MS WINDOWS II

Jádro

Správa objektů

Správa procesů

Zabezpečení

Správa paměti

JÁDRO I

- ntoskrnl.exe
- napsán v C (příp. assembler)
- základní mechanismy poskytované executivám
  - trap dispečink
  - synchronizace přístupů
  - plánování vláken

JÁDRO II

Trap dispečink

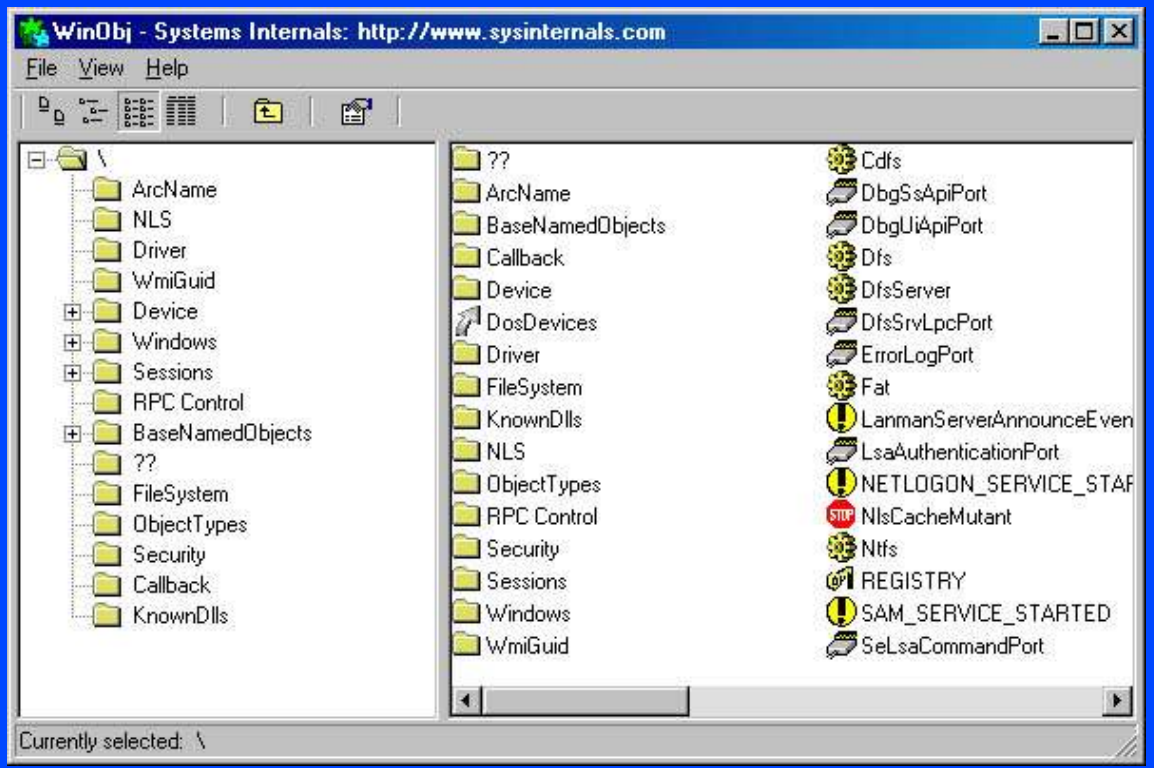
- HW a SW přerušení
- HW a SW výjimka
- volání systémové služby

procesor vykonává instrukce mimo svůj běžný instrukční tok, stav před přerušením uložen na zásobník

