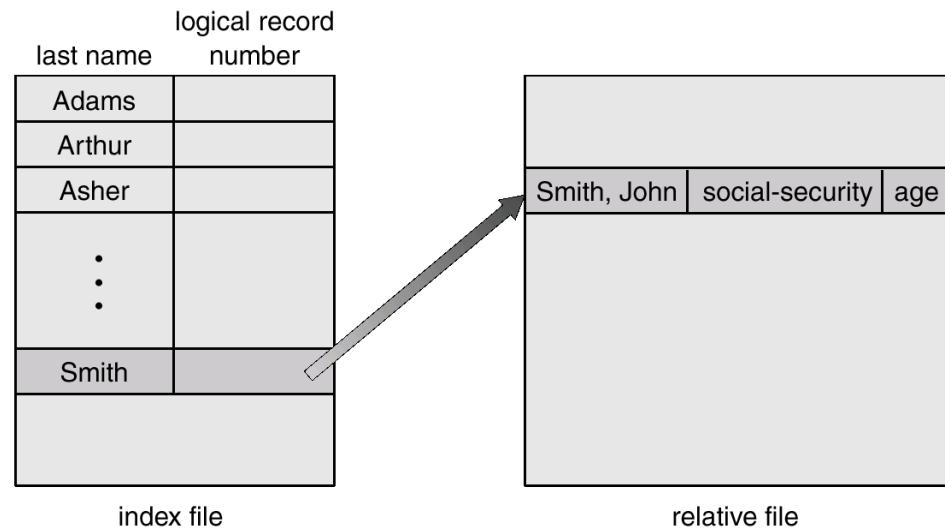
# Accesso diretto

- Le istruzioni di lettura e scrittura devono quindi specificare su quale blocco devono essere eseguite:
  - **Lettura:** **read(n)**, legge il blocco con posizione relativa n.
  - **Scrittura:** **write(n)** scrive il blocco con posizione relativa n.
  - **Riposizionamento:** **seek(n)**, si posiziona sul blocco
- L'accesso sequenziale è facilmente realizzabile se si ha a disposizione l'accesso diretto (cp means current position):

sequential access	implementation for direct access
<i>reset</i>	$cp = 0;$
<i>read next</i>	<i>read cp;</i> $cp = cp+1;$
<i>write next</i>	<i>write cp;</i> $cp = cp+1;$

# Indici

- Un altro metodo di accesso, che offre supporto alla ricerca veloce di occorrenze in un file, è quello che prevede la costruzione di un **indice**.
- L'indice contiene una o più chiavi di ricerca a cui sono associati i puntatori ai diversi blocchi del file.
- Il file contenente l'indice viene quindi associato ad un file di contenuti.



# Strutture del file system: File Control Block

- Per il sistema operativo i file vengono memorizzati in un opportuno descrittore, detto File Control Block che contiene, tra l'altro:

- Nome
- Proprietario
- Dimensioni
- Permessi di accesso
- Posizioni dei blocchi



- Il descrittore occupa un blocco su disco.
- Il descrittore si chiama inode nei file system unix.
- Altri blocchi sono utilizzati come blocchi dei dati.

# Allocazione dei blocchi

---

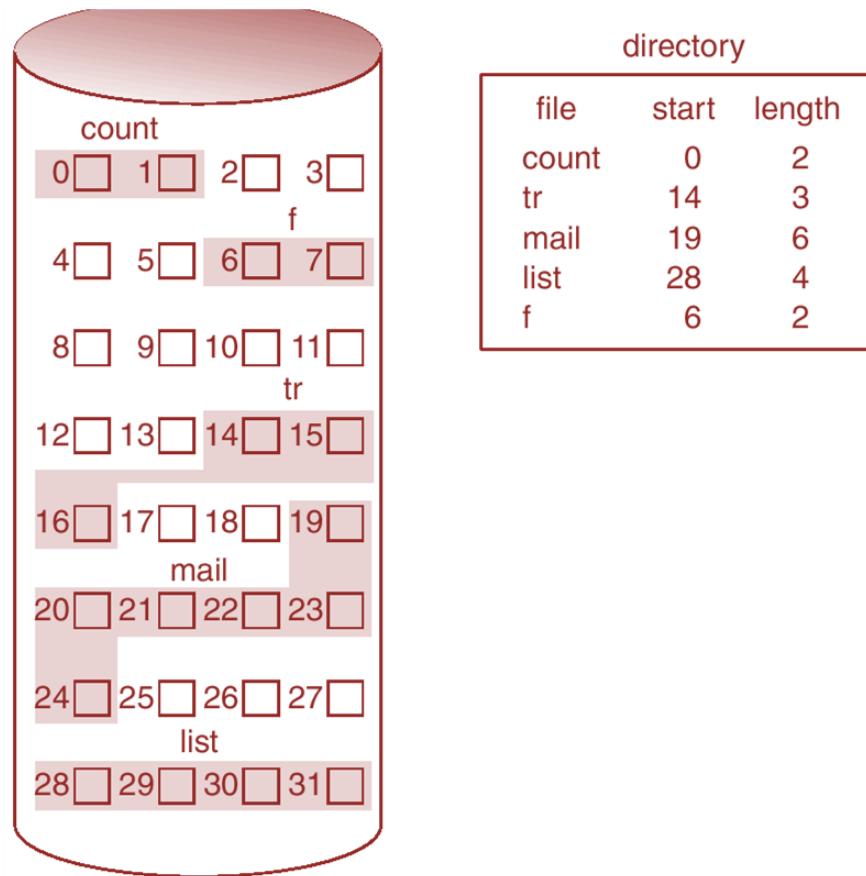
- Un elemento che incide fortemente sulle prestazioni è il **metodo di allocazione dei blocchi**, che specifica come i blocchi del disco sono allocati ai diversi file.
- Ci sono sostanzialmente tre metodologie per allocare i blocchi:
  - Contiguous allocation (allocazione **contigua**).
  - Linked allocation (allocazione **concatenata**).
  - Indexed allocation (allocazione **indicizzata**).

# Allocazione contigua

---

- Nell'**allocazione contigua** ogni file deve occupare un insieme di blocchi contigui del disco.
  - Gli indirizzi del disco definiscono un ordinamento lineare dei blocchi.
  - L'accesso sequenziale al blocco **b+1** seguente all'accesso al blocco **b** non richiede spostamento della testina.
  - L'accesso diretto è fatto semplicemente calcolando la posizione assoluta in base a quella relativa.
  - Il file è definito dalla posizione iniziale e dalla lunghezza.
  - L'accesso è molto semplice.

# Allocazione contigua



# Allocazione contigua

---

- La difficoltà sta nel reperire una porzione di disco sufficientemente grande da contenere tutto il file: il sistema di gestione dello spazio libero deve risolvere questo problema e alcune soluzioni sono lente.
- Il problema è simile a quello dell'allocazione della memoria e in questo caso le strategie più utilizzate sono **first fit** e **best fit**.
- Il sistema soffre di **frammentazione esterna** che viene risolta con routine di **deframmentazione**.

# Allocazione contigua

---

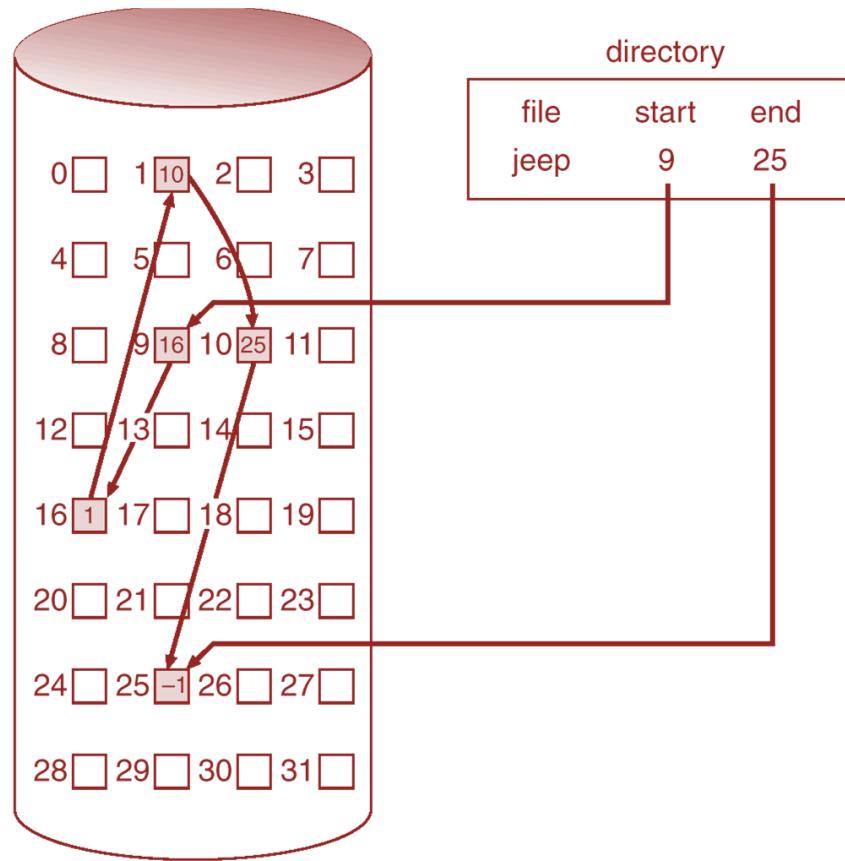
- Se lo spazio allocato è quasi uguale alla dimensione del file il file è difficilmente **estendibile**, poiché occorre **copiare** il contenuto del file in una nuova allocazione più ampia prima di consentire l'estensione.
- Se per evitare la copia si alloca uno spazio più grande della dimensione attuale del file (**preallocazione**), si genera **frammentazione interna**.
- Si possono usare meccanismi per compattare lo spazio, recuperando quello perso in frammentazione esterna mediante copie di spostamento (ma l'operazione è lenta e non risolve la frammentazione interna).

# Allocazione concatenata

---

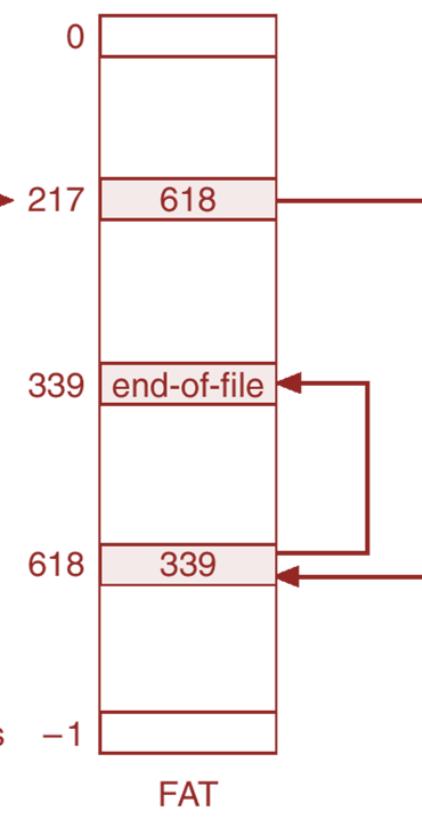
- Per risolvere i problemi di frammentazione introdotti dall’allocazione contigua si può utilizzare **l’allocazione concatenata**.
- Ogni file è costituito da una lista concatenata di blocchi del disco che possono essere distribuiti in qualunque parte del disco stesso.
- La directory contiene un puntatore al primo blocco del file.

