

SISTEMI OPERATIVI

File System
Interfaccia del File System

Lezione 1 – File e loro caratteristiche

Vincenzo Piuri

Università degli Studi di Milano - SSRI - CDL ONLINE

Sommario

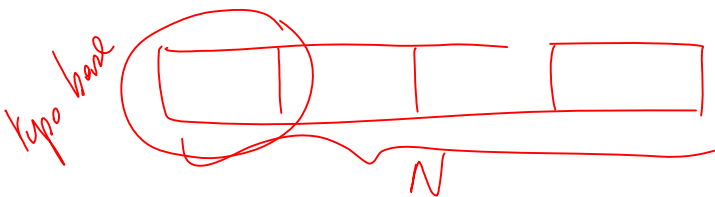
- File system
- Concetto di file
- Tipi di file
- Struttura dei file
- Attributi
- Operazioni
- Uso del file
- Metodi di accesso

File System

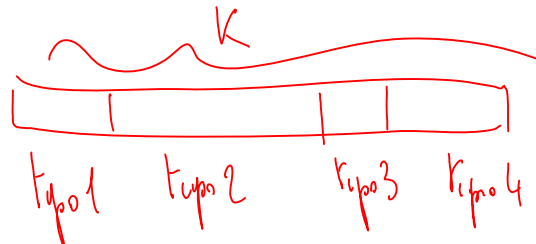
- Astrazione delle informazioni nei dispositivi fisici
- Visione *logica* dei dispositivi fisici di memorizzazione e trasferimento di informazioni
- Visione *omogenea* dei dispositivi fisici
- Supporto per la memorizzazione di lungo termine e al trasferimento di informazioni
- Consiste nella collezione e gestione di:
 - informazioni (dati, programmi) → **file**
 - metainformazioni (metadati) → **direttori** (directory)

Aggregazione di informazioni

- Array: N elementi omogenei

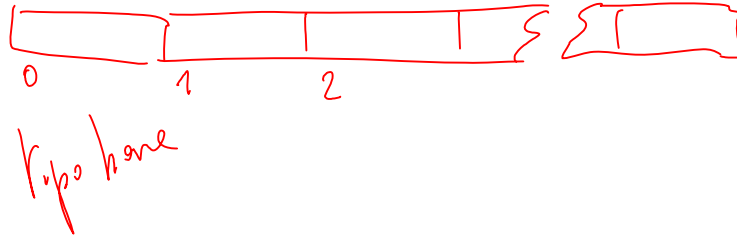


- Record: K elementi eventualmente disomogenei



File

Elementi omogenei in numero a priori non definito



Tipi di file (1)

- Dati
 - numerici
 - alfabetici → character
 - binari → byte
- Programmi

Tipi di file (2)

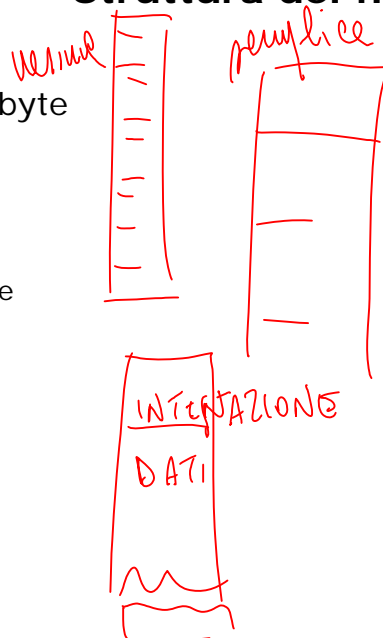
- Eseguibile (.exe, .com, .bin, nessuna)
- Oggetto (.obj, .o)
- Codice sorgente (.c, .cc, .java, .pas, .asm, .a)
- Batch (.bat, .sh)
- Testo (.txt, .doc)
- Elaborazione testi (.doc, .wp, .rtf, .tex)
- Libreria (.lib, .a, .so, .dll)
- Grafico (.ps, .pdf, .jpg, .gif, .png, .bmp)
- Archivio (.zip, .arc, .tar, .gz)
- Multimedia (.mpeg, .mov, .rm)

Struttura dei file

- Nessuna sequenza di parole o byte

- Struttura semplice
 - linee
 - lunghezza fissa o variabile

- Struttura complessa
 - documento formattato
 - file caricabile rilocabile



Attributi

- Nome
- Identificatore
- Tipo
- Locazione
- Dimensione
- Data di creazione
- Data di ultimo accesso
- Proprietario
- Protezione
- Formato
- ...

Descrittore del file

Operazioni sui file

- Creazione
- Scrittura
- Lettura
- Riposizionamento
- Cancellazione
- Troncamento
- Accodamento
- Modifica di attributi
- Blocco per condivisione
- ...

Uso dei file (1)

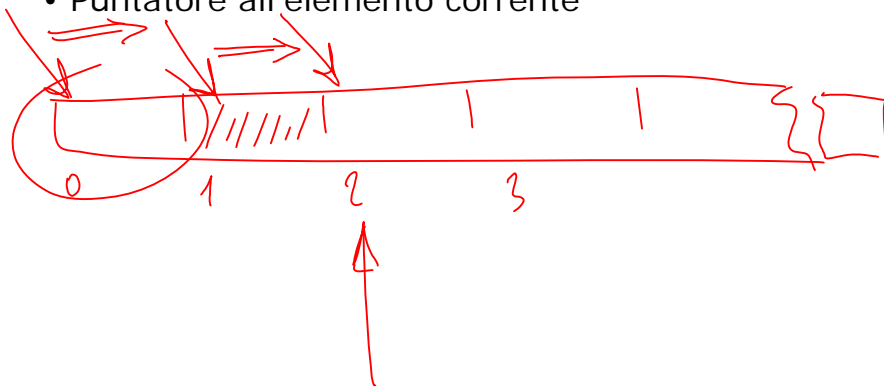
Apertura di un file

- Verifica delle autorizzazioni all'accesso
- Identificazione del descrittore del file nel file system
- Identificazione della locazione nei dispositivi fisici
- Verifica e gestione dello stato di uso condiviso
- Inizializzazione delle informazioni per la gestione efficiente (tabella dei file aperti)

Uso dei file (2)

Lettura e scrittura

- Puntatore all'elemento corrente



Uso dei file (3)

Lettura e scrittura

- Accesso attraverso la tabella dei file aperti per reperire:
 - posizione dei componenti del file nei dispositivi fisici
 - puntatore al file per identificare l'elemento correntemente in uso
 - blocco per accesso condiviso

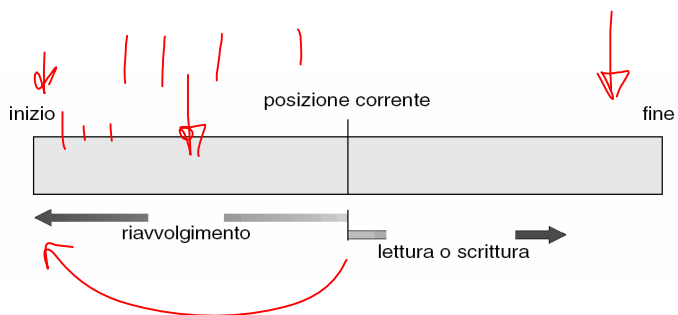
Uso dei file (4)

Chiusura di un file

- Aggiornamento delle informazioni di gestione
- Rilascio dell'uso condiviso
- Cancellazione delle informazioni di gestione nella tabella dei file aperti

Metodi di accesso (1)

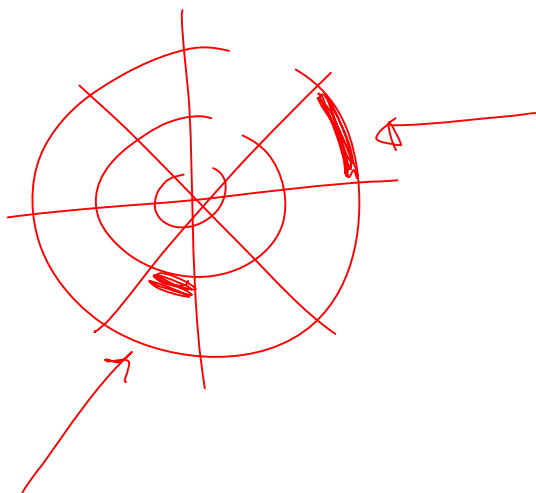
Accesso sequenziale



nastri

Metodi di accesso (2)

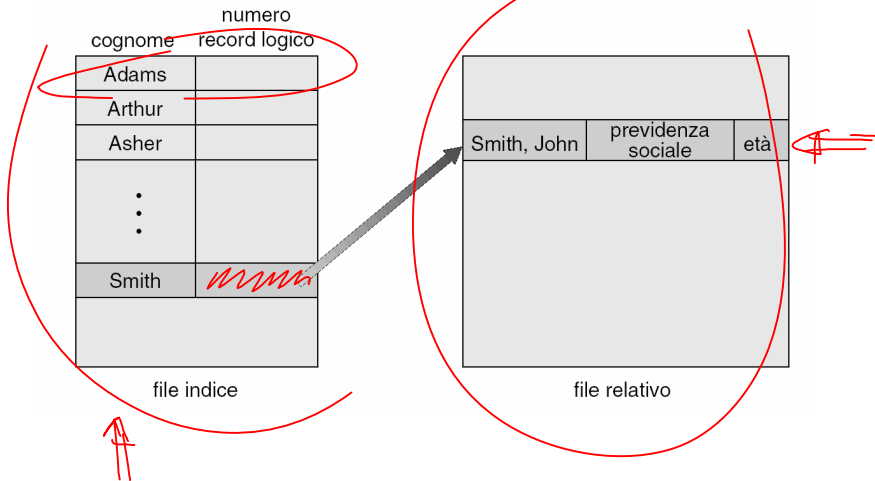
Accesso diretto



dischi

Metodi di accesso (3)

Accesso indicizzato



In sintesi

- File system
- Concetto di file
- Tipi di file
- Struttura dei file
- Attributi
- Operazioni
- Uso dei file
- Metodi di accesso

SISTEMI OPERATIVI

File System
Interfaccia del File System

Lezione 2 – Direttori e loro caratteristiche

Vincenzo Piuri

Università degli Studi di Milano - SSRI - CDL ONLINE

Sommario

- Concetto di direttorio (*directory*)
- Operazioni sui direttori
- Struttura del file system
- Partizioni
- Montaggio del file system

Direttorio (*Directory*)

- Supportare il raggruppamento di file in base a criteri logici
- Supportare gestione efficiente dell'accesso ai file
- Supportare condivisione e protezione
- Collezione omogenea di informazioni (attributi) su gruppi di file



Operazioni

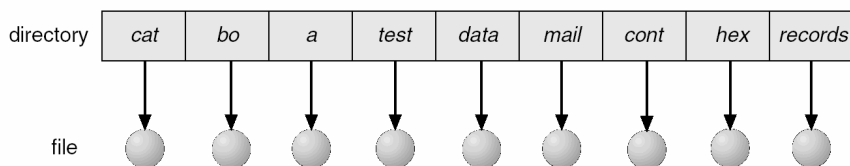
- Su file:
 - creare
 - cancellare
 - ridenominare
 - modifiche degli attributi
 - ...
- Su direttori:
 - individuare posizione logica di un file nel file system
 - elencare file
 - ricercare file
 - ...