SPRÁVA OBJEKTŮ I

Objekt

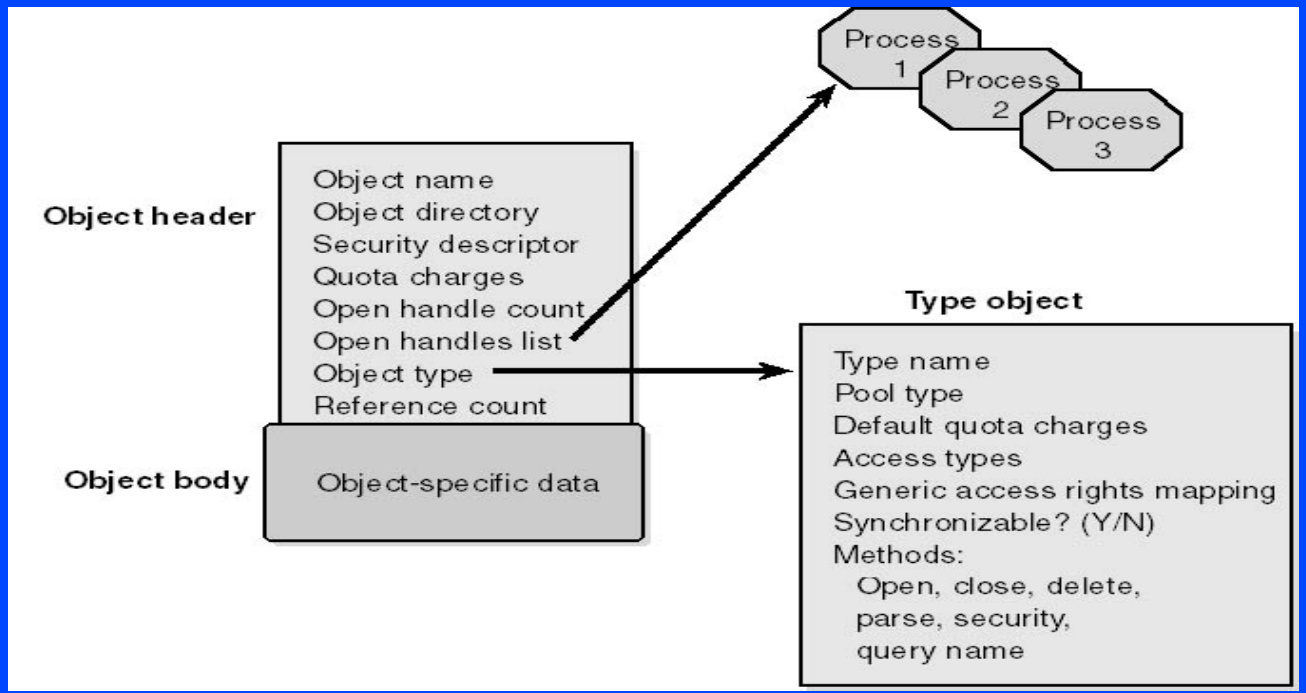
- samostatná jednotka obsahující data a metody pro práci s nimi
- proces, vlákno, soubor, registr.., příp. vlastní



SPRÁVA OBJEKTŮ II

Správce objektů

- jednotný přístup, bezpečnost objektů
- spravuje hlavičku objektu, zatímco vlastník tělo
- procesy žádají o handle objektu
- kontrola přístupových práv