# Allocazione concatenata



# File-Allocation Table

directory entry



# Allocazione concatenata

---

- Non esiste **frammentazione esterna** perché ogni blocco viene allocato singolarmente (quindi tutti i blocchi sono candidati ad essere allocati).
- Non esiste **frammentazione interna** perché non è necessario pre-allocare il file (che cresce al bisogno).
- In questo caso l'allocazione è semplificata a spese dell'accesso.
- **Problemi:**
  - È relativamente efficace nell'accesso sequenziale, perché comporta lo spostamento delle testine al nuovo blocco.
  - È inefficiente nell'accesso diretto, perché occorre scorrere il file per trovare la locazione  $i$ -esima.
  - Usa molto spazio per i puntatori, poiché ogni blocco c'è un puntatore al successivo.

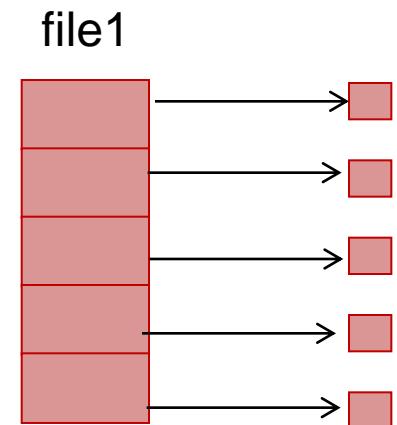
# Clustering

---

- Per risolvere quest'ultimo problema solitamente non si allocano blocchi ma gruppi (**cluster**) di blocchi (ad esempio 4):
  - **Vantaggi**: meno puntatori, meno movimenti della testina, più semplice la gestione dei blocchi liberi.
  - **Svantaggi**: frammentazione interna (parte del blocco può rimanere inutilizzata).

# Allocazione Indicizzata

- La maggioranza dei problemi riscontrati con l'allocazione concatenata può essere risolto inserendo tutti i puntatori ai blocchi in una apposita tabella detta blocco indice (**index block**).
- Questo approccio è detto **allocazione indicizzata**.

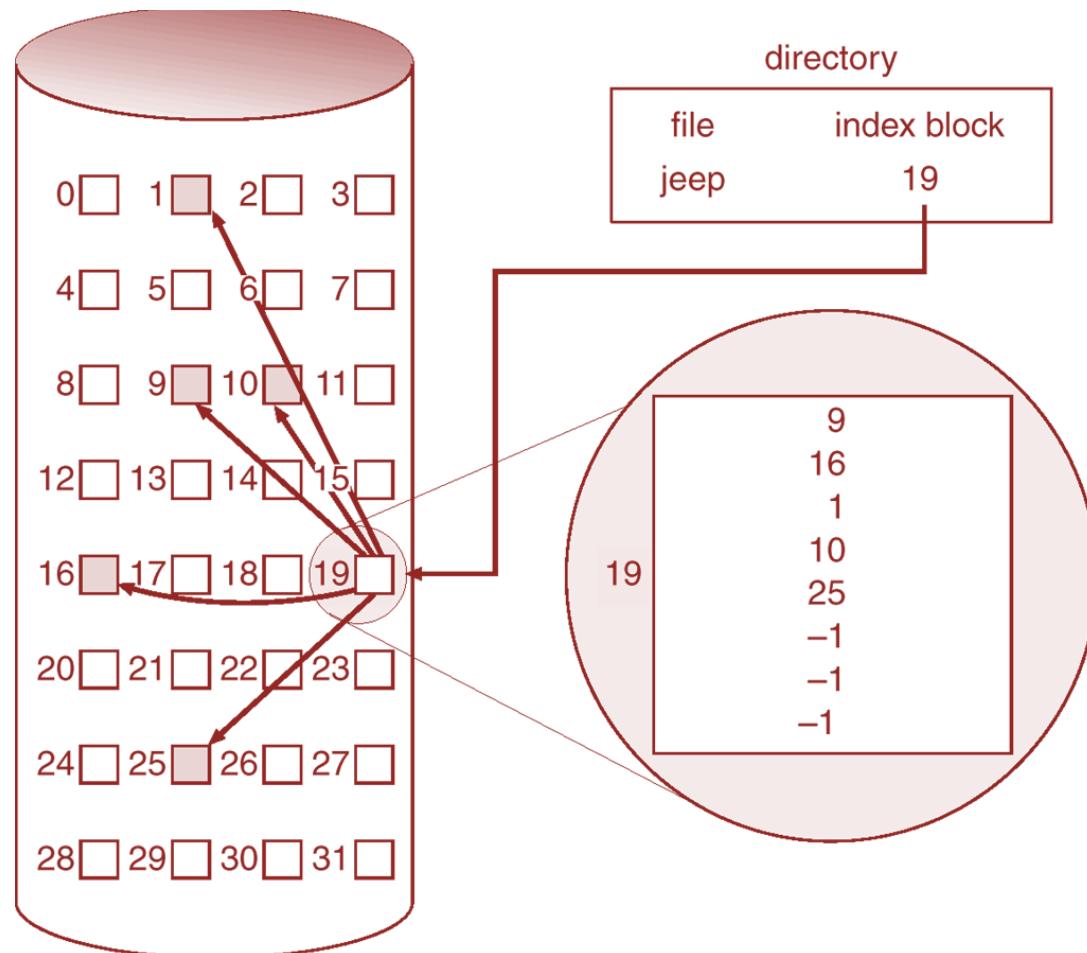


# Allocazione indicizzata

---

- Ogni file ha il proprio blocco indice in cui l’i-esimo elemento (del blocco indice) punta all’i-esimo elemento del file.
- Supporta l’eccesso diretto **senza frammentazione**.
- Comporta un certo **spreco di spazio** per il blocco indice che deve essere della giusta dimensione per consentire di aumentare le dimensioni del file e contemporaneamente non sprecare spazio.

# Allocazione Indicizzata

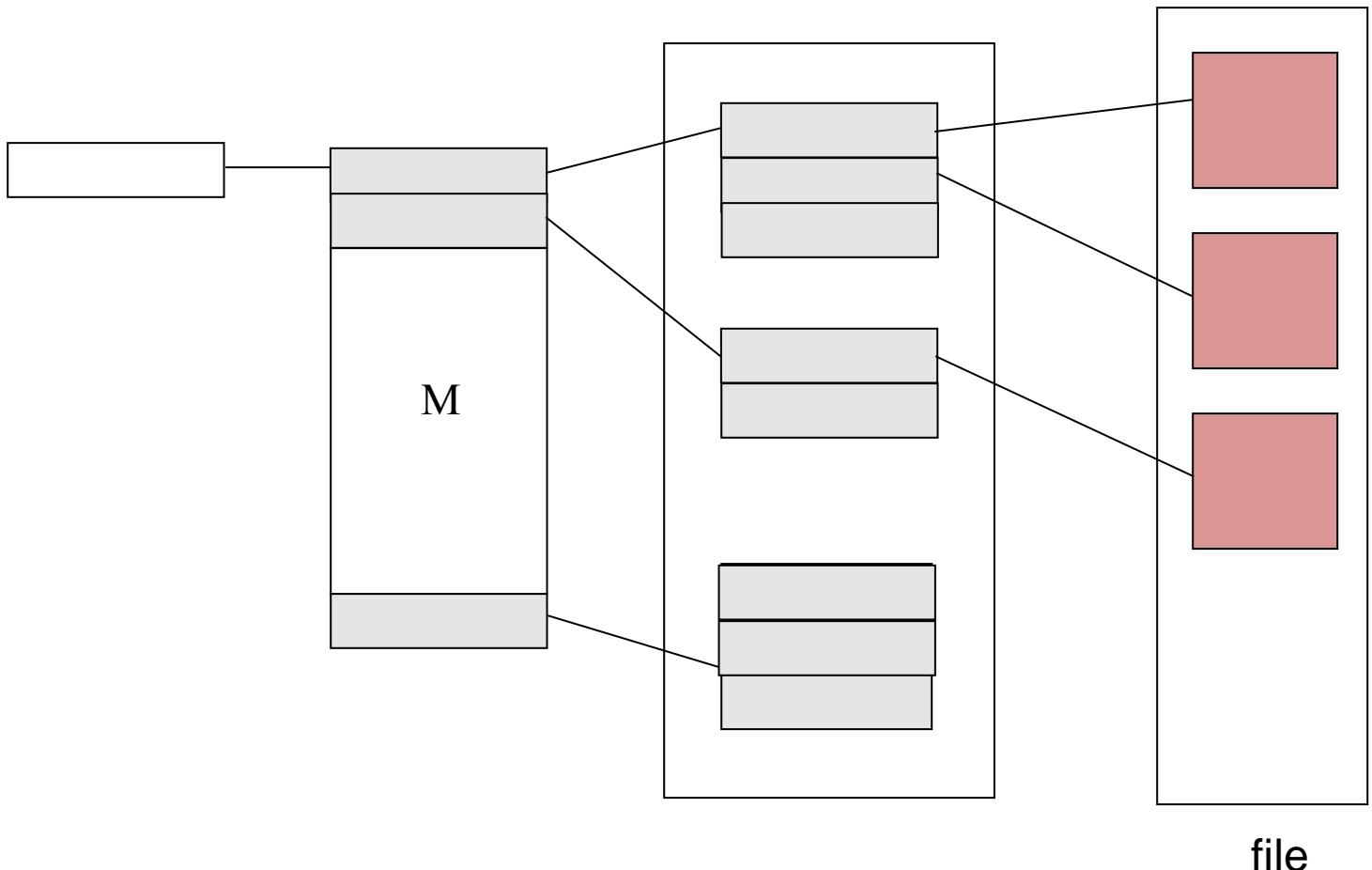


# Allocazione indicizzata

---

- La dimensione e la **memorizzazione** del blocco indice è critica:
  - **Schema concatenato:** il blocco indice occupa esattamente un blocco. Se non è sufficiente un blocco l'ultimo puntatore del blocco indice punta ad un altro blocco indice.
  - **Indice multilivello:** il blocco indice di primo livello punta ad altri blocchi indice di secondo livello e così via
  - **Schema combinato.**