Strutturazione del file system

Organizzazione dei direttori:

- a singolo livello
- a due livelli
- ad albero
- a grafo aciclico
- a grafo generale

Direttorio a singolo livello

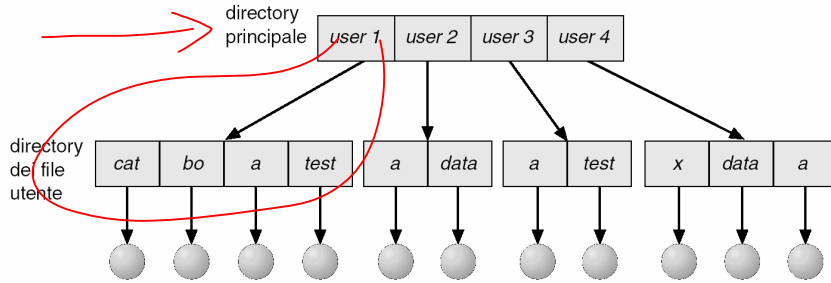


Struttura tipica di vecchi sistemi mono-utente
con piccola memoria di massa

Problemi:

- gestione omonimie
- ridenominazione
- raggruppamento

Direttorio a due livelli

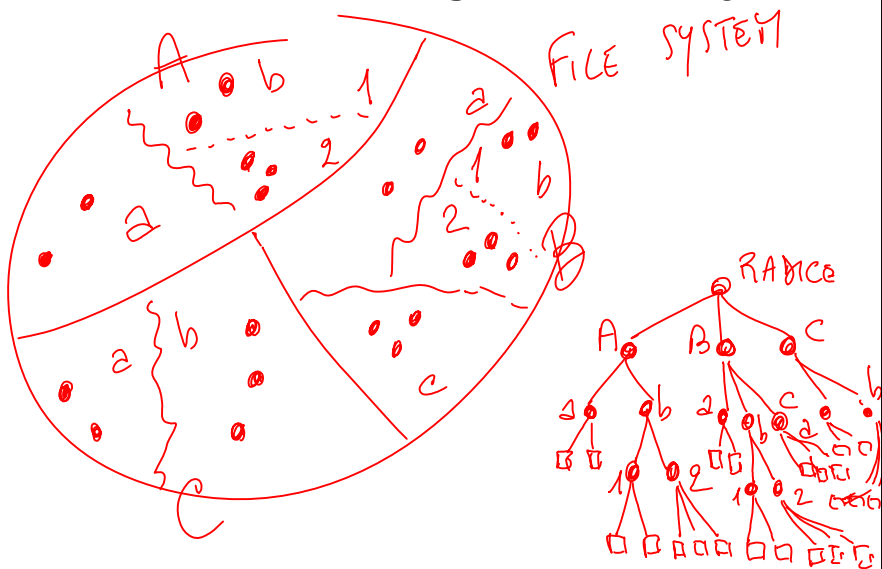


Un direttorio per utente

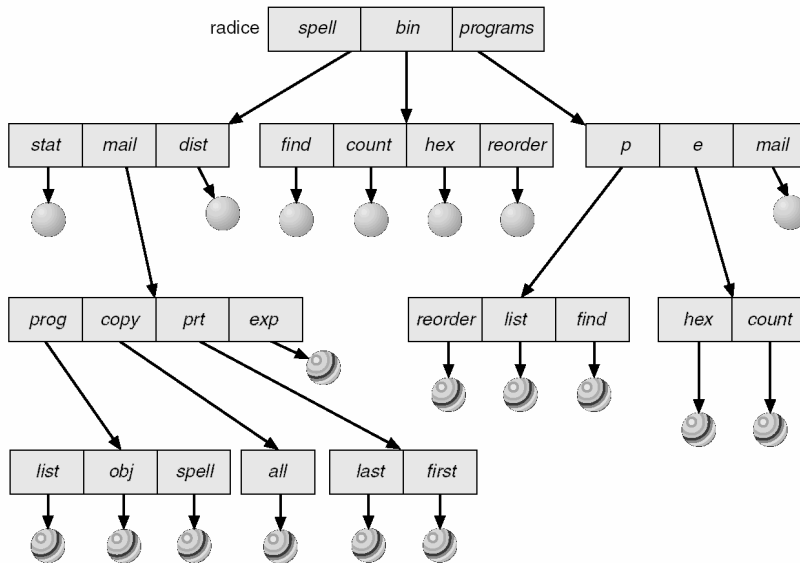
Tipico di piccoli vecchi sistemi multi-utente

- File omonimi per utenti diversi
- Ricerca più efficiente per singoli utenti
- Nessuna capacità di raggruppamento
- Nessuna possibilità di condivisione

Visione logica del file system



Direttorio ad albero (1)



Direttorio ad albero (2)