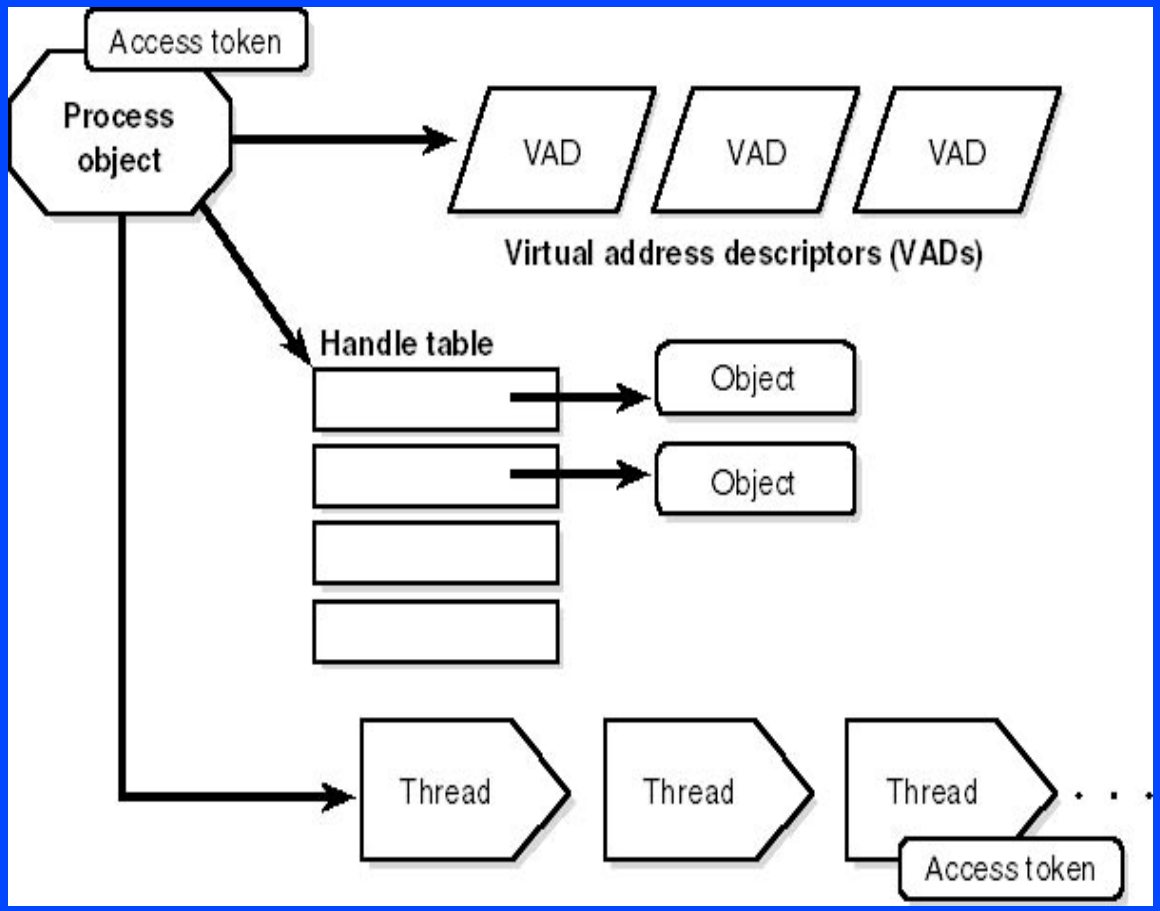
SPRÁVA PROCESŮ I

Program – statická sekvence instrukcí

Proces – kontejner pro sadu zdrojů užitých vlákny

- ID procesu, ID rodičovského procesu
- virtuální adresový prostor
- bezpečnostní kontext
- tabulka handlů
- kernel blok
- spustitelný program
- min. jedno vlákno