# Multilivello



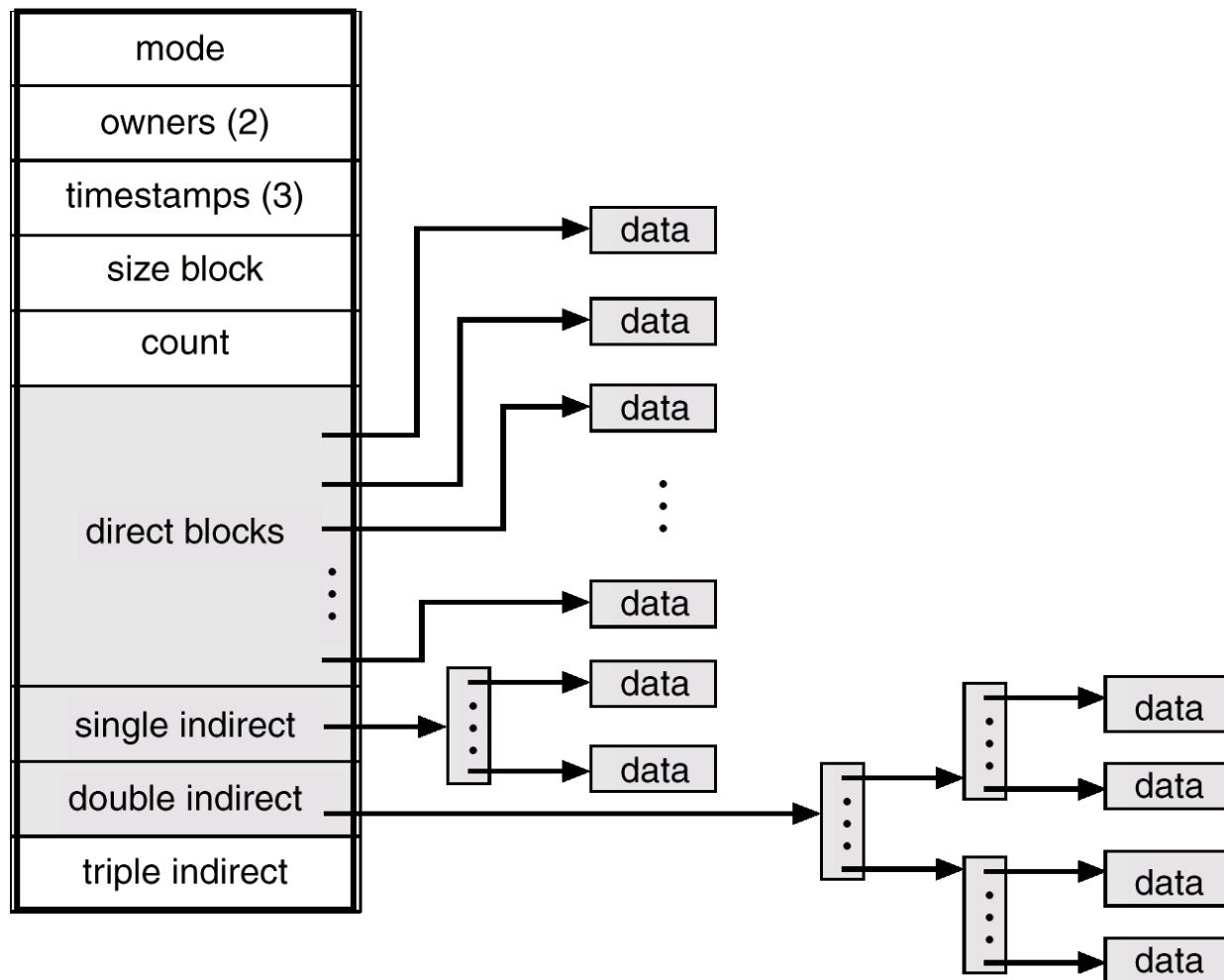
# Allocazione dei Blocchi

## Schema combinato

---

- Usato negli **inode** di alcune versioni di Unix.
- Una parte dei puntatori del blocco indice puntano direttamente ai blocchi del file (**blocchi diretti**).
- Una parte punta invece a indici multilivello (**blocchi indiretti singoli, doppi o tripli**)
- Se il file è piccolo si usano solo i blocchi diretti, più è grande e più indirezioni vengono coinvolte.

# Allocazione dei Blocchi, Schema combinato inode



# Panoramica su architetture per Virtualizzazione di sistemi

---

Prof. Vittorio Ghini

Sistemi Operativi 2021/22

Corso di Laurea in Ingegneria e scienze informatiche

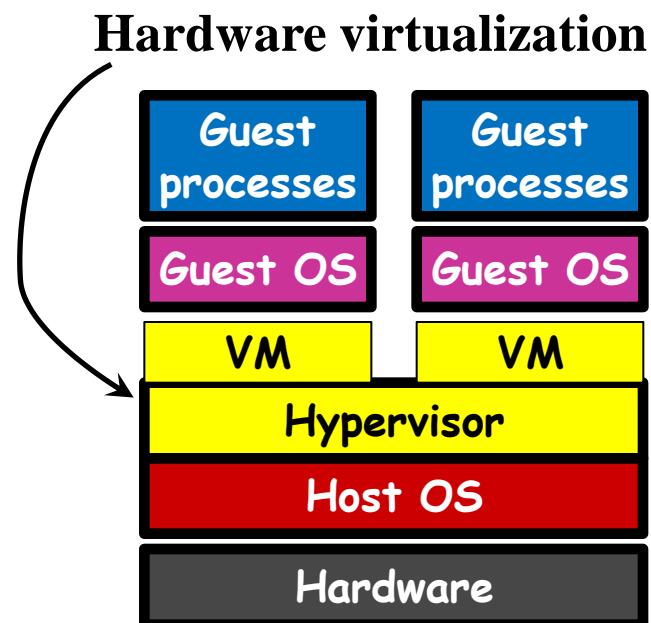
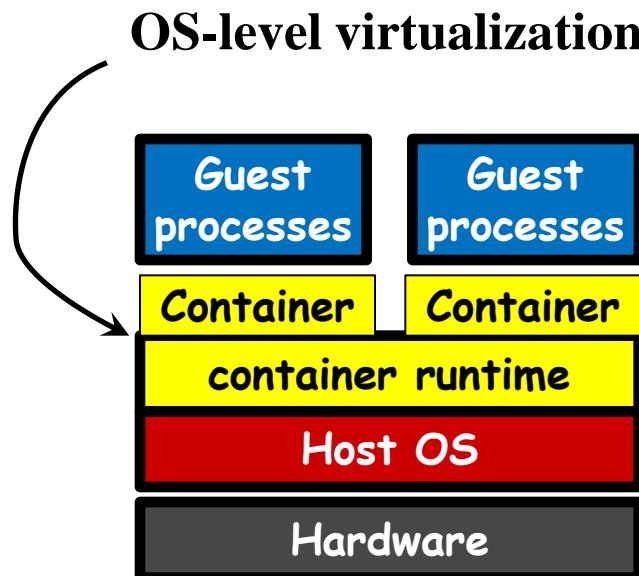
Università di Bologna

# Virtualizzazione vs. Emulazione

- Tramite **virtualizzazione** è possibile eseguire uno o più sistemi operativi (ed il relativo software applicativo) su un unico PC, in un ambiente protetto e monitorato che prende il nome di *macchina virtuale (VM)*.
- Il sistema operativo in cui viene eseguita la macchina virtuale, viene detto *ospitante (host)*
- La macchina virtuale è chiamata *ospite (guest)*.
- Il codice della macchina virtuale viene eseguito direttamente dal sistema ospitante, ma il sistema ospite "pensa" di essere eseguito su una macchina reale.
  - Il codice della macchina virtuale, perciò deve essere codice macchina eseguibile dalla macchina hardware reale sottostante.
  - Non posso virtualizzare un sistema operativo, che dovrebbe girare su un x86 a 64 bit, su un processore ARM.
- **Emulazione di processore.** In questo caso l'hardware viene completamente emulato dal programma di controllo, cioè ogni istruzione che il sistema guest esegue viene tradotta in una sequenza di istruzioni della macchina host. Il processo di emulazione risulta più lento rispetto alle due forme di virtualizzazione precedenti, a causa della traduzione delle istruzioni dal formato del sistema ospite a quello del sistema ospitante.

# Virtualizz. del Livello HW o Livello OS

- La prima grande distinzione riguarda il tipo di risorse virtuali che si vuole presentare all'utente: **macchine virtuali** oppure **partizioni (container) isolate**.
- Nel caso delle **macchine virtuali** (livello Hardware) all'utente del sistema di virtualizzazione viene presentata un'interfaccia su cui installare un sistema operativo, quindi una CPU virtuale (ma dello stesso tipo della CPU fisica) e risorse HW virtuali.
- Nel caso dei **container** (livello OS) all'utente viene presentata una partizione (container) del sistema operativo corrente, su cui installare ed eseguire applicazioni che rimangono isolate nella partizione, pur accedendo ai servizi di uno stesso o.s.



# Livello HW vs. Livello OS(container)

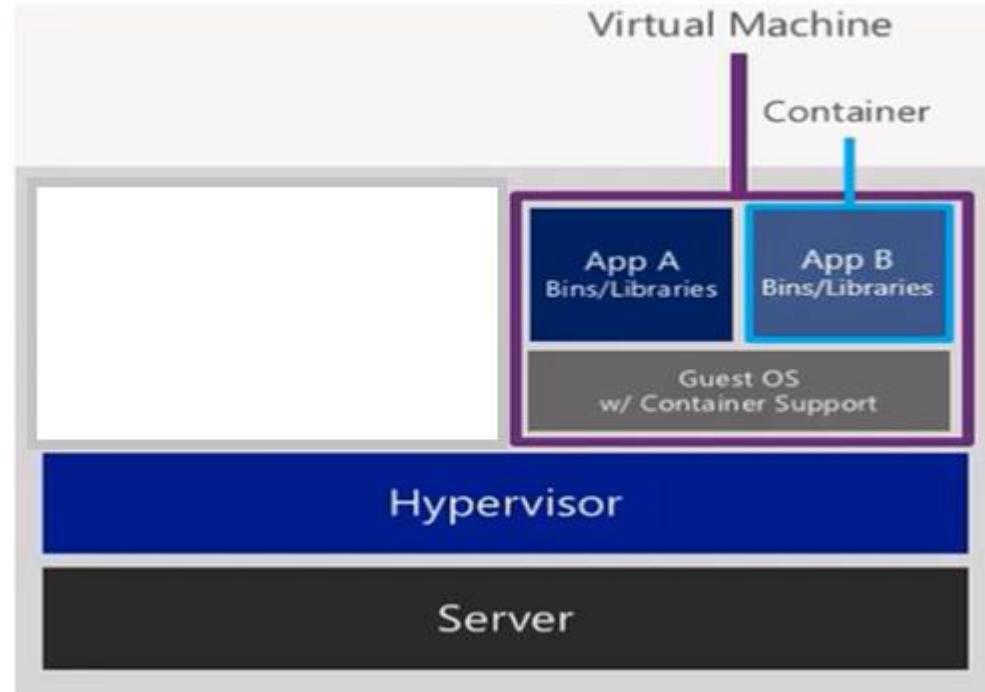
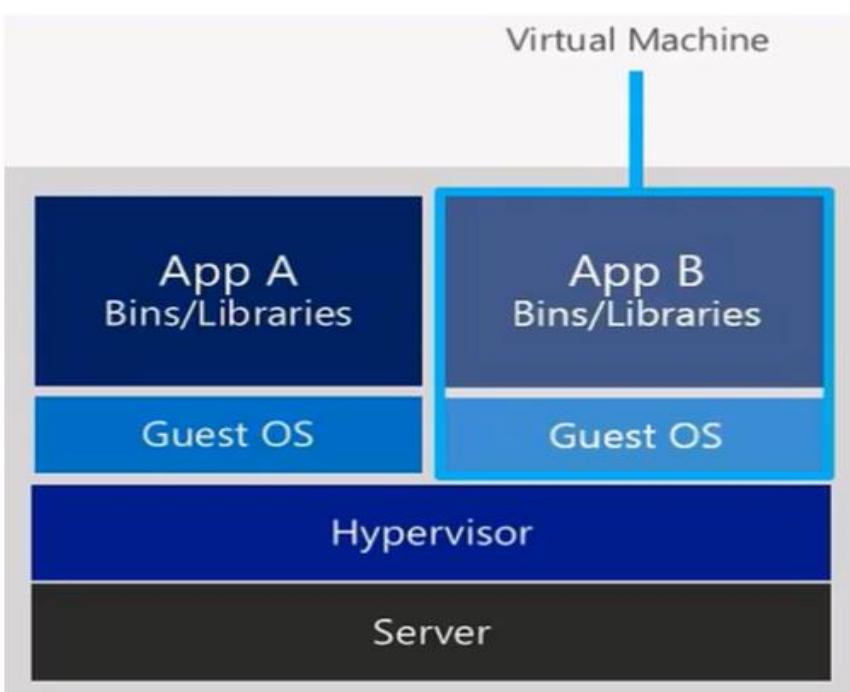
- La virtualizzazione OS-level è composta da un solo kernel (quello del sistema operativo host) e multiple istanze isolate di user-space (chiamate anche partizioni o contenitori), che possono essere avviate e spente in maniera indipendente tra loro. Ogni container contiene un proprio filesystem e proprie interfacce di rete. Viene garantito l'isolamento del filesystem, IPC e network. Inoltre fornisce un sistema di gestione delle risorse quali CPU, memoria, rete e operazioni I/O.
- Nella virtualizzazione hardware, i sistemi operativi eseguono in modo concorrente sullo stesso hardware e possono solitamente essere eterogenei. L'**hypervisor** (chiamato anche *Virtual Machine Monitor*) si occupa di multiplexare l'accesso alle risorse hardware e garantire protezione e isolamento tra le macchine.