Gestione adatta a sistemi multi-utente

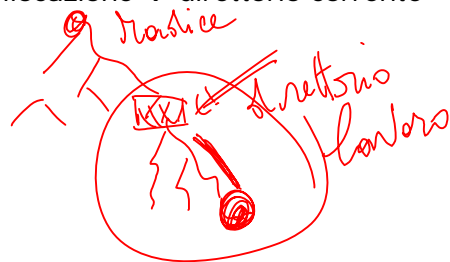
Ricerca efficiente

Capacità di raggruppamento

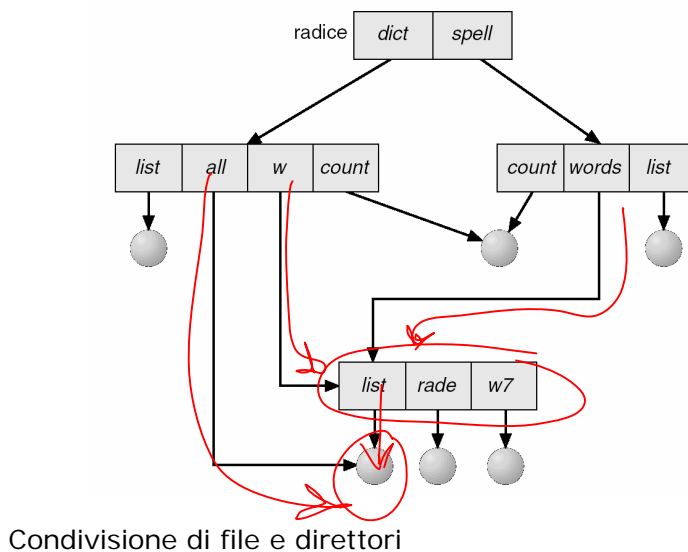
Capacità di condivisione

Identificazione e capacità di rilocalizzazione → direttorio corrente

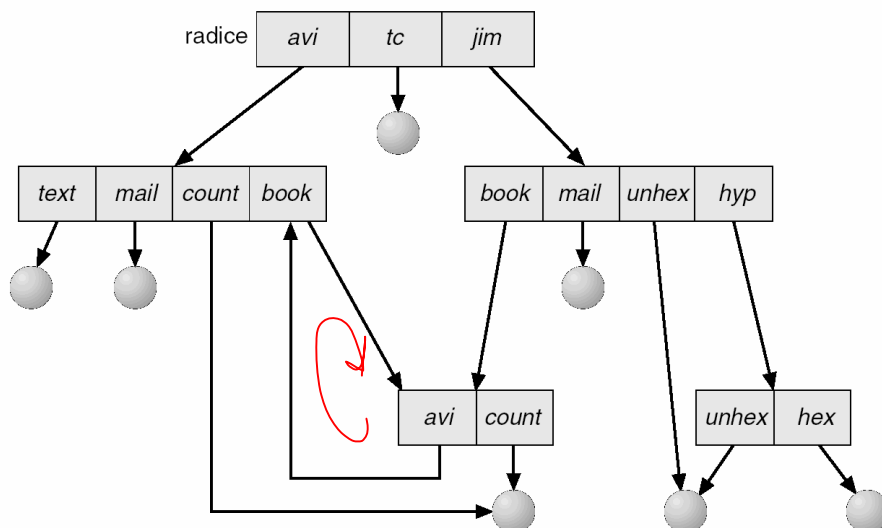
- percorso relativo
- percorso assoluto



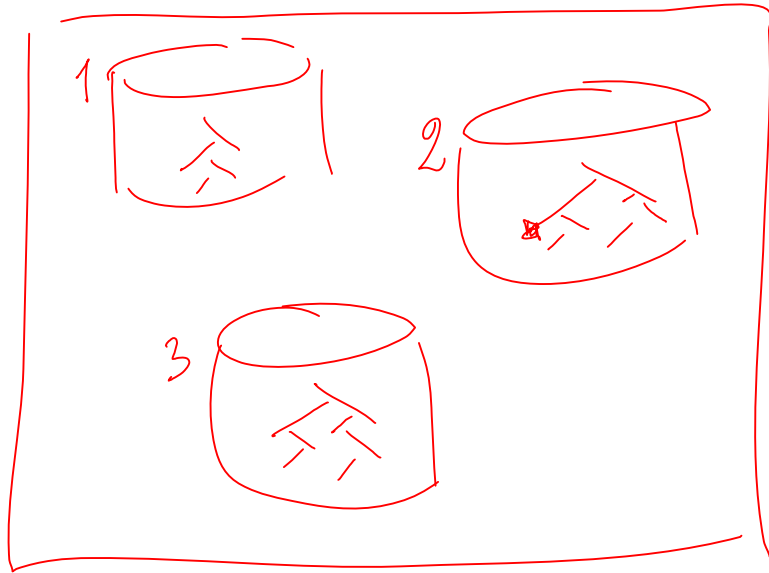
Direttorio a grafo aciclico



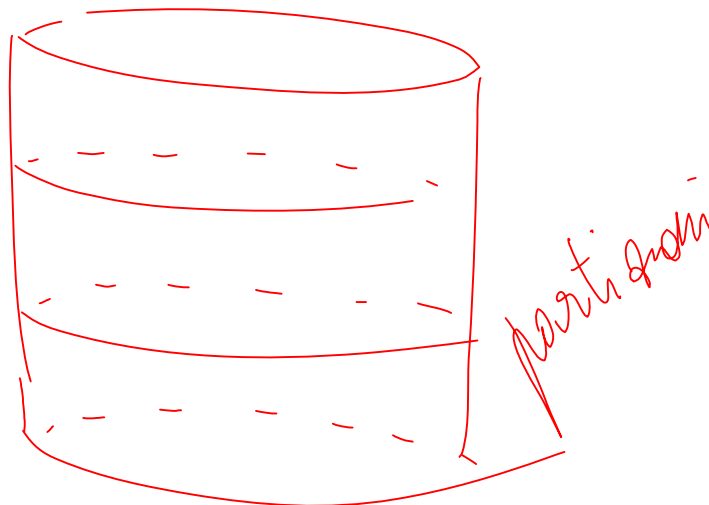
Direttorio a grafo generale



Memorie di massa a dischi multipli

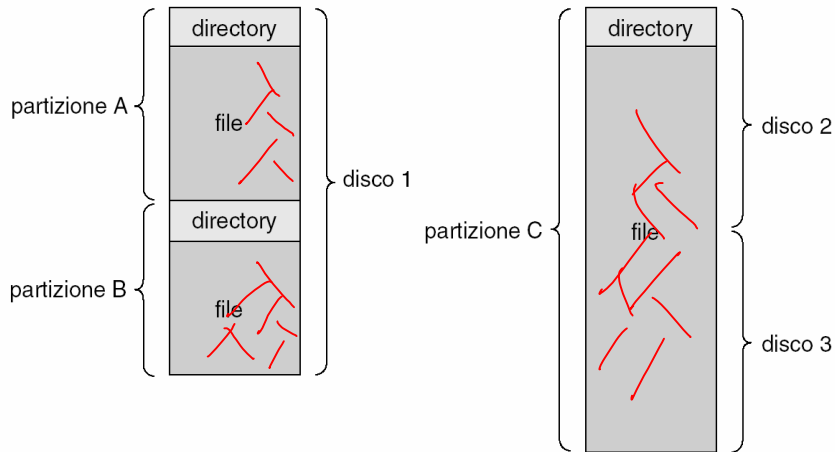


Memorie di massa con grossi dischi



Partizione

Astrazione del dispositivo fisico
di memorizzazione di massa



Montaggio dei file system



In sintesi

- Direttorio
- Operazioni
- Organizzazione del file system:
 - direttorio a singolo livello
 - direttorio a due livelli
 - direttorio ad albero
 - direttorio a grafo
- Visione logica del file system e dell'organizzazione dei direttori
- Partizioni
- Montaggio del file system

SISTEMI OPERATIVI

File System
Interfaccia del File System

Lezione 3 – Condivisione dei file e protezione

Vincenzo Piuri

Università degli Studi di Milano - SSRI - CDL ONLINE

Sommario

- Condivisione dei file
 - Sistema centrale
 - Sistema distribuito
- Coerenza
- Protezione
 - Controllo degli accessi

Condivisione dei file

Sistemi multi-utente

Utile per supportare:

- condivisione di informazioni
- collaborazione tra utenti

Accesso al file:

- contemporaneo → operazioni compatibili
- in mutua esclusione → operazioni incompatibili

Sistemi multi-utente

 autenticazione

- Identificazione univoca degli utenti e dei gruppi
- Definizione e verifica degli accessi ai file in funzione dei diritti assegnati
- Attributi articolati per definire autorizzazioni all'accesso per
 - utente proprietario
 - gruppo a cui appartiene il proprietario
 - altri

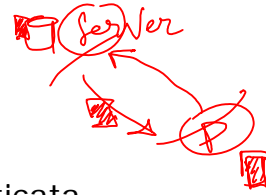
File system remoti

Metodi di condivisione:

- Trasferimento di file

- ftp
- http

con modalità anonima o autenticata



- File system in rete

- file system di rete con modello client/server
- file system distribuito



Coerenza

- Specifica la modalità di accesso ad un file condiviso per garantire la consistenza delle informazioni
- Definisce le modalità di aggiornamento dei file condivisi
 - modifiche immediatamente visibili
 - modifiche visibili solo immediatamente dopo la chiusura del file
 - modifiche visibili solo nelle sessioni successive alla chiusura del file
 - file condivisi immutabili

Coerenza in caso di guasti

- Cause di guasto nei sistemi in rete:
 - guasti locali a client
 - guasti locali a server
 - guasti alla rete
- Gestione dei guasti:
 - rilevamento
 - ripristino
 - sopravvivenza con capacità limitate
 - tolleranza ai guasto mediante ridondanza
- Stato del file system

Protezione

Obiettivo:

proteggere le informazioni da accessi impropri
e garantirne la consistenza rispetto a tali accessi

Tecniche:

- accesso fisico
- permessi su operazioni:
 - lettura
 - scrittura
 - esecuzione
 - cancellazione
 - accodamento

*autenticazione
+
verifica permessi*

Controllo dell'accesso

- Accesso ad una risorsa dipendente dall'identità in funzione delle autorizzazioni concesse a ciascun utente
- Lista di controllo degli accessi
Access Control List, ACL
 - approccio flessibile
 - lista lunga e di difficile gestione
- Versione ridotta della lista di controllo accessi:
proprietario / gruppo / universo
- Lista delle capacità (Capabilities)
- Password

In sintesi

- Condivisione di file
- Coerenza
- Protezione

SISTEMI OPERATIVI

File System
Implementazione del File System

Lezione 1 – Struttura e realizzazione

Vincenzo Piuri

Università degli Studi di Milano - SSRI - CDL ONLINE

Sommario

- Obiettivo
- Struttura della gestione del file system
- Strutture dati per la gestione del file system

Obiettivo del file system

- Gestire in modo omogeneo
le risorse informative e fisiche
del sistema di elaborazione
come flussi di informazioni elementari
- Focalizziamo l'attenzione
sulle informazioni memorizzate
nelle memorie secondarie
(memorie di massa: dischi)
e sulla loro gestione nel file system

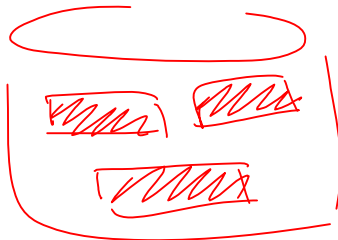
Supporto fisico del file system

Memoria secondaria

- Dischi

Caratteristica per gestione del file system

- Dispositivo di memorizzazione a blocchi
- Partizioni

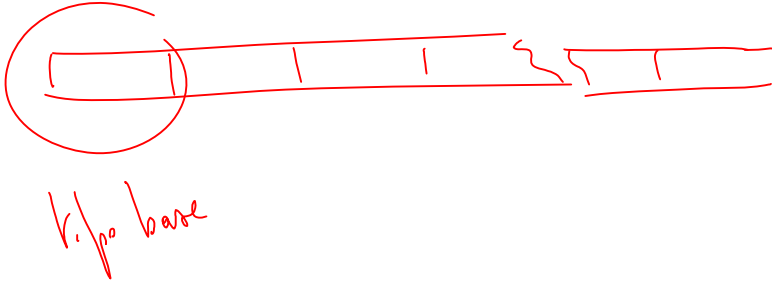


Visione utente delle informazioni nel file system

File

Caratteristica per gestione del file system

- Flusso di elementi omogenei



File system

La gestione del file system nel sistema operativo
deve trasformare

(il livello fisico di memorizzazione delle informazioni
a blocchi nella memoria di massa
nel livello logico di visione come file

- Astrazione della rappresentazione fisica
- Virtualizzazione delle informazioni

Struttura della gestione del file system

- Gestione della periferica
Comunicazioni con periferica, gestione dipendente dal dispositivo, gestione indipendente dal dispositivo
- File system di base
Gestisce la lettura/scrittura di blocchi fisici
- Modulo di organizzazione dei file
Costruisce la sequenza di blocchi fisici che contengono il file e gestisce lo spazio libero
- File system logico
Gestisce i metadati che definiscono la struttura del file system e l'identificazione dei file

Strutture dati per la gestione del file system (1)

Strutture su disco

- blocco di controllo del boot
- blocco di controllo della partizione
- directory
- blocchi di controllo dei file

Strutture dati per la gestione del file system (2)

permessi sul file
date del file (creazione, accesso, scrittura)
proprietario, gruppo, ACL del file
dimensione del file
blocchi di dati del file