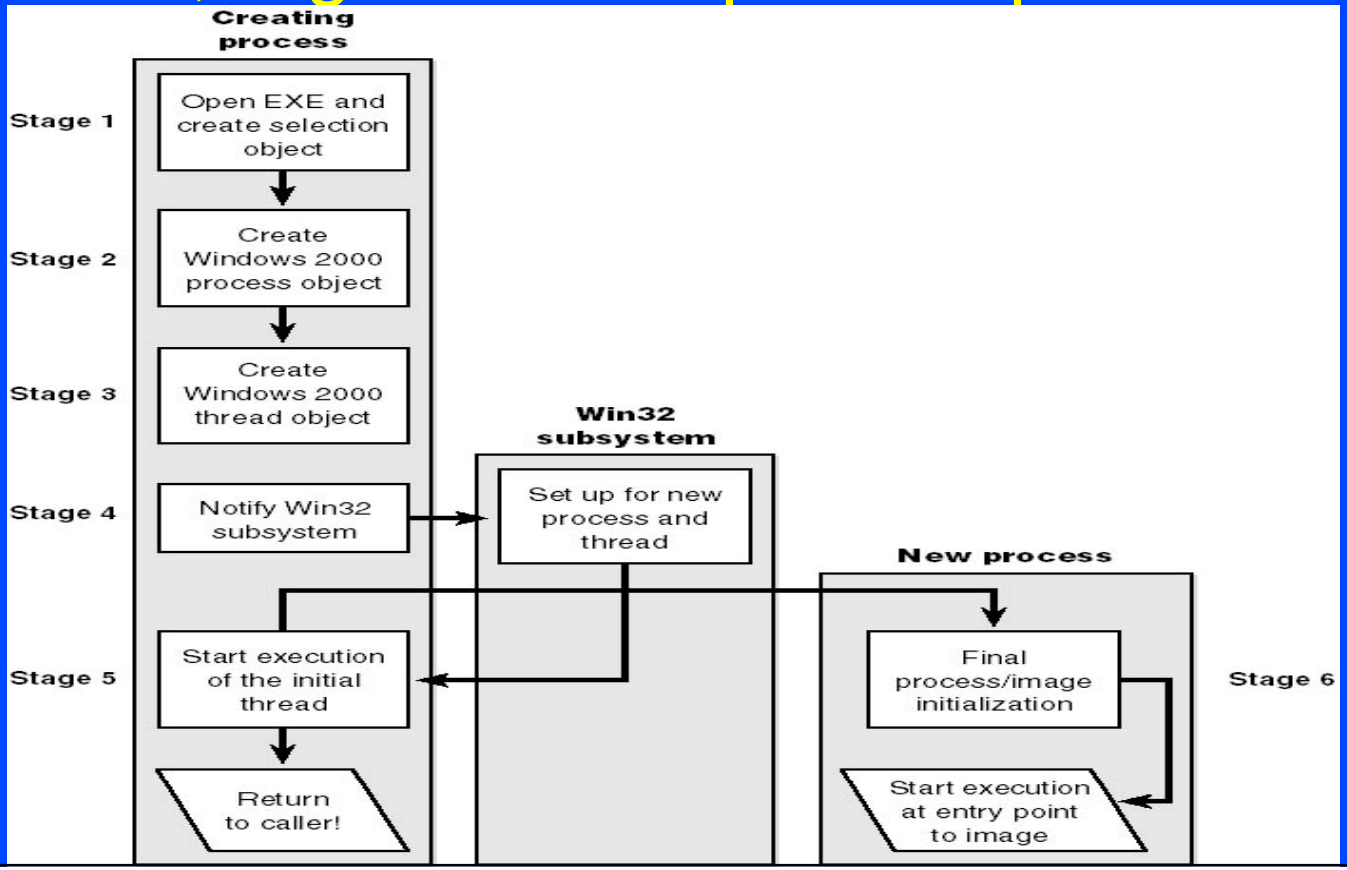
SPRÁVA PROCESŮ II



SPRÁVA PROCESŮ III

Vznik procesu

- CreateProcess, otevření image souboru
- vytvoření a registrace objektu proces
- vytvoření, registrace a spuštění poč. vlákna



SPRÁVA PROCESŮ IV

Vlákno – entita v procesu plánovaná ke spuštění

- ID vlákna, ID rodičovského procesu
- obsah CPU registrů a zásobníku
- bezpečnostní kontext
- kernel blok
- místní úložiště vlákna

vlákno sdílí paměť rodičovského procesu, příp. sdílenou paměť jiného procesu

SPRÁVA PROCESŮ V

Vznik vlákna

- CreateThread
- vytvoření a registrace objektu vlákno
- vytvoření HW kontextu
- vrácení ID a handlu volajícímu programu
- naplánováno ke spuštění

Plánování vláken

- kernel dispečer
- preemptivní, řízené prioritou
- přidělení časového kvanta
- přepnutí kontextu, spuštění dalšího vlákna

SPRÁVA PROCESŮ VI

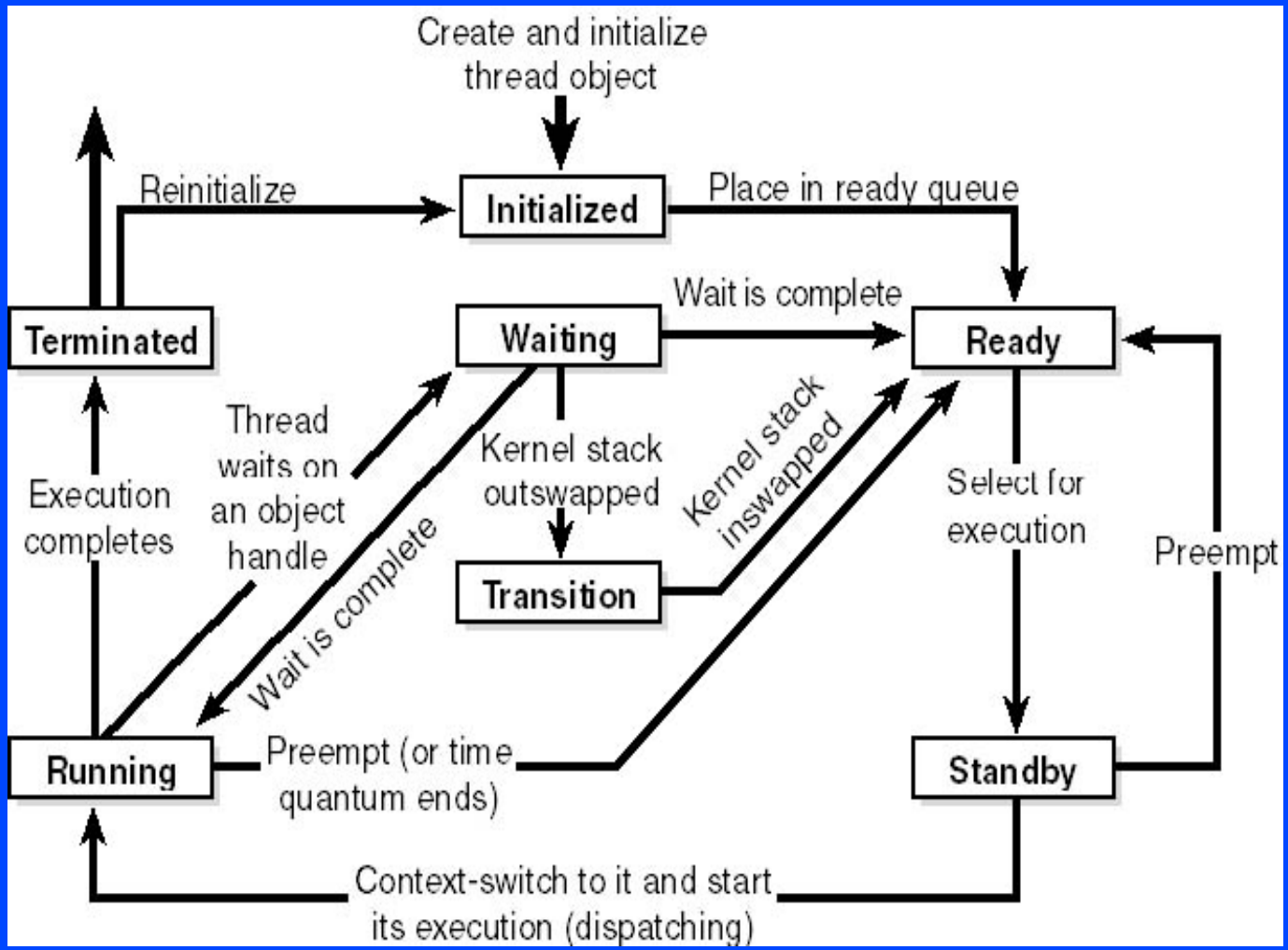
Priorita
- 0-32
- priorita procesu + relativní priorita
- fronty priorit
- podpora hladovějících vláken