Quindi:

- **OS-level (o container-level):** offre contenitori per applicazioni ed esegue un solo kernel, quello del o.s. Host.
  - Vantaggi: basso overhead per il context-switch, basso overhead di memoria
  - Svantaggi: non può ospitare sistemi operativi differenti, l'isolamento non può essere del tutto perfetto
- **hardware-level:** quando offre macchine virtuali.
  - Vantaggi/Svantaggi: speculari rispetto a OS-level

# 2 parole sui Container - perché?

- Creano uno spazio utente isolato, con proprie interfacce di rete, librerie e files, isolando una applicazione dal resto del sistema operativo.
  - **Pacchettizzo una applicazione, rendendola pronta per il deployment.**
- Più container possono appoggiarsi ad uno stesso spazio kernel, risparmiando spazio disco e condividendone i servizi di base.
- Costruito e customizzato un container per una specifica applicazione, posso replicare quel container più volte, anche su una stessa VM o su VM diverse.



# Quali Container ?

Ricordiamo solo i principali:

- **Docker**
  - Si appoggia sul s.o. **Linux** che fornisce, a livello kernel) un supporto per container detto **LXC (Linux Container)**.
    - Non confonete LXC con LXD che è un sistema per dispiegare facilmente virtual machine Linux.
- **Hyper-V** di Microsoft (fornisce unità di isolamento chiamate Container, in realtà sono delle macchine virtuali).
  - Tra l'altro, si parla di container di Hyper-V, ma su sistemi diversi (ad esempio, windows server e windows 10) sono piuttosto differenti, come tipo di isolamento fornito
- **Container di Windows Server** (sono effettivamente dei container)
- NB: E' possibile installare il s.o. Windows server in una configurazione minimale, detto Nano Server, ottimizzato per stare dentro macchine virtuali di hyper-v o per sostenere container di windows server.  
<https://docs.microsoft.com/it-it/windows-server/get-started/getting-started-with-nano-server>

# Docker - Contents

- 0. Immagini di container disponibili su repository docker hub.
- 1. Eseguire un container Docker interattivamente.
- 2. Installare applicazioni in un container docker.
- 3. Salvare i cambiamenti di un container creando una nuova immagine di container.
- 4. Eseguire una immagine di container salvata localmente esponendo all'esterno una porta di protocollo del container.
- 6. Kubernetes
- 7. Kubernetes-as-a-Service.
- 8. Container-as-a-Service
- 9. Functions-as-a-Service.

# 0. Lavorare con le immagini docker

- I container Docker sono eseguiti a partire da immagini di container che possono essere scaricate dal repository Docker Hub, un cosiddetto "registro" di immagini Docker gestito dalla compagnia che sostiene il progetto Docker.
  - Ciascuno può scaricare un'immagine docker ed eseguirla localmente.
  - Dopo che l'immagine del container è stata scaricata, la runtime machine di docker crea il container dall'immagine.
  - La copia dell'immagine scaricata viene salvata su un registro (local registry).
- 
- Per verificare se il sistema docker funziona puoi provare a scaricare l'immagine di test denominata hello-world  
`docker run hello-world`

# 1. Eseguire container docker interattivamente

- **Containers interattivi.** Come esempio eseguiamo un container usando l'ultima immagine disponibile di Ubuntu. La combinazione dei flags `-i` `-t` consente di interagire con una shell bash all'interno del container connessa mediante `stdin/stdout/stderr` alla shell in cui lanciamo il container in foreground:

```
docker run -it --name myubuntu ubuntu
```

- L'opzione `--name myubuntu` assegna il nome `myubuntu` al container. Se non è specificato il nome, docker assegna un nome generato casualmente.
- Your command prompt should change to reflect the fact that you're now working inside the container and should take this form:  
`root@d9b100f2f636:/#`
- Note the container id in the command prompt. In this example, it is `d9b100f2f636`. You'll need that container ID later to identify the container when you want to remove it.

# 1.1. Eseguire interattivamente comandi bash all'interno di un container.

- Ora puoi eseguire dei comandi all'interno del container myubuntu.
- Per esempio esegui il comando ls
  - ls
- Poi edita un file
  - echo ciao > miofile.txt
- E verifica l'esistenza del file nel container
  - cat myfile.txt
- Ogni cambiamento apportato al filesystem del container rimane confinato al filesystem del container.
- Per terminare il container, digita exit al prompt dentro il container. La shell termina e con esso termina il container.
- Se fai partire nuovamente il container dall'immagine ubuntu, il file precedentemente creato non c'è più nel nuovo container.
- Prova ancora "docker run -it --name myubuntu1 ubuntu" e verifica che il file myfile.txt non c'è.

## 2. Installare applicazioni in container

```
docker run -it --name myubuntu ubuntu
```

- Installare il pacchetto node.js e alcune altre utility:

```
apt update
```

```
apt install vi wget curl
```

```
apt install nodejs
```

- Configura il server http dinamico editando il file /root/index.js

```
var http = require('http');
http.createServer(function (request, response) {
    response.writeHead(200, {'Content-Type': 'text/plain'});
    response.end('ciao a tutti\n');
}).listen(8888);
console.log('Server running at http://127.0.0.1:8888/');
```

- Fai partire il server nodejs

```
node index.js &
```

- Testa il funzionamento del server nodejs dall'interno del container

```
curl http://127.0.0.1:8888/
```

# 3. Salvare i cambiamenti creando una nuova immagine del container in locale

- Dopo avere eseguito un container interattivamente, battezzandolo myubuntu, e dopo averne modificato il filesystem, installando il server http dinamico nodejs,
- termine l'esecuzione del container
- e poi ne salvo l'immagine in locale chiamando la nuova immagine di container ubuntuVic

```
docker commit -m "added node.js" -a "Vic" myubuntu vic/ubuntuvic
```

- Ora localmente ho la nuova immagine del mio container e posso eseguire dei container partendo da questa immagine. Nei container creati mi ritrovo installato il mio server nodejs e le utility vi e wget

```
docker run -it --name myubuntu vic/ubuntuvic
```

- Prova dentro il container a far partire il server web e ad usarlo con curl  
node index.js &  
curl http://127.0.0.1:8888/

# 4. Eseguire un container in background esponendo una porta all'esterno del container

```
docker run -it -d --rm -p 80:8888 --name myubuntu2 vic/ubuntuic node index.js
```

i parametri hanno i seguenti scopi:

vic/ubuntuic è l'immagine del container.

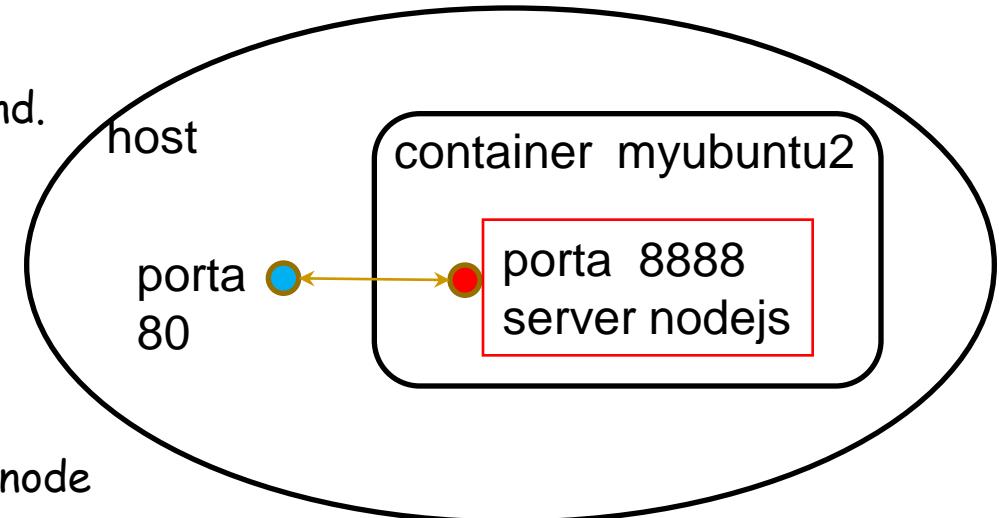
-d significa esegui il container in background.

--rm elimina il container quando termina.

-p 80:8888 collega la porta 80 dell'host alla porta 8888 interna del container.

node è il comando da lanciare non appena il container viene creato e parte.

index.js è l'argomento passato al comando node da eseguire quando il container parte.