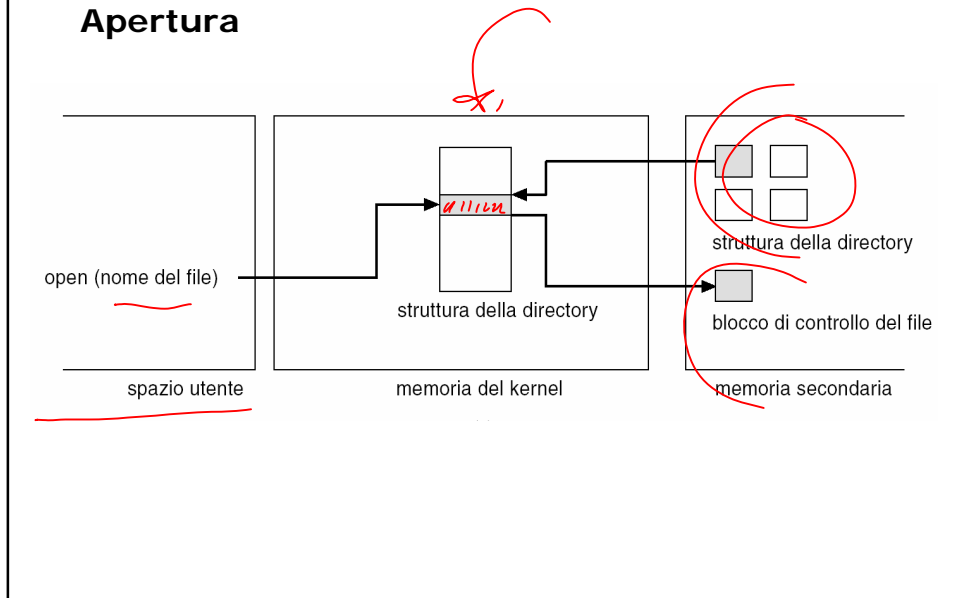
Strutture dati per la gestione del file system (3)

Strutture in memoria centrale

- tabella delle partizioni
- descrittori delle directory
- tabella dei file aperti del sistema
- tabella dei file aperti per un processo
- tabella di montaggio dei file system

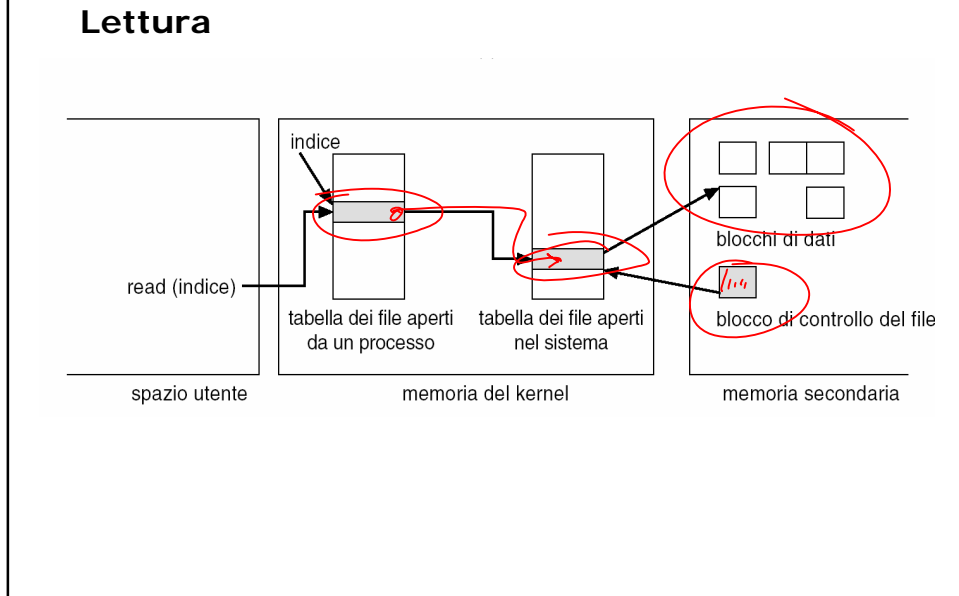
Strutture del file system in memoria

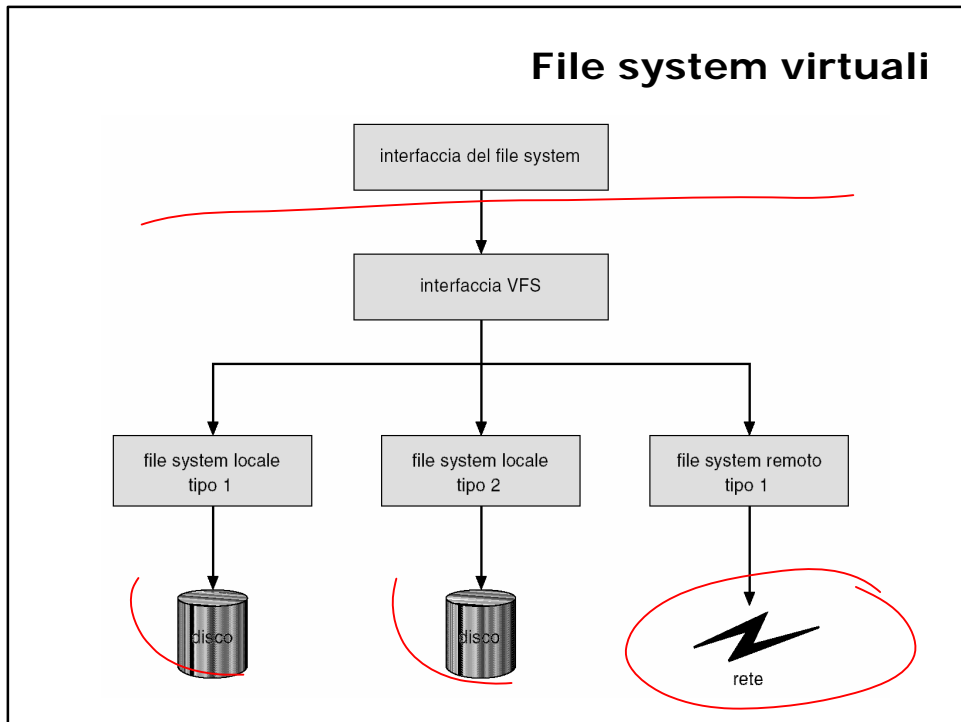
Apertura



Strutture del file system in memoria (2)

Lettura





In sintesi

- Struttura della gestione del file system
- Strutture dati per la gestione del file system

SISTEMI OPERATIVI

File System
Implementazione del File System

Lezione 2 – Realizzazione dei direttori

Vincenzo Piuri

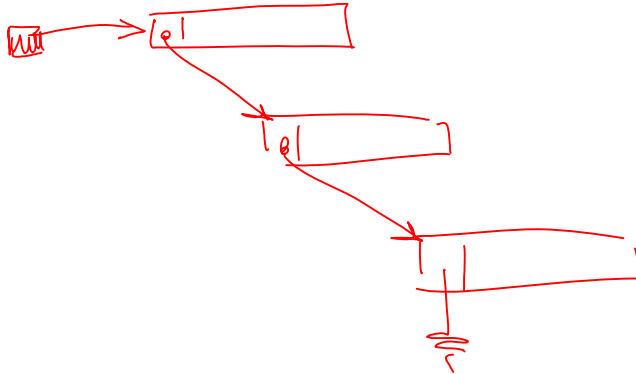
Università degli Studi di Milano - SSRI - CDL ONLINE

Sommario

- Tecniche per la realizzazione dei direttori
 - Lista
 - Tabella di hash
- Prestazioni

Struttura a lista (1)

Elenco di file e dei riferimenti ai blocchi di dati

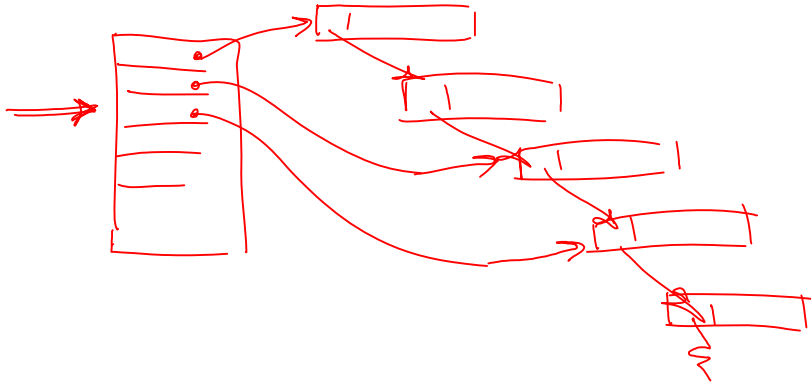


Struttura a lista (2)

- Implementazione semplice
- Efficiente per visualizzazione dell'elenco ordinato dei file
 - Richiede ordinamento
- Accesso costoso: scansione lineare
 - Miglioramenti:
 - cache
 - lista ordinata
 - B-tree

Struttura a tabella di hash (1)

- Lista per memorizzare elementi
- Tabella con funzione di hashing per identificare rapidamente elementi nella lista



Struttura a tabella di hash (2)

- Scelta della funzione di hash
- Velocizza accesso alla lista
- Collisioni

In sintesi

- Struttura a liste
- Struttura a tabella di hash

SISTEMI OPERATIVI

File System
Implementazione del File System

Lezione 3 – Realizzazione dei file: Gestione dell'astrazione dei file

Vincenzo Piuri

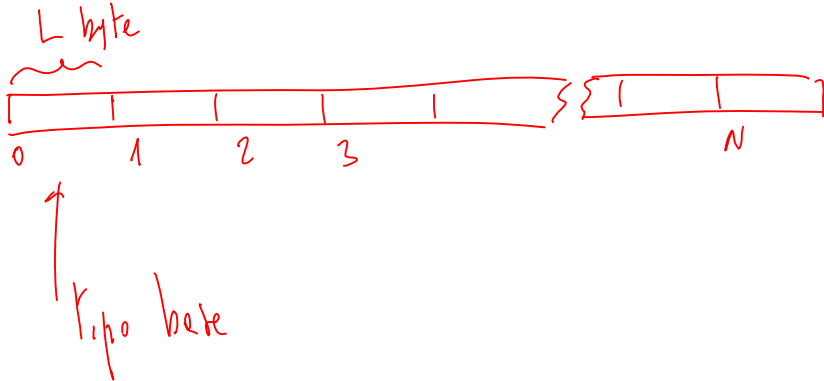
Università degli Studi di Milano - SSRI - CDL ONLINE

Sommario

- Memorizzazione di un file in memoria di massa
 - Visione fisica
 - Byte stream
- Gestione dell'astrazione dei file