Kvantum
- různá délka, snižuje se při přerušení hodinami

Spuštění dispečera
- vlákno se dostalo do stavu Ready
- vlákno opouští stav Running
- vlákno změnilo svou prioritu

SPRÁVA PROCESŮ VII

Stavy procesu



SPRÁVA PROCESŮ VIII

Úloha

- sdružuje několik procesů se všemi potomky
- spravována,manipulována jako ucelená jednotka
- společná identita
- nastavení limitů procesoru

Prohlížení procesů – task manager, tasklist..

ZEBEZPEČENÍ I

SID

- bezpečnostní identifikátor
- unikátní číslo proměnné délky
- počítač jej získává při instalaci, pak vytváří SIDy dalších účtů přidáním RID

- př. S-1-5-21-1463437245-1224812800-863842198-1128
- př. 500 – administrátor, 501 – guest
- př. S-1-0-0 – everyone, S-1-2-0 – local, S-1-5-2 - network

ZABEZPEČENÍ II

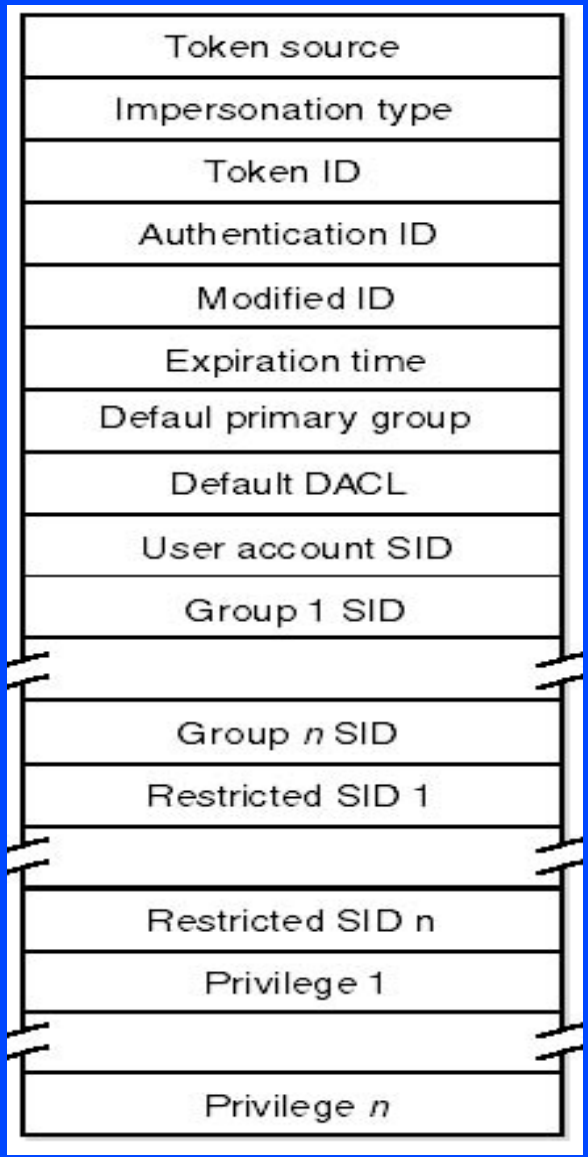
Access token

- přidělen každému procesu, jeho vlákna jej dědí
- seznam SIDů, seznam privilegií
- restrikce
- výchozí nastavení
- různá délka