Verificare: stando nella macchina in cui si esegue il container, e quindi FUORI dal container, eseguire

```
curl http://127.0.0.1:80/
```

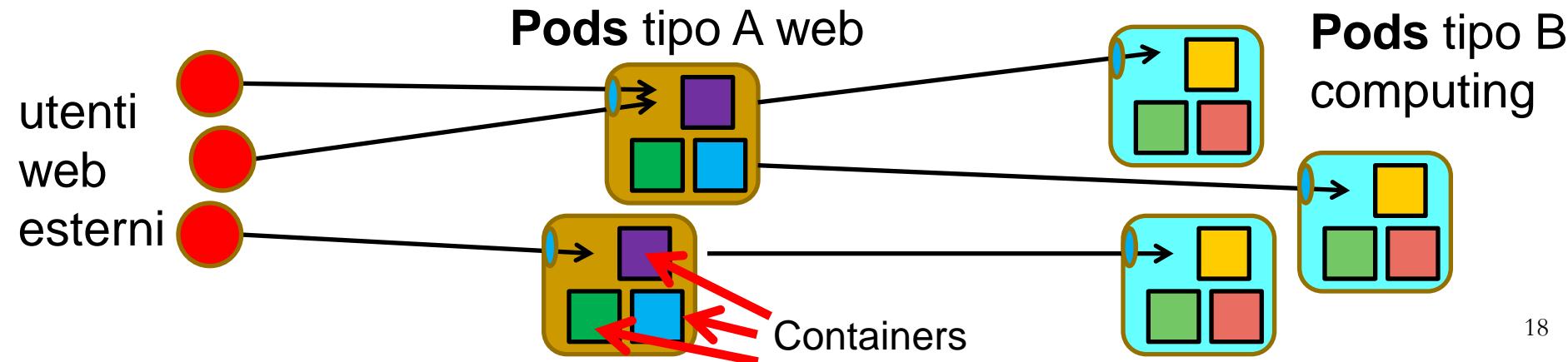
per accedere al servizio fornito dal container stando FUORI dal container.

## 6. Orchestrazione di container con KUBERNETES

fornire automaticamente  
scalabilità e resilienza  
ad applicazioni  
basate su container docker  
in esecuzione su cluster  
di host fisici o virtuali

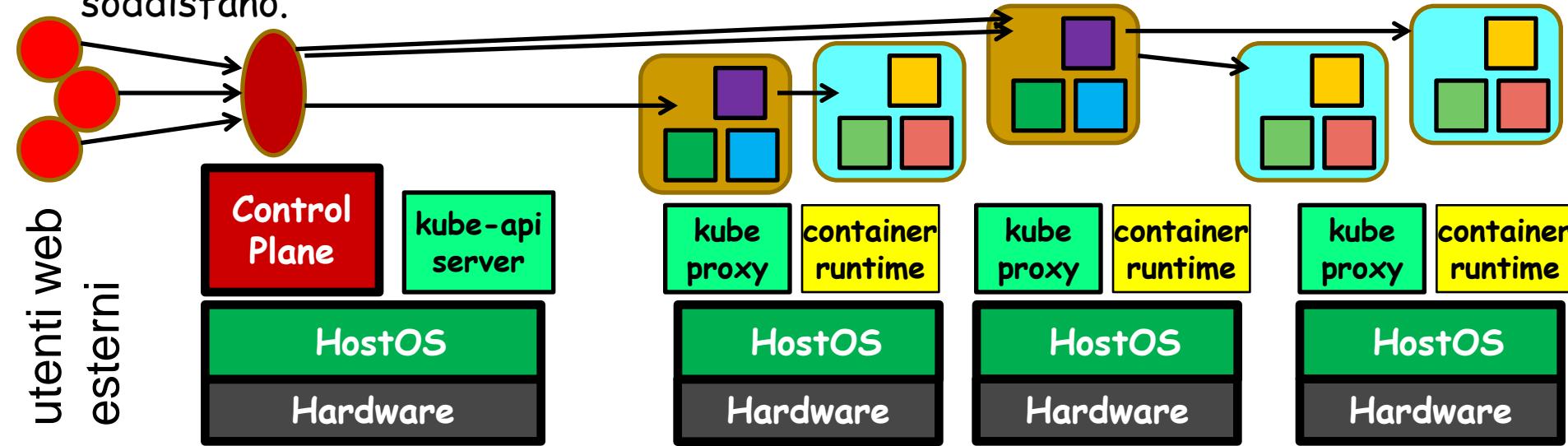
# 6.1 Applicazioni per kubernetes

- Le applicazioni progettate per kubernetes sono costituite da più **pods**.
- Ciascun pods è un insieme di container che cooperano e comunicano tra loro come se si trovassero in un unico host fisico e svolgono nel complesso un certo servizio, ad esempio un **pod può realizzare un servizio web** mentre un altro **pod può eseguire una serie di calcoli**, oppure può salvare dati in un database.
- Un **pod può essere replicato in più istanze** se occorre eseguire in parallelo le stesse operazioni e distribuire il carico. Le diverse istanze dei pods possono eseguire su uno stesso host oppure su host diversi per distribuire meglio il carico.
- Ciascun pods può esporre delle porte di protocollo per ricevere comunicazioni da container di altri pods.
- In tal modo, uno dei pod di tipo A, che espone il servizio web, riceve le richieste dagli utenti web esterni, poi chiede ad uno dei pod di tipo B di effettuare un calcolo, ricevuto il risultato del calcolo lo restituisce all'utente web esterno.



## 6.2 Cluster kubernetes - replicare pods su host diversi per distribuire carico

- Kubernetes organizza degli host (**nodi del cluster**) fisici o virtuali per poter eseguire e replicare i pods sui nodi, distribuendo così il carico dell'applicazione.
- L'applicazione decide quanti pods utilizzare e kubernetes decide automaticamente su quali nodi allocare i pods.
- Uno degli host svolge il ruolo di controllore del cluster (control plane), monitora gli altri host del cluster, decide automaticamente in quali nodi eseguire i pods e svolge il ruolo di punto di accesso al cluster dall'esterno. Gli altri host (nodi worker) eseguono i pods della o delle applicazioni.
- Gli utenti web esterni vedono solo il nodo controllore gli inviano le richieste.
- Il nodo controllore instrada le richieste ricevute ai pods dei nodi worker, che le soddisfano.



## 6.3 Cluster kubernetes - gestione resilienza

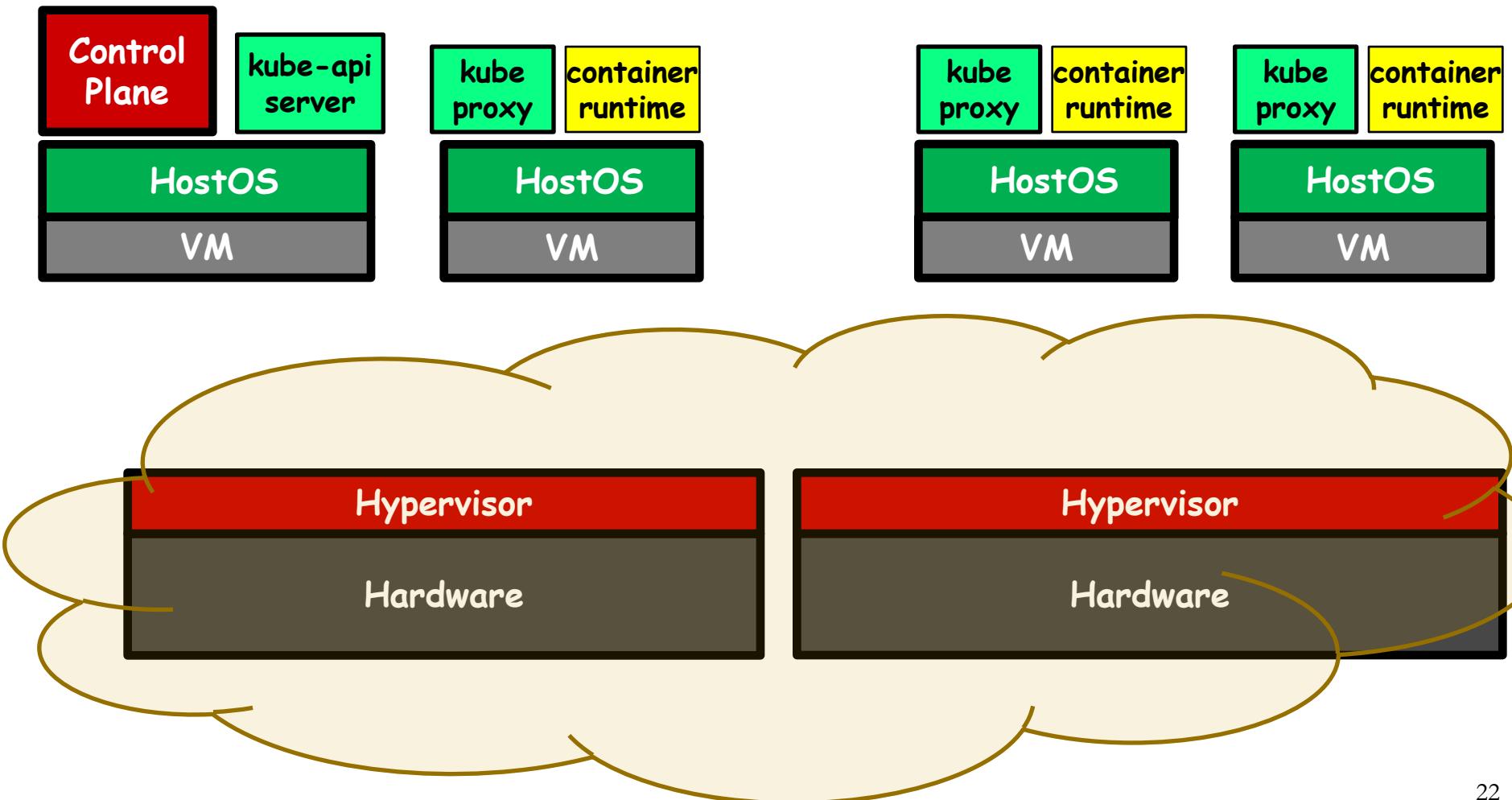
- Se un pod va in crash kubernetes ne crea immediatamente una nuova istanza.

## 6.4 Cluster kubernetes - gestione scalabilità

- L'applicazione decide quanti pods utilizzare e kubernetes decide automaticamente su quali nodi allocare i pods.
- L'applicazione può configurare Kubernetes affiche questo, all'aumentare del carico dell'applicazione, effettui 3 tipi di operazioni:
  - **autoscaling verticale**: aumenti le risorse a disposizione di un pod (uso della CPU, quantità di memoria usata).
  - **autoscaling orizzontale**: aumenti il numero delle repliche dei pods applicativi.
  - **cluster autoscaling**: aumenti il numero dei nodi che compongono il cluster redistribuendo i pods.
- Ciò consente di scalare aumentando o diminuendo il numero dei pods e/o dei nodi al crescere o al calare delle esigenze applicative.
- Ciò consente anche di mantenere l'applicazione in funzione anche se qualche host si guasta poiché ne rimangono altri a disposizione.
- La possibilità di realizzare il **cluster autoscaling** dipende da quali host usiamo:
- Per host fisici occorre un sistema di accensione degli host fisici guidabile via software (wake on lan o ...) mentre per gli host virtuali occorre un supporto, da parte del cloud pubblico o privato che ci fornisce le macchine virtuali, che ci dia la possibilità di creare e configurare nuove VM in automatico via software.