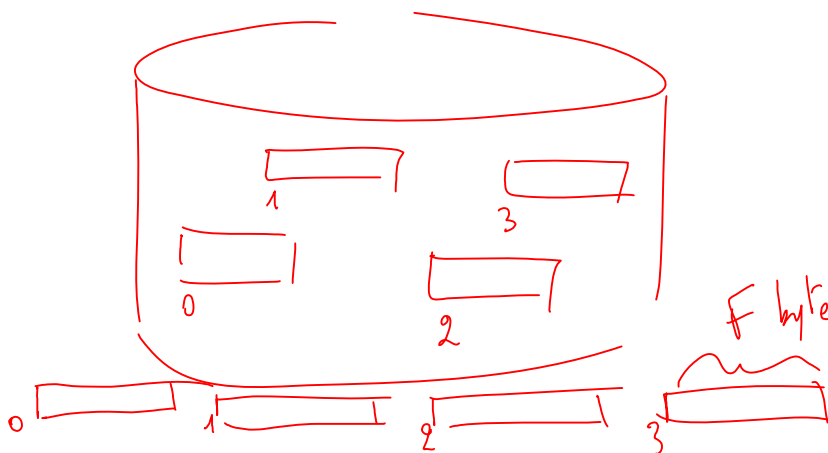
Visione logica del file

Sequenza di elementi omogenei (**record logici**)
in numero non limitato



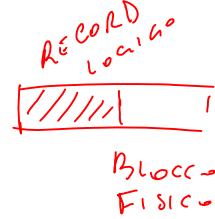
Visione fisica del file

Insieme ordinato di elementi fisici (**blocchi fisici**)
del supporto di memoria di massa



Mappaggio della visione logica sulla visione fisica del file

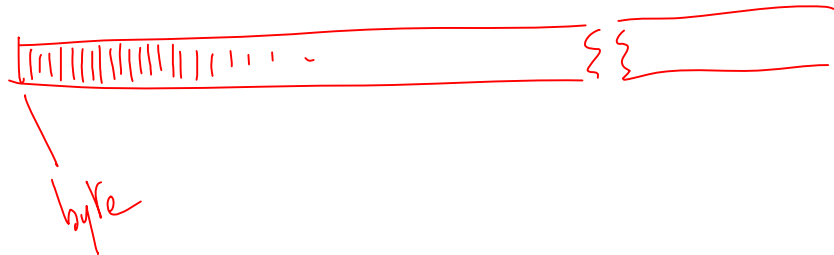
- Record logici tipizzati
 - Dimensione: **L** byte
- Blocchi fisici uniformi per supporto di memoria di massa
 - Dimensione: **F** byte
- Mappaggio per la memorizzazione
 - Un record logico in un blocco fisico
 - $L < F \rightarrow$ sfridi
 - $L > F \rightarrow$ tipo base non memorizzabile
 - K record logici in un blocco fisico: $K = \max\{ n \mid nL = F \}$
 - $KL < F \rightarrow$ sfridi



Visione logica omogenea del file

Byte stream

Flusso di byte

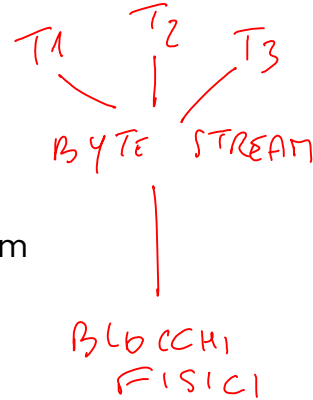


Tutti i file vengono visti come sequenze di byte
 Tipo base: byte

Mappaggio con byte stream (1)

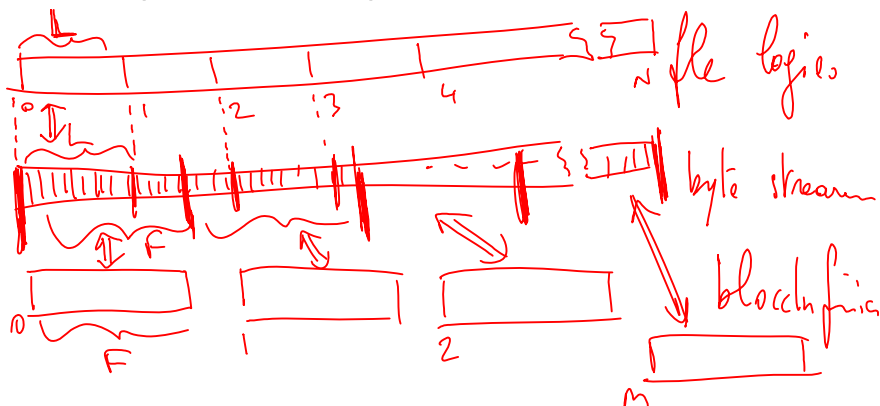
Come mappare la visione logica
nella visione fisica
attraverso la visione logica a byte stream?

- Mappare la visione logica nella visione a byte stream rimuovendo la tipizzazione
- Mappare la visione a byte stream nella visione fisica imponendo raggruppamento degli elementi logici (byte) in blocchi fisici

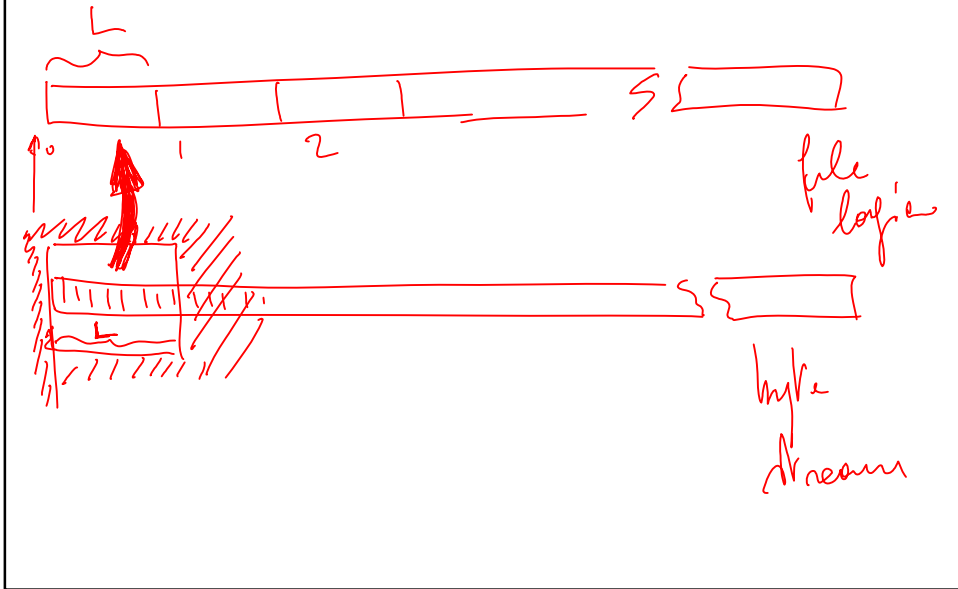


Mappaggio con byte stream (2)

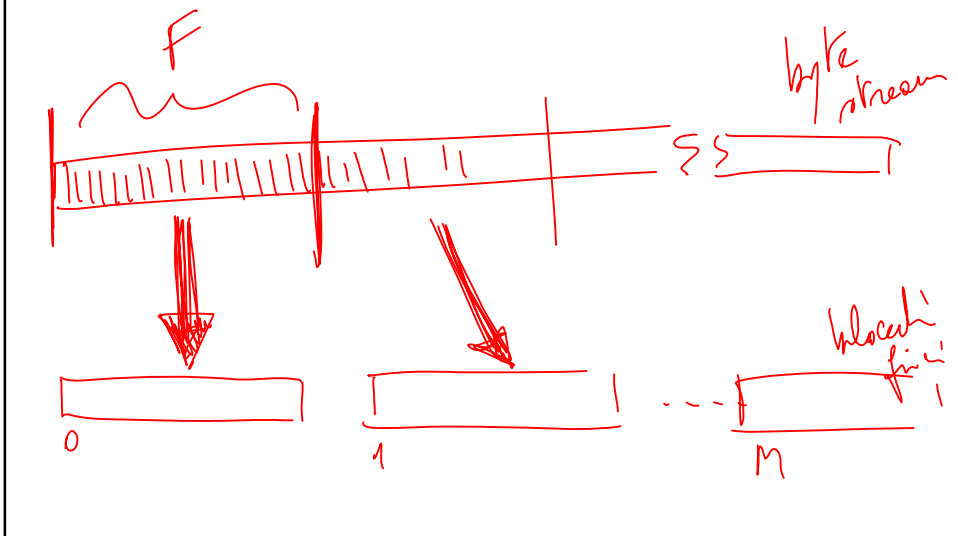
- Sempre possibile
- Sfridi sempre nulli poiché il tipo base (byte) è sempre sottomultiplo di F



Mappaggio con byte stream (3)