Impersonifikace

- např. v modelu klient/server
- úroveň lze omezit

ZABEZPEČENÍ III



ZABEZPEČENÍ IV

Security Descriptor

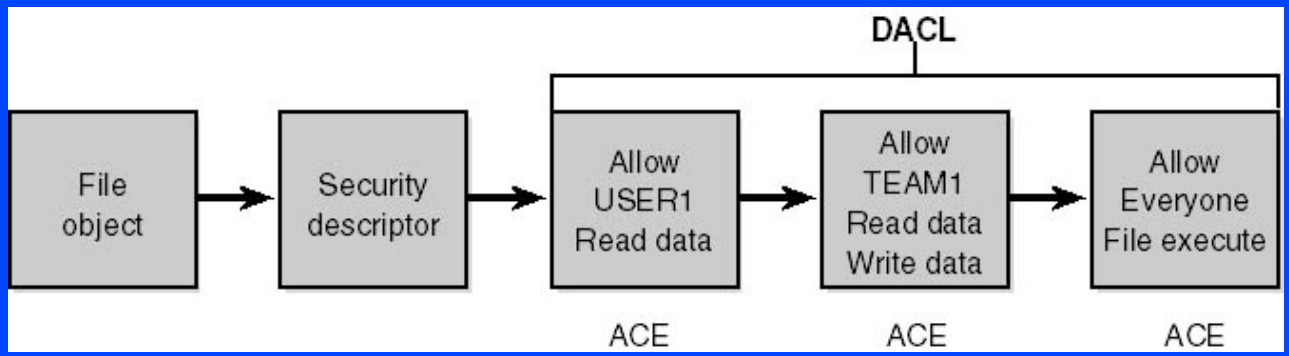
- nastavení práv na straně objektu
- dědění, SID vlastníka, DACL, SACL

ACL (Access Control List)

- seznam záznamů ACE

ACE (Access Control Entry)

- SID a jemu přidělená práva



ZABEZPEČENÍ V

Prázdný ACL – žádná práva pro nikoho
Žádný ACL – plná práva pro všechny

Vlastník – vždy právo na zápis DACL
Administrátor – vždy privilegium převzít vlastnictví

Přidělení ACL objektu

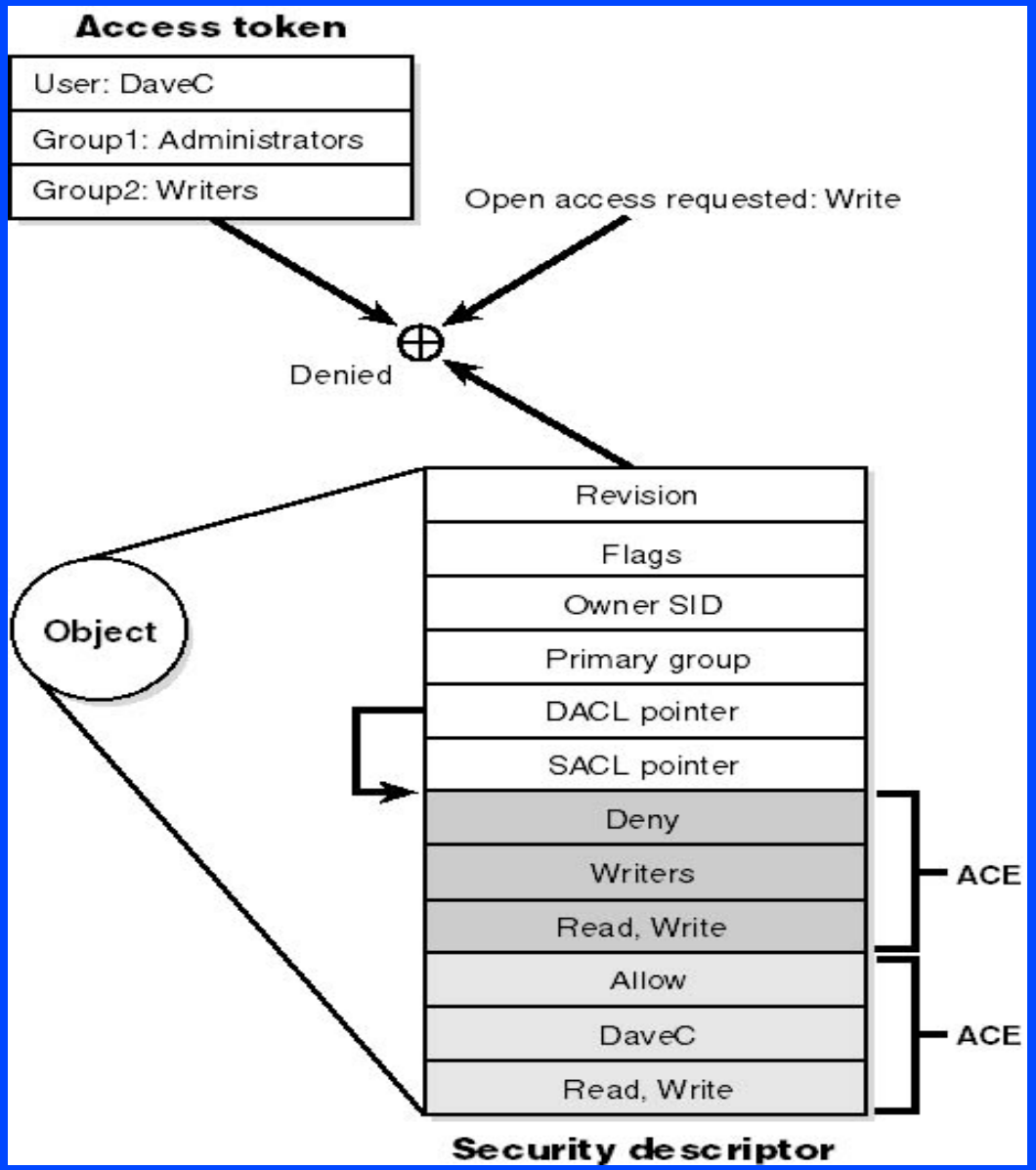
- explicitní
- zděděný
- výchozí
- žádný