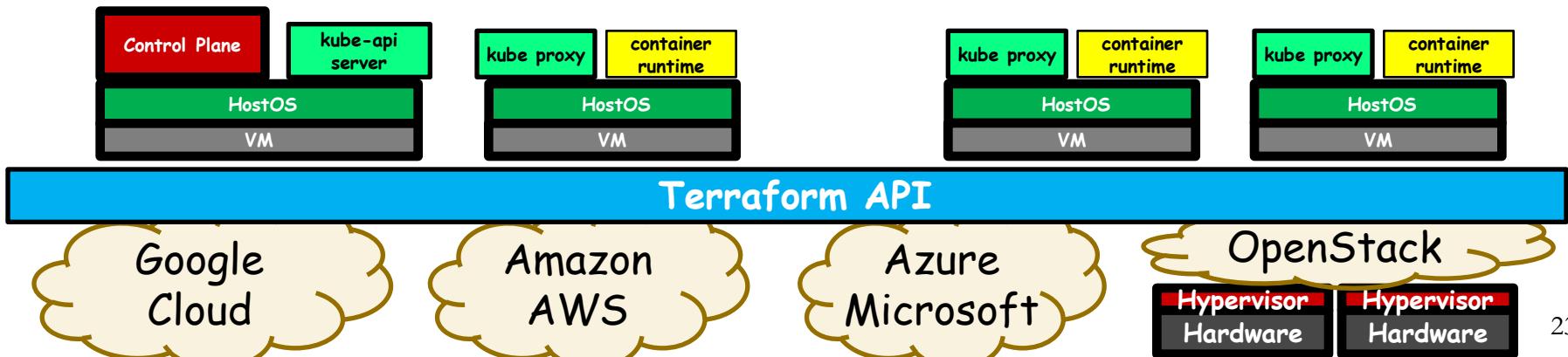
## 6.5 Cluster kubernetes con nodi virtuali

- E' possibile creare un cluster kubernetes formato da host che siano macchine virtuali. Questi macchine virtuali possono essere create manualmente su host fisici oppure possono essere create via software su cloud pubblici o privati.



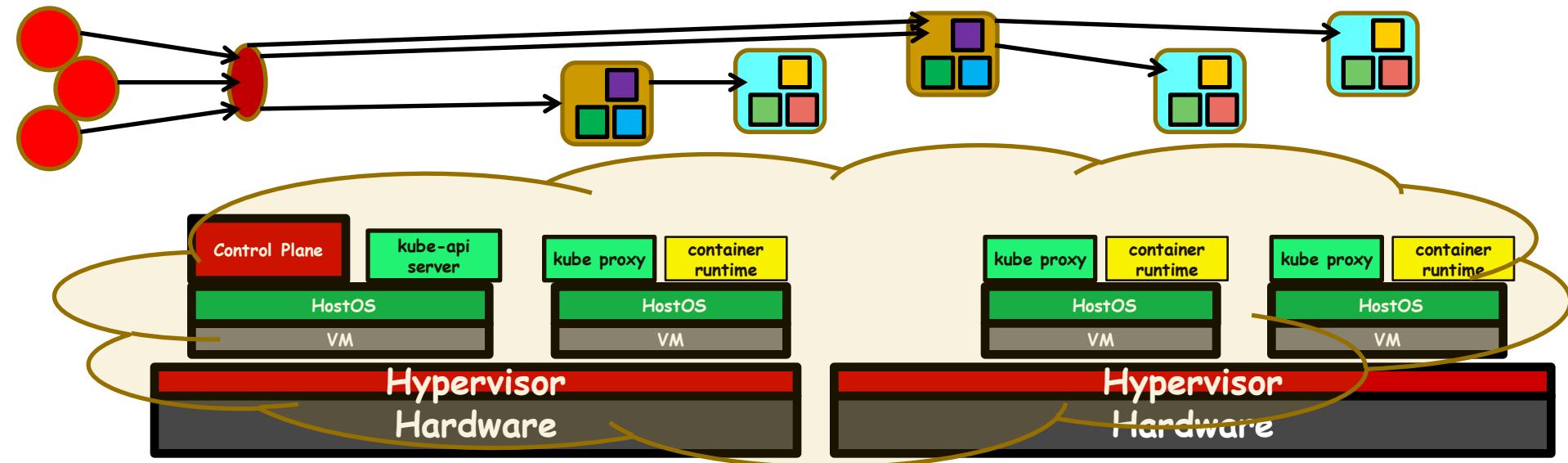
## 6.5.1 Cluster kubernetes con nodi virtuali

- Esistono cloud di diversi provider, i principali sono Google Cloud, Azure di Microsoft, AWS di Amazon, I.
- E' anche possibile costruire un cloud privato, partendo da macchine fisiche in una propria sala macchine, gestendo le proprie macchine con un insieme di applicativi open source basati su Ubuntu, noto col nome di **Openstack**.
- I sistemi cloud forniscono delle API mediante le quali possiamo ordinare, ,per via software, la creazione e la configurazione di VM e di reti virtuali tra le VM.
  - Purtroppo le API differiscono da cloud a cloud.
- Fortunatamente, alcuni software (ad esempio **Terraform**) offrono uno strato software che astrae dai sistemi cloud sottostanti ed offre un insieme di API utilizzabile su tutti i sistemi cloud per creare e configurare le VM.
- In tal modo è possibile creare un cluster kubernetes formato da host virtuali ed applicare il cluster autoscaling configurando kubernetes affinché usi Terraform per creare nuove macchine virtuali quando necessario per scalare.



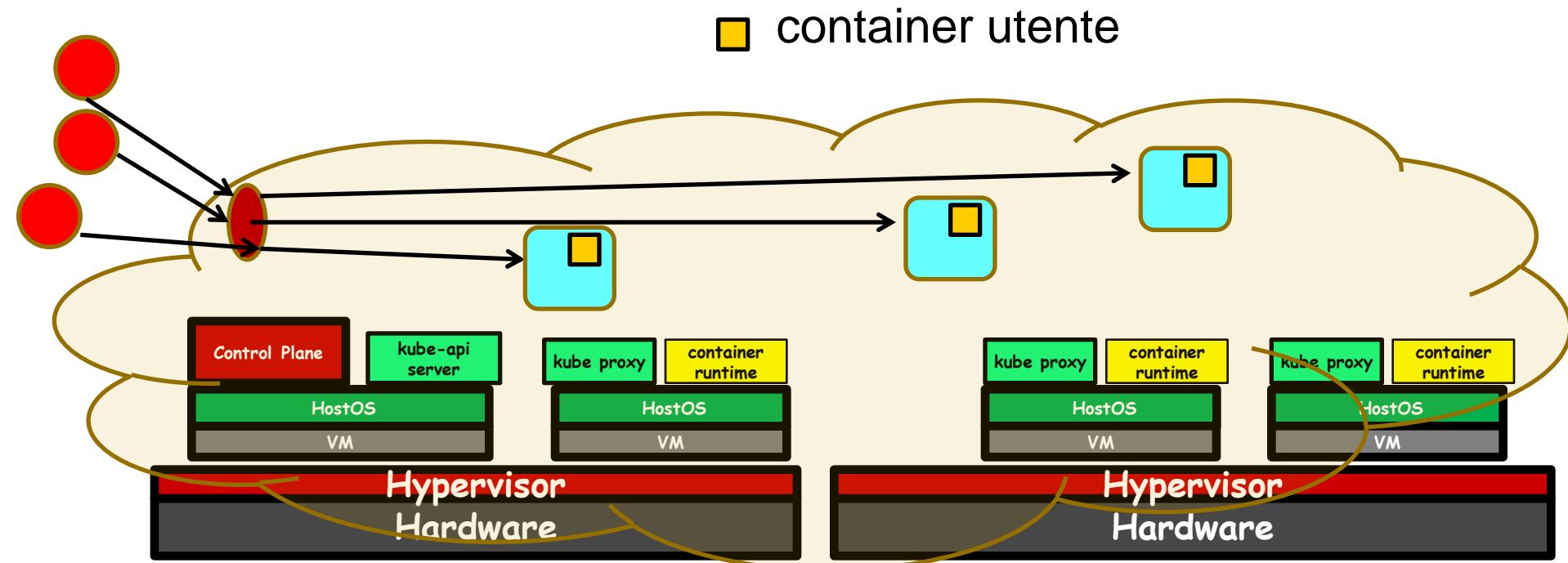
# 7. Kubernetes-as-a-Service

- Alcuni sistemi cloud offrono un servizio kubernetes senza che sia necessario creare esplicitamente il cluster kubernetes.
- Il cluster viene creato ed installato dal provider cloud su richiesta via software e a chi produce l'applicazione vengono fornite delle API mediante le quali chiedere di inizializzare il cluster kubernetes e di disegnarvi sopra l'applicazione organizzata per kubernetes.
- Si installa una applicazione per kubernetes facendo costruire il cluster kubernetes al provider cloud.
- In tal modo è possibile costruire applicazioni scalabili e resistenti in maniera più semplice pagando al provider cloud il costo (non piccolo) del cluster.



# 8. Container-as-a-Service

- Alcuni sistemi cloud, in particolare offrono la possibilità di:
- far eseguire un container, la cui immagine è fornita dallo sviluppatore dell'applicazione, in molteplici istanze su un cluster kubernetes-as-a-service costruito nascostamente dal provider stesso.
- Il container viene encapsulato in un pod predisposto dal provider cloud ed eseguito nel cluster kubernetes. In tal modo lo sviluppatore non si deve occupare di gestire il cluster ma solo di costruire il container da far eseguire.
- Questo approccio è fornito da: Google Container Engine (GKE), Amazon EC2 Container Service (ECS), Azure Container Service (ACS), IONOS Container Cluster.



## 9. Serverless o Function-as-a-Service (FaaS)

- Alcuni provider cloud astraggono ulteriormente e offrono un servizio che consente di implementare delle funzioni che vengono eseguite, anche in più istanze contemporaneamente apparentemente senza definire né container né macchine virtuali e nemmeno cluster kubernetes su cui tali funzioni vengono eseguite.
- Quello che accade è che il provider cloud "probabilmente" incorpora la funzione definita dall'utente in un container e lo esegue su un cluster kubernetes replicandolo man mano che aumenta il carico di richieste da servire.
- Per l'utente è facile creare queste funzioni ed il problema della creazione del contesto di esecuzione (container e pod) è risolto, ovviamente dietro pagamento, dal provider cloud.
- Il provider offre alcune funzioni di libreria, lo sviluppatore implementa diverse altre funzioni, ciascuna delle quali può utilizzare, chiamandole, altre funzioni dello sviluppatore o di libreria, in modo da poter implementare così anche funzionalità complesse.
- Troviamo questo approccio nei principali provider cloud: **AWS Lambda** in Amazon AWS, **Azure Functions** in Microsoft Azure e **Cloud Functions** in Google Cloud.