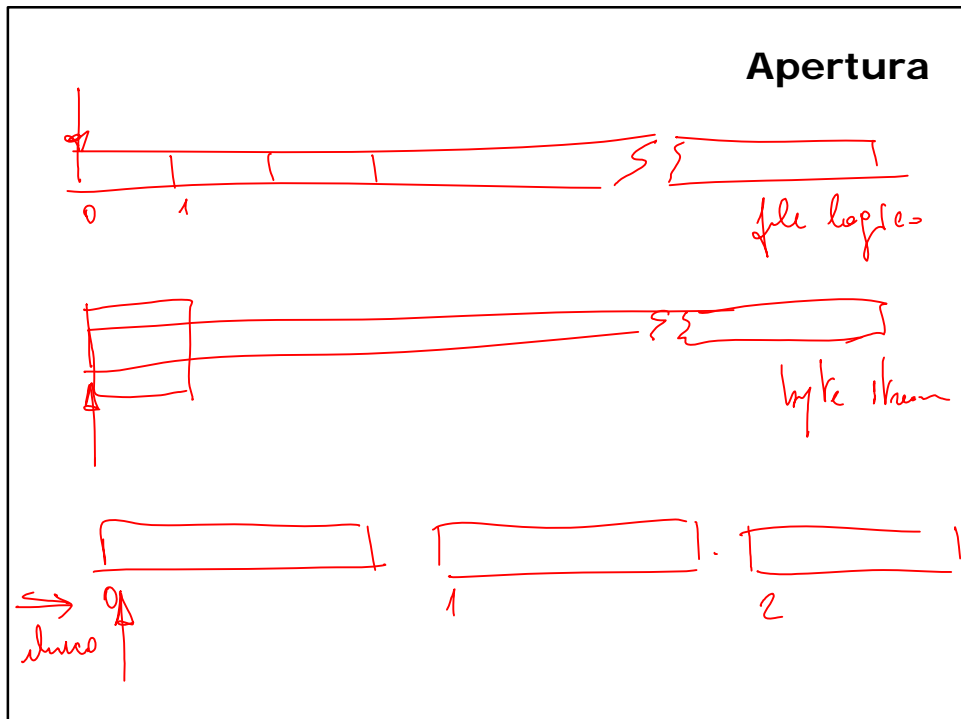


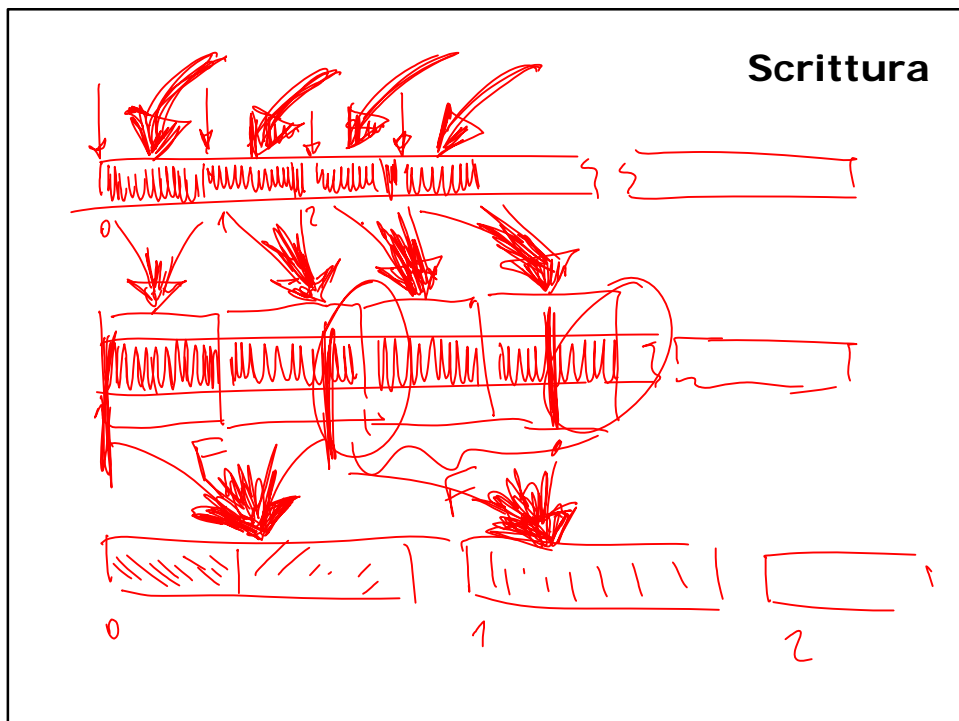
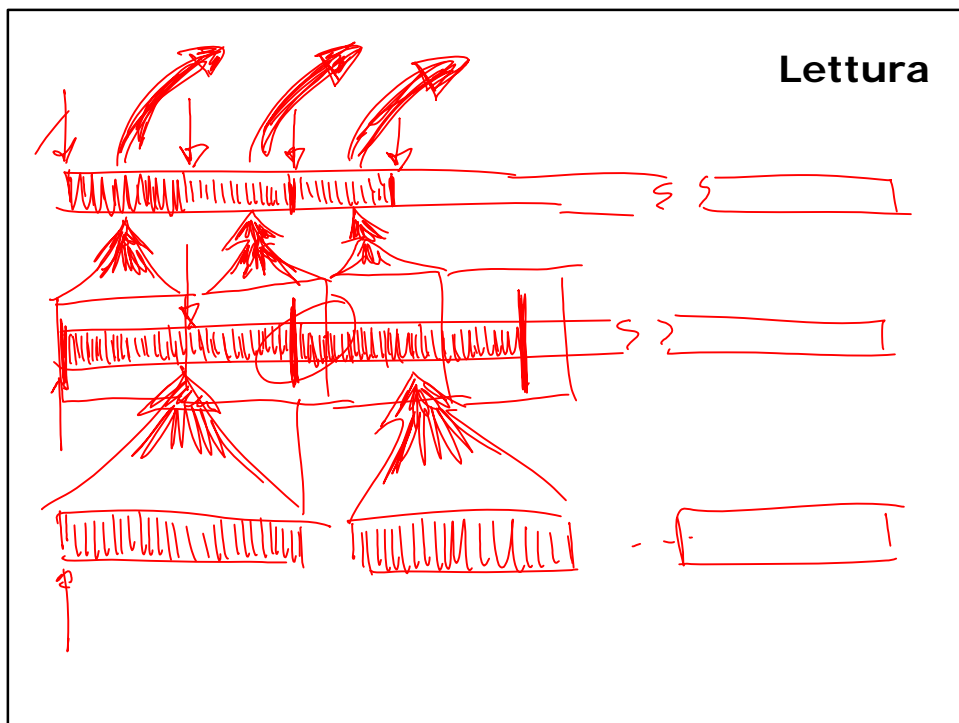
Mappaggio con byte stream (4)



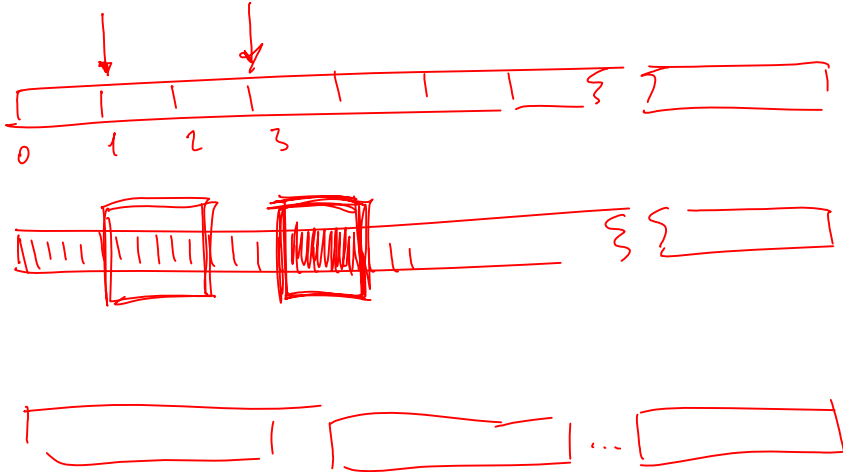
Gestione dell'astrazione dei file

- Apertura
- Lettura
- Scrittura
- Posizionamento (seek)
- Chiusura





Posizionamento - Seek



Chiusura

- Lettura
 - Libera strutture dati di gestione dei file
- Scrittura
 - Salva su disco l'eventuale byte stream non salvato
 - Libera strutture dati di gestione dei file

In sintesi

- Memorizzazione di un file in memoria di massa
- Gestione dell'astrazione dei file

SISTEMI OPERATIVI

File System
Implementazione del File System

Lezione 4 – Realizzazione dei file: Allocazione dei blocchi

Vincenzo Piuri

Università degli Studi di Milano - SSRI - CDL ONLINE

Sommario

- Allocazione dei blocchi fisici
- Gestione della lista libera dei blocchi fisici

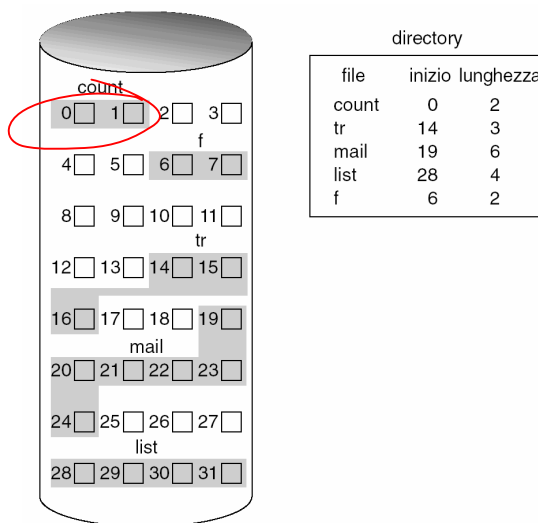
Allocazione dei blocchi

Creare l'insieme ordinato dei blocchi fisici
a supporto dell'astrazione dei file

- Allocazione contigua
- Allocazione collegata
- Allocazione indicizzata

Allocazione contigua (1)

Ordinamento sequenziale adiacente dei blocchi

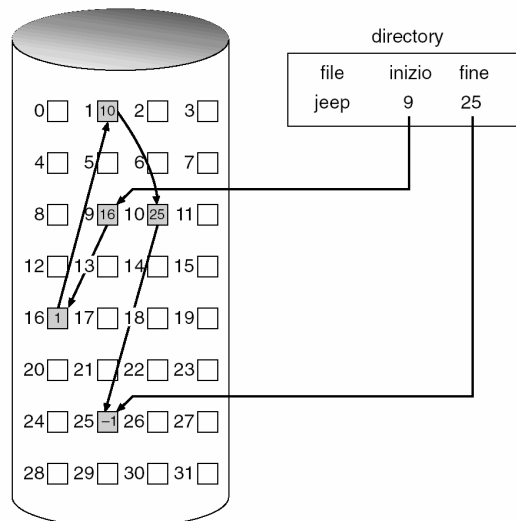


Allocazione contigua (2)

- Accesso rapido al blocco successivo
- Accesso diretto lento
- Problema di mancanza di spazio contiguo per l'allocazione
 - nuovo file
 - estensione di file esistente
- Frammentazione esterna
 - compattazione
- Estensione dei file
 - frammentazione interna

Allocazione collegata (1)

Lista collegata di blocchi (linked allocation)

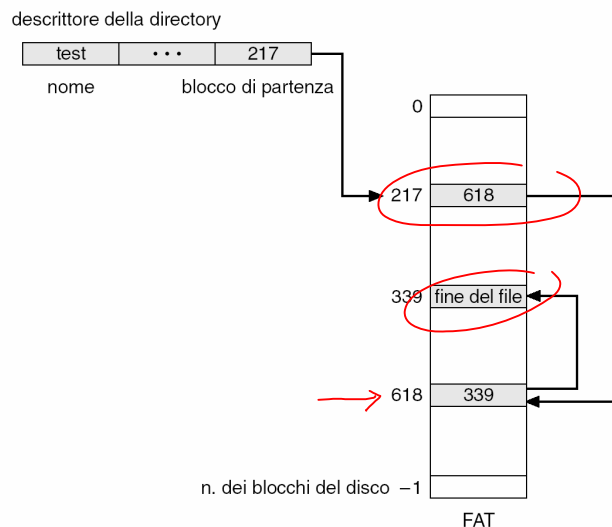


Allocazione collegata (2)