ZABEZPEČENÍ VI

Přístup procesu k objektu

- žádost správci objektů (jméno objektu, access token, druh přístupu)
- ověření identity procesu proti DACL objektu
- přidělení handlu, zapsán do procesu
- při příštím přístupu již bez kontroly

ZABEZPEČENÍ VII



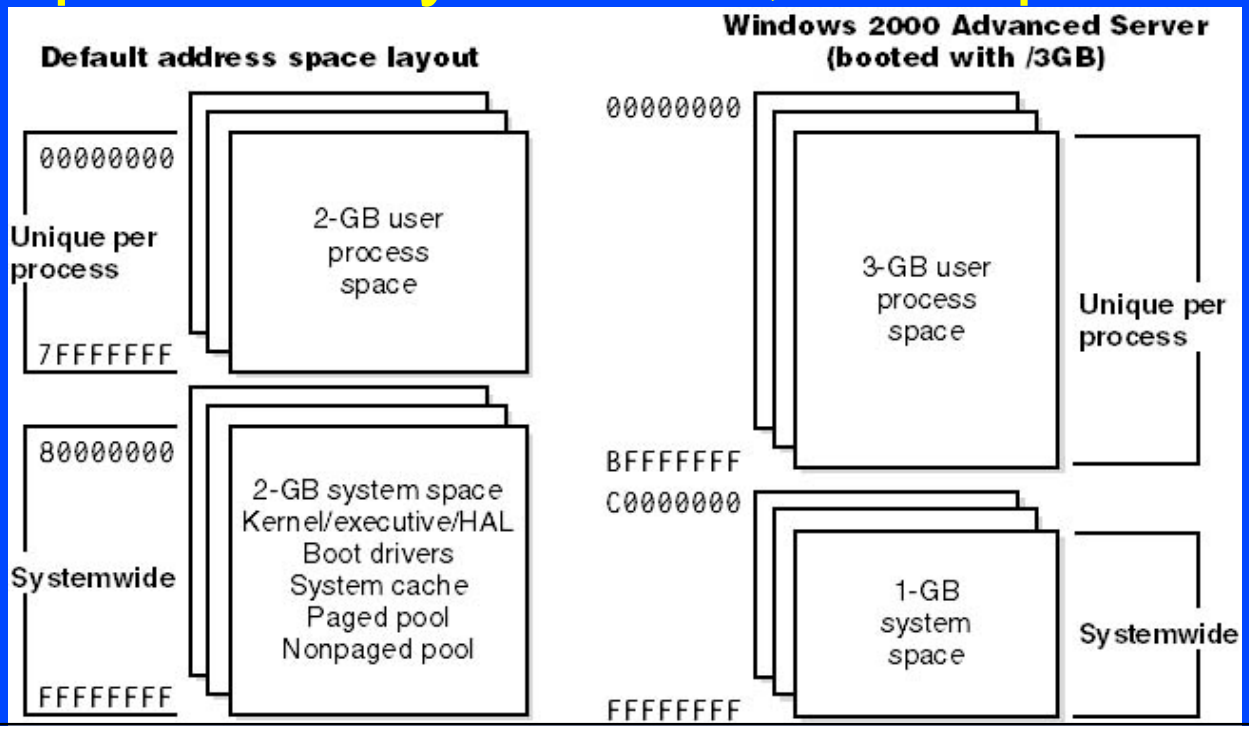
SPRÁVA PAMĚTI I

Fyzická paměť

- 32b lineární adresace

Virtuální paměť

- skupina adres dostupných vláknům procesu
- spodní polovina systémová, horní privátní



SPRÁVA PAMĚTI II

Stránka

- souvislá oblast paměti
- řízená HW ochrana (read-only, execute..)