# L' ENTRY POINT DI UN ESEGUIBILE E IL LINKING CON LIBRERIE DI DEFAULT. CHIAMATA AD INTERRUPT SOFTWARE E CHIAMATA A SYSTEM CALLS.

Prof. Vittorio Ghini, Appunti delle lezioni di Sistemi Operativi,  
Corso di Laurea in Ingegneria e Scienze Informatiche, Università di Bologna

## 0. IL FORMATO DEL MODULO OGGETTO E DELL'ESEGUIBILE E IL PROCESSORE SU CUI PUO' ESEGUIRE.

Usando il comando 'objdump -f nomeeseguibile.exe' oppure 'objdump nomefileoggetto.o' posso vedere il formato dell'eseguibile e il processore per cui è stato creato.

Con il comando 'ld -V' mi faccio dire dal linker quali formati di eseguibile è in grado di creare.

## 1. INIZIO ESECUZIONE DI UN ESEGUIBILE

Quando io lancio l'eseguibile per farlo eseguire, il loader crea il processo (riempiendo tutte le necessarie tabelle di sistema) e carica in memoria l'immagine del processo, poi passa il controllo al processo caricato e ne fa eseguire la prima istruzione macchina. Nell'eseguibile, il formato **ELF** prevede una sezione header in cui e' contenuto un campo "**Entry point address**" il cui valore e' l'**indirizzo in cui si trovera' l'istruzione iniziale da eseguire dopo che il processo sara' stato caricato in memoria dal loader**.

Si può lanciare il comando `readelf -h nomefileeseguibile` per vedere questo campo.

Nel codice assembly, **la prima istruzione macchina da eseguire è etichettata con la label \_start**, che ne rappresenta l'indirizzo.

**Quando il linker genera l'eseguibile**, cerca l'istruzione etichettata con **\_start** e ne pone l'indirizzo nel campo "**Entry point address**" della sezione header.

Se il linker non trova questa label, produce un errore e non genera l'eseguibile.

## 2. LINKING PER CREAZIONE di ESEGUIBILE scritto in LINGUAGGIO C CON gcc

- Quando io scrivo un programma codice in C, il punto di inizio del mio codice e' la funzione main.
- Ma **la prima istruzione che viene eseguita** su ordine del loader, dopo il caricamento in memoria del programma, **non e' quella del main**.

Infatti, prima di poter cominciare ad eseguire il codice del main, occorre svolgere alcune operazioni preliminari, atte a garantire il successivo corretto funzionamento della libc (la libreria standard del C), quali ad esempio impostare il vettore degli interrupt per il processo, inizializzare parte dello stack e altre ancora.

Queste operazioni non sono implementate all'interno del main ma vengono svolte da codice aggiunto autonomamente dal gcc quando effettua l'operazione di linking di moduli scritti in linguaggio C.

Questo codice aggiunto autonomamente dal gcc durante il linking fa parte delle librerie standard del C ed e' "stranamente" contenuto in dei moduli oggetto, ad esempio

```
/usr/lib/x86_64-linux-gnu/crt1.o  
/usr/lib/gcc/x86_64-linux-gnu/5/crtbegin.o  
/usr/lib/gcc/x86_64-linux-gnu/5/crtend.o
```

- E' dentro questo codice macchina, aggiunto dal gcc al momento del linking, che si trova l'istruzione macchina iniziale etichettata con \_start.

## Entry point in eseguibile scritto in C e linkato con gcc

ELF Header	OS/ABI: UNIX - System V ABI Version: 0 Type: EXEC (Executable file) Machine: Advanced Micro Devices X86-64 Version: 0x1 <b>Entry point address: 0x4000b0</b>
crt1.o	<pre>.text: 0x000000: xor %ebp,%ebp 0x000008: 0x0400b0 &lt;_start&gt; : mov %rsp,%rdx 0x0400b9: 0x0400d2: call main 0x0200da: mov \$0x1,%eax 0x0200d6: int \$0x80</pre>
print_usa_main.o	<pre>.text: 0x0500b0 &lt;main&gt; : movl \$4, %eax 0x0500bf: ... 0x0500c2: &lt;fine&gt; : mov \$0x1,%eax 0x0500ca: retq</pre>

eseguibile binario print\_usa\_main.exe

Solo dopo avere eseguito il codice aggiunto che inizia in `_start` il codice stesso passerà il controllo al `main` effettuando un salto al codice di inizio del `main` stesso.

### Core OS C Runtime Objects (CRT)

The `crt1.o`, `crti.o`, and `crtn.o` objects comprise the core CRT (C RunTime) objects required to enable basic C programs to start and run. CRT objects are typically added by compiler drivers when building executables and shared objects.

`crt1.o` provides the `_start` symbol that the runtime linker, `ld.so.1`, jumps to in order to pass control to the executable, and is responsible for providing ABI mandated symbols and other process initialization, for calling `main()`, and ultimately, `exit()`. `crti.o` and `crtn.o` provide prologue and epilogue `.init` and `.fini` sections to encapsulate ELF init and fini code.

`crt1.o` is only used when building executables. `crti.o` and `crtn.o` are used by executables and shared objects.

These CRT objects are compatible with position independent (PIC), and position dependent (non-PIC) code, including both normal and position independent executables (PIE).

**Nota bene:** il gcc, quando deve eseguire il linking, in realtà lancia `ld` passandogli alcuni argomenti che indicano quale codice aggiungere e altre informazioni.

Ad esempio, in un sistema Linux su processore x64 o amd, se voglio linkare il mio modulo `print_usa_main.o` il gcc lancia il linker `ld` e gli passa i seguenti argomenti:

```
/usr/bin/ld      -plugin    /usr/lib/gcc/x86_64-linux-gnu/5/liblto_plugin.so      -plugin-
                  opt=/usr/lib/gcc/x86_64-linux-gnu/5/lto-wrapper               -plugin-opt=
```

```
fresolution=/tmp/cc7yRp5X.res      -plugin-opt=-pass-through=-lgcc -plugin-opt=-pass-
through=-lgcc_s -plugin-opt=-pass-through=-lc -plugin-opt=-pass-through=-lgcc -plugin-
opt=-pass-through=-lgcc_s --sysroot=/ --build-id --eh-frame-hdr -m elf_x86_64 --hash-
style=gnu --as-needed -dynamic-linker /lib64/ld-linux-x86-64.so.2 -z relro -o
print_usa_main.exe /usr/lib/gcc/x86_64-linux-gnu/5/../../x86_64-linux-gnu/crt1.o
/usr/lib/gcc/x86_64-linux-gnu/5/x86_64-linux-gnu/crti.o
/usr/lib/gcc/x86_64-linux-gnu/5/crtbegin.o      -L/usr/lib/gcc/x86_64-linux-gnu/5 -
L/usr/lib/gcc/x86_64-linux-gnu/5/../../x86_64-linux-gnu -L/usr/lib/gcc/x86_64-linux-
gnu/5/../../lib -L/lib/x86_64-linux-gnu -L/lib/../lib -L/usr/lib/x86_64-linux-gnu -
L/usr/lib/../lib -L/usr/lib/gcc/x86_64-linux-gnu/5/.../.. print_usa_main.o -lgcc --as-
needed -lgcc_s --no-as-needed -lc -lgcc --as-needed -lgcc_s --no-as-needed
/usr/lib/gcc/x86_64-linux-gnu/5/crtend.o          /usr/lib/gcc/x86_64-linux-
gnu/5/.../x86_64-linux-gnu/crtn.o
```

Se guardate li' in mezzo, vedete elencati anche i moduli standard aggiunti dal gcc che vi ho citato prima.

### 3. LINKING PER CREAZIONE di ESEGUIBILE scritto in ASSEMBLY CON Id

Se invece io scrivo in assembly il codice del mio modulo principale, sono io che devo indicare quale e' la istruzione iniziale etichettata con `_start` che deve essere eseguita per prima. Sono io che scrivo tutto cio' che deve essere fatto dall'inizio, **il linker non aggiunge niente**.

Nel mio codice assembly quindi **esiste la istruzione iniziale** ed e' indicata dalla etichetta/indirizzo `_start`.

Se scrivo codice assembly, allora per linkare il mio codice macchina devo usare il linker **Id** (usato anche dal gcc stesso) che costruisce l'eseguibile usando il mio codice macchina ma non aggiunge altro codice in autonomia.

Ad esempio, per linkare il mio modulo assembly `print.o` lancero' il linker Id con questi parametri:

```
Id -o print.exe print.o
```

## Entry point in eseguibile scritto in assembly e linkato con ld

ELF Header	OS/ABI: UNIX - System V ABI Version: 0 Type: EXEC (Executable file) Machine: Advanced Micro Devices X86-64 Version: 0x1 <b>Entry point address: 0x4000b0</b>	eseguibile binario print.exe
print.o	.text: <b>0x0400b0 &lt;_start&gt;</b> : mov %rsp,%rdx 0x0400b9: movl \$4, %eax 0x0400d2: ... 0x0400d2: ... 0x0200e0: mov \$0x1,%eax 0x0200d6: int \$0x80	

### 4. PROBLEMA nel LINKING con gcc PER CREAZIONE di ESEGUIBILE scritto in ASSEMBLY

Se invece io scrivo in assembly il codice del mio modulo principale, indicando l'istruzione iniziale etichettata con `_start` e poi linko il mio modulo oggetto chiamando il gcc senza parametri speciali, **il gcc normalmente aggiunge dei moduli aggiuntivi che contengono essi stessi una istruzione iniziale etichettata con `_start`.**

- In tal modo, **durante il linking saranno presenti due istruzioni etichettate con `_start` ed il linker non sa quale usare come istruzione iniziale da far eseguire.**  
Percio' il linker provoca un errore e non genera l'eseguibile.  
**L'errore viene indicato cosi': "multiple definition of `\_\_start'"**

Inoltre, **nel codice aggiunto dal gcc c'e' un salto alla istruzione del main, ma nel mio codice assembly non ho messo una label main, perche' sono partito da `_start`.**

- Quindi **il linker non riesce a trovare una etichetta main e perci' non riesce a risolvere il simbolo main che manca.**  
Il linker quindi provoca un altro errore e non genera l'eseguibile.  
**L'errore viene indicato cosi': "In function `\_\_start': undefined reference to `main'"**

## **4. SOLUZIONI del PROBLEMA nel LINKING con gcc PER CREAZIONE di ESEGUIBILE scritto in ASSEMBLY**

Esistono due modi diversi per risolvere il problema che impedirebbe di linkare con gcc dei moduli scritti in assembly.

### **4.1 MODO 1 - LINKING con gcc, SENZA LIBRERIE STANDARD, di ESEGUIBILE scritto in ASSEMBLY**

Ordino al gcc di fare il linking SENZA USARE LE SUE LIBRERIE STANDARD, che tanto non mi servono perche' io uso solo istruzioni assembly.