- Nessuna frammentazione esterna
- Accesso diretto lento
- Spazio per i puntatori al blocco successivo
 - cluster
- Problemi di affidabilità in caso di guasto in un blocco fisico

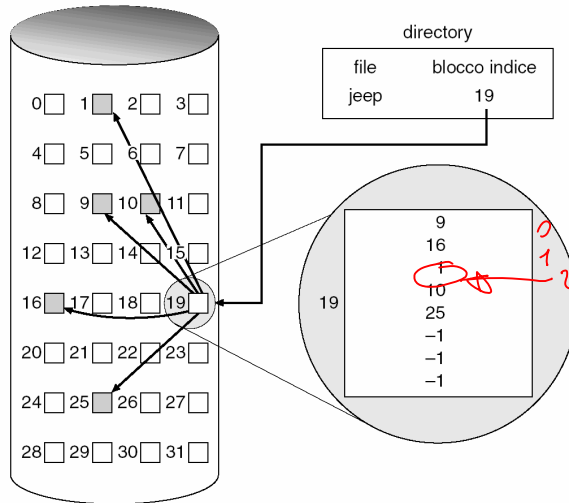
Allocazione collegata (3)

File Allocation Table (FAT)



Allocazione indicizzata (1)

Indice (**i-node**) contenente la sequenza dei puntatori ai blocchi fisici

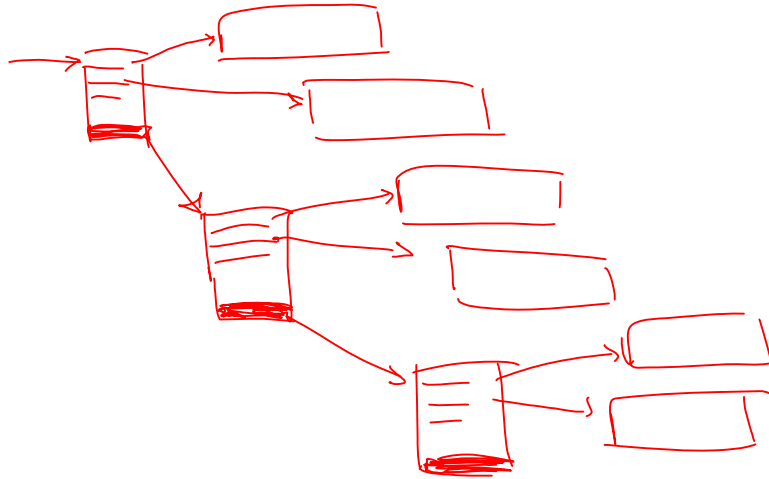


Allocazione indicizzata (2)

- Un indice per file
- Nessuna frammentazione esterna
- Accesso diretto veloce
- Affidabilità
- Dimensionamento del blocco indice
 - schema collegato
 - indice multilivello
 - schema combinato

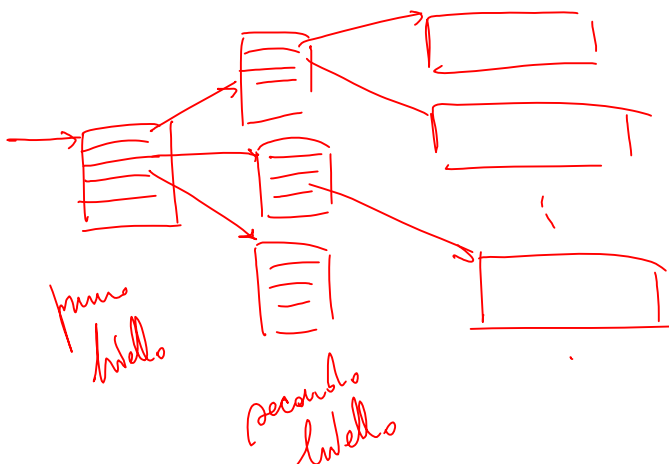
Allocazione indicizzata (3)

Blocco indice con schema collegato



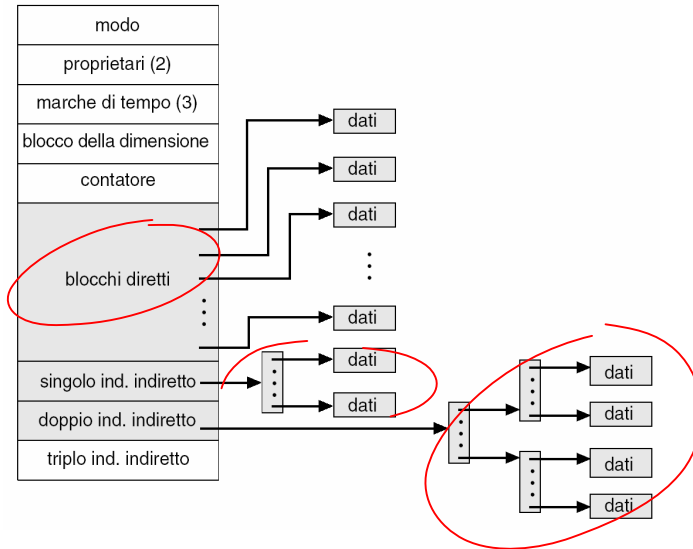
Allocazione indicizzata (4)

Blocco indice con indice multi-livello



Allocazione indicizzata (5)

Blocco indice con schema combinato



Miglioramento delle prestazioni per allocazione

- Caching delle informazioni di gestione
- Lettura anticipata (read ahead)

Gestione dello spazio libero (1)

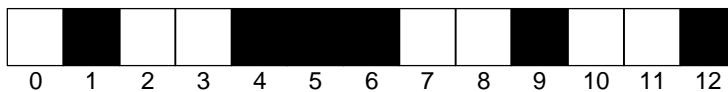
- Vettore di bit
- Lista collegata
- Raggruppamento
- Conteggio

Gestione dello spazio libero (2)

Vettore di bit

Bitmap

1011000110110

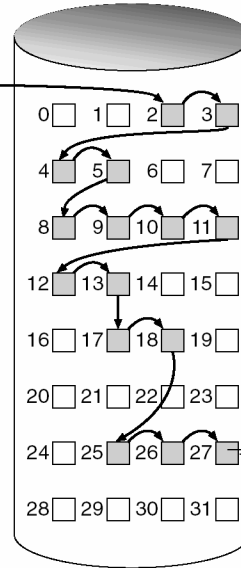


- Efficiente se supporto hardware

Gestione dello spazio libero (3)

Lista collegata

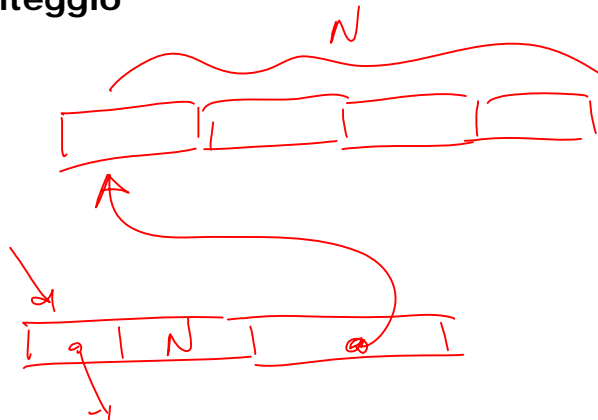
testa della lista
dello spazio libero



Raggruppamento

Gestione dello spazio libero (4)

Conteggio



In sintesi

- Allocazione dei blocchi fisici
- Gestione della lista libera dei blocchi fisici

SISTEMI OPERATIVI

File System
Implementazione del File System

Lezione 5 – Valutazione dell'efficienza e delle prestazioni

Vincenzo Piuri

Università degli Studi di Milano

Sommario

- Efficienza:
uso ottimale delle risorse per il file system
- Prestazioni:
uso rapido delle risorse per il file system
- Tecniche per migliorare l'efficienza
- Tecniche per migliorare le prestazioni

Efficienza

Sfruttamento ottimale delle risorse per il file system

- Dimensionamento
 - Blocchi
 - Puntatori
 - Metadati
- Rendimento dello spazio
 - Frammentazione interna
 - Frammentazione esterna
 - Aree usate per informazioni di gestione

Tecniche per migliorare l'efficienza

Cluster di dimensioni differenti

Definizione di

- dimensione di blocchi, puntatori e metadati
- metadati

in funzione della tecnologia e delle modalità di uso

Esempi:

- FAT10, FAT16, FAT32
- allocazione statica e dinamica delle tabelle in memoria

Prestazioni

Rapidità di uso delle risorse per il file system

- Modo di uso delle risorse per il file system
- Strutture dati a supporto dell'uso delle risorse per il file system
- Supporti hardware all'uso delle risorse per il file system
 - Memoria centrale
 - Cache

Tecniche per migliorare le prestazioni ⁽¹⁾

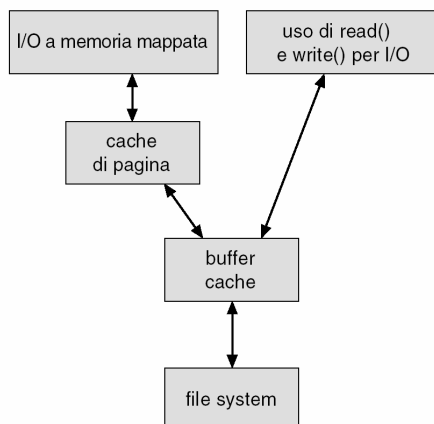
- Algoritmi semplici
- Strutture dati ad accesso veloce

Tecniche per migliorare le prestazioni (2)