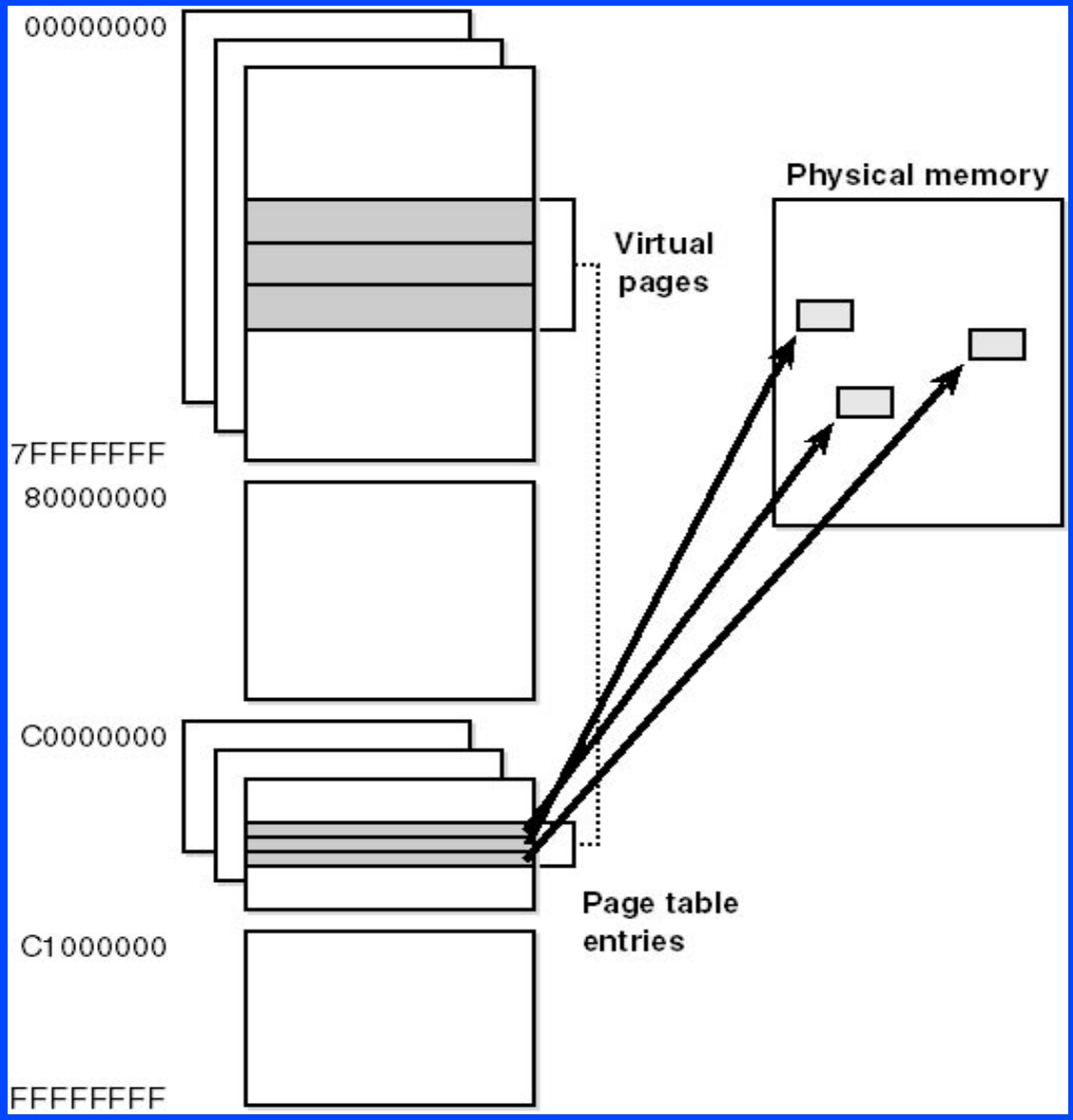
Swapování

- odkládání stránek na disk
- některé stránky se nikdy neswapují (nonpaged pool)

Překlad adres

- z virtuálních na fyzické
- vykonává procesor podle struktur OS
- kontrola přístupu

SPRÁVA PAMĚTI III



SPRÁVA PAMĚTI IV

Správce paměti

- součást Windows executive
- správa a alokace paměti
- obsluha chyb při překladu a přístupu
- „úklid“ paměti
- swapování
- správa cache, stránkovacích struktur..

nastavení správy paměti – registr HKLM
prohlížení paměti – taskmanager

univerzální nástroj (procesy, vlákna, objekty..) – process explorer (www.sysinternals.com)