Per fare cio' AGGIUNGO NEL COMANDO DI LINKING ordinato al gcc il flag **-nostdlib** che ordina di non usare le librerie standard del C.

```
gcc -nostdlib -o print.exe print.o
```

In tal modo il gcc non aggiunge i moduli aggiuntivi iniziali e quindi non aggiunge l'istruzione etichettata con \_start e nemmeno aggiunge il salto verso l'etichetta main.

#### **Risolto.**

Nasce il problema che non posso usare le librerie standard del C all'interno del mio codice assembly.

### **4.2 MODO 2 - LINKING con gcc, CON LIBRERIE STANDARD, di ESEGUIBILE scritto in ASSEMBLY**

Modifico il mio codice assembly NON FACENDOGLI FARE la parte iniziale di esecuzione. Cioè faccio partire il mio codice assembly non da \_start bensì' da main, come se fosse un programma scritto in C.

In pratica, nel mio codice assembly principale, al posto delle due righe di codice seguenti:

```
.globl _start  
_start:
```

devo sostituire le due righe seguenti:

```
.globl main
```

```
main:
```

Poi assemblero' il sorgente assembly con l'assemblatore as o col gcc

```
as -o print.o --gstabs print.s # assemblaggio diretto con as
```

```
oppure con
```

```
gcc -c -g -o print.o print.s # assemblaggio tramite gcc che chiama as
```

A questo punto posso usare il gcc per linkare normalmente senza dover chiedere di escludere le librerie di default.

```
gcc -o print.exe print.o
```

Infatti, in questo modo, il gcc linker aggiunge il suo codice macchina (che parte da \_start e che poi salta al main) e trova nel modulo oggetto originato dall'assembly il simbolo main che indica da dove far partire il codice utente.

In questo modo, nel mio eseguibile mi ritrovo anche le librerie standard e quindi, volendo, potrei richiamare da assembly anche le funzioni C presenti nelle librerie standard, purché sia io da assembly a preparare correttamente lo stack per la chiamata a funzione C, come farebbe il compilatore, e analogamente a recuperare il risultato e ripulire lo stack dopo la fine della chiamata a funzione.

## 5. CHIAMATA AD INTERRUPT SOFTWARE

Un programma in assembly, che opera su un processore Intel, può invocare l'esecuzione di un interrupt software chiamando l'istruzione ' int' e passandole come argomento un numero che identifica l'interrupt software da eseguire. Ad esempio la seguente istruzione invoca l'interrupt numero 8016 (80 in esadecimale).

**int \$0x80**

La routine di gestione di quell'interrupt può essere quella originariamente contenuta nel BIOS della CPU oppure può essere stata sostituita, dopo il boot, da una diversa routine di gestione stabilita e implementata dal sistema operativo.

Solitamente, se il programma assembly deve passare dei parametri ad un interrupt, i parametri vengono messi in alcuni registri PRIMA di chiamare l'interrupt, e poi la routine di gestione dell'interrupt controlla il contenuto di quei registri e agisce di conseguenza. Ad esempio, nel seguente codice, prima di chiamare l'interrupt 0x80 viene collocato il valore 1 nel registro eax e questo dice all'interrupt che deve eseguire un particolare servizio, cioè la terminazione del processo stesso.

```
movl $1, %eax           /* servizio da ottenere: terminazione processo */
int $0x80               /* ordine di eseguire l'interrupt numero 0x80 */
```

In altri casi, i parametri vengono collocati in un'area di memoria e poi l'indirizzo di inizio viene messo in alcuni registri. Ad esempio, nel seguente codice, prima di chiamare l'interrupt 0x80 viene collocata in un'area di memoria una stringa da stampare e poi l'indirizzo di inizio di questa stringa viene copiata nel registro ecx, mentre la lunghezza della stringa da stampare viene collocata nel registro edx. Solo dopo questo, viene invocato l'interrupt, il quale scatena la routine di gestione che controlla il contenuto di questi registri e si comporta in funzione di quello che trova in questi registri.

```
.data
miastringa: .string "STRUNZ\n" # stringa da stampare con a capo finale
...
movl $4, %eax           /* servizio da ottenere: stampa */
movl $1, %ebx           /* sottoservizio da ottenere: stampa da indirizzo */
movl $miastringa, %ecx  /*indirizzo di inizio stringa in registro ecx*/
movl $7, %edx           /* lunghezza stringa in registro edx */
int $0x80               /* ordine di eseguire interrupt */
```

## 6. CHIAMATA A SYSTEM CALL

Un programma in assembly, che opera su un processore Intel, tipicamente invoca le system call:

- **chiamando l'esecuzione dell'interrupt 0x80**
- e mettendo, prima, nel registro **eax** il numero identificatore della system call da eseguire
- e mettendo in altri registri i parametri necessari a quella system call.

Ad esempio, per stampare a video una stringa a partire da un indirizzo, il programma assembly può invocare l'esecuzione della system call 4 mettendo il valore 4 nel registro EAX (specifica il servizio) ed il valore 1 nel registro EBX (specifica il sottoservizio) poi chiamando l'interrrupt 0x80. Inoltre, prima della chiamata ad interrupt, il programma assembly mette nel registro ECX l'indirizzo di inizio della stringa da stampare e nel registro EDX il numero di byte da stampare. Vedere esempio sopra.

## 7. LIMITI dell' ISTRUZIONE 'int 0x80' (usare system call) IN PROCESSORI A 64 bit.

L'istruzione 'int 0x80' serve per invocare le system call quando eseguo codice in un processore Intel a 32 bit. Questa istruzione prende argomenti in registri a 32 bit. Ad esempio eax ed ebx per stabilire il servizio da utilizzare, edx per la lunghezza della stringa da stampare ed ecx per l'indirizzo della stringa da stampare.

Se io modifico il codice per eseguirlo su processore a 64 bit, utilizzando i registri a 64 bit rax rbx rcx ed rdx invece dei registri eax ebx ecx ed edx per passare i parametri all'istruzione 'int 0x80' allora possono accadere errori a run-time per due motivi:

a) **l'istruzione 'int 0x80' NON LEGGE TUTTO IL CONTENUTO DEI REGISTRI a 64 bit ma solo i 32 bit meno significativi di quei registri**, cioè la parte che equivale al corrispondente registro a 32 bit. I 32 bit più significativi vengono ignorati. Ciò implica che perdo parte del valore inserito nel registro. Se il registro conteneva un indirizzo a 64 bit, perdo parte dell'indirizzo e quando l'istruzione 'int 0x80' cerca di accedere all'indirizzo sbagliato può provocare un segmentation fault e far killare il processo.

a.1) Come caso particolare del precedente, se l'istruzione 'int 0x80' effettua operazioni di accesso allo stack posso avere problemi legati all'indirizzo della locazione nello stack.

Infatti, l'istruzione 'int 0x80' legge solo indirizzi a 32 bit anche se io li metto in registri a 64 bit. Se la locazione di memoria a cui voglio accedere si trova più in basso dell'indirizzo ( $2^{32}$ ) allora accedo correttamente. Se invece si trova nei  $2^{32}$  byte dall'indirizzo  $2^{32}$  compreso in su allora il tentativo di accesso fallisce e provoca un segmentation fault. Purtroppo, nelle architetture a 64 bit, lo stack è tipicamente collocato nella parte alta della memoria, sopra i  $2^{32}$  byte. Quindi se la system call chiamata dall'istruzione 'int 0x80' cerca di accedere allo stack, probabilmente causerà un segmentation fault. Se invece la system call chiamata dall'istruzione 'int 0x80' cerca di accedere solo alla sezione 'data' e alla sezione 'text' allora probabilmente tutto andrà a buon fine perché si accede a parti di memoria indirizzabili con i soli 32 bit meno significativi dei registri.

.

### **3. Invocare le system call in ambiente a 64 bit sostituendo l'istruzione 'int 0x80' con l'istruzione 'syscall'.**

Se devo invocare una system call a cui devo passare un indirizzo a 64 bit, non posso usare l'istruzione 'int 0x80' che esegue l'interrupt che attiva le system call.

Per invocare la system call devo fare 3 modifiche al codice:

- A. Usare l'istruzione 'syscall' invece che 'int 0x80'.
- B. Passare gli argomenti alla syscall nei registri giusti (diversi da quelli usati nella istruzione 'int').
- C. Passare il giusto numero che identifica ciascuna system call da eseguire (diverso da quello usato nella istruzione 'int').

Vediamo qualche dettaglio:

- A. Usare l'istruzione 'syscall' invece che 'int 0x80'.
- B. usare, per passare gli argomenti alla syscall, dei registri diversi da quelli che avrei usato per passare gli argomenti all'istruzione 'int 0x80'.

Posso trovare informazioni sulle system call usate a 64 bit nel file . In particolare si vede quali registri sono genericamente usati:

```
/*
 * System call entry. Upto 6 arguments in registers are supported.
 * SYSCALL does not save anything on the stack and
```

```

* does not change the stack pointer.
* Register setup:
* rax system call number
* rdi arg0
* rcx return address for syscall/sysret, C arg3
* rsi arg1
* rdx arg2
* r10 arg3      (--> moved to rcx for C)
* r8 arg4
* r9 arg5
* r11 eflags for syscall/sysret, temporary for C
* r12-r15,rbp,rbx saved by C code, not touched.
*/

```

**C. specificare correttamente il numero che identifica la system call. Questi numeri sono cambiati nel passaggio dalle architetture a 32 alle architetture a 64 bit.**

Guardare nel file 'unistd\_64.h' o ' /usr/include/asm-generic/unistd.h' per vedere l'elenco delle system calls ed i loro numeri identificativi.

Ad esempio, chiamando l'istruzione 'int 0x80', per ottenere la system call 'write' devo passare come numero di system call nel registro 'eax' il valore '4'.

Invece, chiamando l'istruzione '**syscall**', per ottenere la system call 'write' devo passare come numero di system call nel registro 'rax' il valore '**1**'.

Analogamente, la terminazione si ottiene col valore 1 usando l'interrupt 'int 0x80' mentre si ottiene con la system call numero 60 usando l'istruzione **syscall**.

Ad esempio, il codice a 32 bit per invocare la scrittura a video, di una stringa collocata nella parte dati, potrebbe essere questo:

```

movl $4, %eax          /* servizio da ottenere: write, stampa, in eax, è 4 */
movl $1, %ebx          /* primo arg, sottoservizio da ottenere, in ebx */
movl $mistringa, %ecx /* secondo arg, indirizzo di inizio stringa, in ecx */
movl $7, %edx          /* terzo arg, lunghezza stringa da stampare in edx */
int $0x80

```

Invece, il codice a 64 bit per invocare la scrittura a video di una stringa collocata nella parte dati sarà questo:

```

mov $1, %rax          /* servizio da ottenere: write, stampa, in rax, ora è 1 */
mov $1, %rdi          /* primo arg, sottoservizio da ottenere, in rdi non in rbx */
mov $mistringa, %rsi  /* secondo arg, indirizzo inizio stringa, in rsi non in ecx */

```

```
mov $7, %rdx          /* terzo arg, lunghezza stringa da stampare, in rdx */  
syscall              /* chiamo syscall non int 0x80 */
```