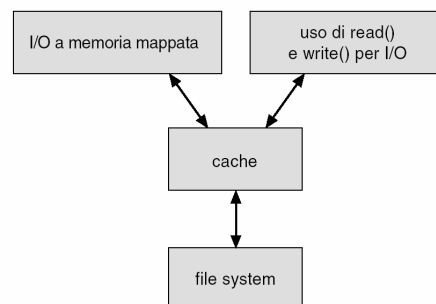
- Supporti hardware dedicati all'accesso ai dischi
 - Cache del disco
 - Cache delle pagine
 - Buffer cache unificata
 - Memoria virtuale unificata

Tecniche per migliorare le prestazioni (3)

Doppia cache



Buffer cache unificata



Tecniche per migliorare le prestazioni (4)

Gestione della cache

- Algoritmo LRU
- Priorità di paginazione

Tecniche per migliorare le prestazioni (5)

I/O mediato da cache

Minimizzare lo spostamento della testina

Scritture asincrone

Alternative all'algoritmo LRU

- free-behind
- read-ahead

Tecniche per migliorare le prestazioni (6)

Memoria virtuale unificata: disco virtuale

- RAM-disk

In sintesi

- Efficienza
- Prestazioni
- Tecniche per migliorare l'efficienza
 - Scelta accurata degli algoritmi e delle strutture dati
- Tecniche per migliorare le prestazioni
 - Scelta accurata degli algoritmi e dei componenti hardware

SISTEMI OPERATIVI

File System
Implementazione del File System

Lezione 6 – Manutenzione del file system

Vincenzo Piuri

Università degli Studi di Milano - SSRI - CDL ONLINE

Sommario

- Errori nel file system
- Coerenza del file system
- Backup e ripristino del file system

Errori nel file system

- Danneggiamenti della struttura dati (consistenza)
- Danneggiamenti del supporto fisico

Coerenza del file system

Allineamento dei valori dei dati e dei metadati in memoria e su disco

- Controllore della coerenza (consistenza)
- Scritture sincrone per i dati e i metadati critici

Backup e ripristino (1)

Salvataggio di sicurezza dei dati e dei metadati
backup

**Creare e conservare copia delle informazioni
per superare situazioni di problemi fisici
ai supporti di memoria di massa**

- malfunzionamenti
- guasti
- catastrofi

Backup completo

Backup incrementali

Backup e ripristino (2)

Ripristino dei dati e dei metadati
restore

**Caricare dati e metadati in memoria di massa
per ripristinare una situazione coerente
precedente a guasti fisici**

Backup e ripristino (3)

File system orientati alle transazioni con registrazione

log-based transaction-oriented file system

File system basato sulla registrazione delle attività

journaling

In sintesi

- Coerenza del file system
- Backup e ripristino del file system

SISTEMI OPERATIVI

File System
Protezione

Lezione 1 – Concetti fondamentali della protezione

Vincenzo Piuri

Università degli Studi di Milano - SSRI - CDL ONLINE

Sommario

- Obiettivi
- Domini di protezione
- Operazioni sui domini di protezione

Protezione

**Proteggere le risorse da accessi non autorizzati
(errati o indebiti)**

Obiettivo

**Definire le autorizzazioni ad utilizzare
le risorse presenti nel sistema**

Regole:

**specificano chi e come
può utilizzare le risorse**

Meccanismi:

strumenti per imporre le regole

Domini di protezione (1)

Risorse:

- risorse fisiche:
CPU, memoria centrale, periferiche
- risorse informative:
file, strutture di comunicazione e
sincronizzazione tra processi, ...

Caratterizzazione delle risorse:

- identificativo
- insieme di operazioni

Domini di protezione (2)

Principio di minima conoscenza

Un processo deve accedere solo alle risorse strettamente necessarie per effettuare la propria computazione

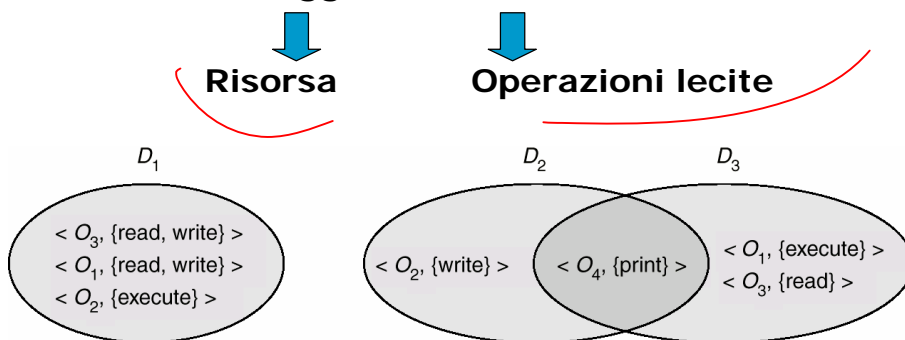
Domini di protezione (3)

**Un dominio di protezione
definisce
un insieme di risorse
e le relative operazioni lecite
per un processo che venga autorizzato
ad accedere a tale dominio**

Domini di protezione (4)

Struttura dei domini di protezione

Dominio = <Oggetto, Diritti>



Associazione processo-dominio

- Associazione statica
- Associazione dinamica
 - cambio di dominio
 - modifica dominio

Cambiamento di dominio

**Un processo può cambiare
dominio di protezione
se possiede i diritti ad effettuare
tale operazione**

Revoca dei diritti d'accesso

Revoca:

- immediata o ritardata
- selettiva o generale
- parziale o totale
- temporanea o permanente

In sintesi

- Concetto di protezione
- Domini di protezione
- Operazioni sui domini di protezione

SISTEMI OPERATIVI

File System
Protezione

Lezione 2 – Tecniche di realizzazione della protezione

Vincenzo Piuri

Università degli Studi di Milano - SSRI - CDL ONLINE

Sommario

- Matrice d'accesso
- Liste di controllo degli accessi
- Liste di capacità dei domini

Realizzazione dei domini di protezione

Rappresentazione

- Matrice degli accessi

Implementazioni

- Matrice completa
- Liste di controllo degli accessi
- Liste di capacità dei domini
- Meccanismo serrature-chiavi (lock-key)

Matrice d'accesso

dominio \ oggetto	F_1	F_2	F_3	stampante
D_1	leggi		leggi	
D_2				stampa
D_3		leggi	esegui	
D_4	leggi scrivi		leggi scrivi	

Matrice d'accesso con domini

dominio \ oggetto	F_1	F_2	F_3	stampante laser	D_1	D_2	D_3	D_4
D_1	leggi		leggi			switch		
D_2				stampa			switch	switch
D_3		leggi	esegui					
D_4	leggi scrivi		leggi scrivi		switch			

Matrice di accesso con diritti di copia

dominio \ oggetto	F_1	F_2	F_3
D_1	esegui		scrivi*
D_2	esegui	leggi*	esegui
D_3	esegui		

Prima della copiatura

Dopo la copiatura

dominio \ oggetto	F_1	F_2	F_3
D_1	esegui		scrivi*
D_2	esegui	leggi*	esegui
D_3	esegui	leggi	

Matrice di accesso con diritti di proprietà

oggetto \ dominio	F_1	F_2	F_3
D_1	proprietario esegui		scrivi
D_2		leggi* proprietario	leggi* proprietario scrivi*
D_3	esegui		

Prima della copiatura

Dopo la copiatura

oggetto \ dominio	F_1	F_2	F_3
D_1	proprietario esegui		
D_2		proprietario leggi* scrivi*	leggi* proprietario scrivi*
D_3		scrivi	scrivi

Uso della matrice di accesso

Raccoglie tutte le informazioni sui diritti di uso

Supporta meccanismi di protezione dinamica

Liste di controllo degli accessi

Per ogni risorsa viene conservata la lista dei diritti per ogni dominio

risorsa: { <dominio,diritto> }

oggetto \ dominio	F_1	F_2	F_3	stampante laser	D_1	D_2	D_3	D_4
D_1	leggi		leggi		switch			
D_2				stampa		switch	switch	
D_3		leggi	esegui					
D_4	leggi scrivi		leggi scrivi		switch			

Liste di capacità dei domini

Per ogni dominio viene conservata la lista dei diritti per ogni risorsa

dominio: { <risorsa,diritto> }

oggetto \ dominio	F_1	F_2	F_3	stampante laser	D_1	D_2	D_3	D_4
D_1	leggi		leggi		switch			
D_2				stampa			switch	switch
D_3		leggi	esegui					
D_4	leggi scrivi		leggi scrivi		switch			

Revoca dei diritti (1)

Lista di controllo degli accessi

- Rimuovere i domini e/o i diritti dalla lista della risorsa
- Revoca immediata
- Revoca generale o selettiva
- Revoca totale o parziale
- Revoca permanente o temporanea

Revoca dei diritti (1)

Liste delle capacità dei domini

- Diritti sparsi nelle liste
- Riacquisizione
- Puntatori alle capacità
- Indirizione
- Chiavi

Confronto

Liste di controllo degli accessi

- Possono essere specificate dagli utenti
- Informazioni globali
- Inefficienti su grandi sistemi

Liste delle capacità dei domini

- Relative agli oggetti
- Informazioni localizzate
- Revoca inefficiente

Meccanismo serratura-chiave

lock-key

Serratura e chiave definite da stringhe di bit

**Il processo può eseguire
una operazione su una risorsa
se la sua chiave
combacia
con la serratura
per l'operazione indicata**

Sistemi operativi basati sulle capacità

Mettono a disposizione un approccio nativo all'uso di risorse basato sulle capacità

- Utenti possono definire e controllare capacità

Protezione basata sul linguaggio ⁽¹⁾

Protezione può essere incorporata nel linguaggio di programmazione

- Gestione affidata al compilatore
- Riferimenti verificati in fase di compilazione o in esecuzione

Protezione basata sul linguaggio (2)

Controllo più granulare

- Progettista (meccanismi, regole base)
- Amministratore (politiche)
- Utente/programmatore (diritti aggiuntivi)

Rispetto ad una protezione basata sul kernel:

- minor sicurezza
- maggior flessibilità
- maggior efficienza

In sintesi

Abbiamo visto:

- Matrice d'accesso
- Liste di controllo degli accessi
- Liste di capacità dei domini

Notiamo che:

- Alcuni sistemi permettono all'utente di definire diritti aggiuntivi
- Linguaggi di programmazione orientati alla protezione permettono una granularità più fine dei diritti d'accesso