17. Stránkování, segmentace, stránkování a segmentace, Reálný a chráněný režim – rozlišení stránky a segmentu, popis, vysvětlení, použití reálného chráněného režimu, jejich porovnání, adresace, přerušení.

Rozlišení stránky a segmentu

Stránka

- Pevně daný blok paměti s přesným počtem řádků.
- Délka stránky se v celé paměti nemění.

Segment

- Virtuální adresní prostor různé velikosti začínající od (virtuální) adresní nuly.
- Každý segment může mít různá přístupová práva (kódový segment jen pro spuštění, do zásobníkového segmentu může přistupovat jen jeden proces atp.).

Reálný a chráněný režim

Reálný režim

Popis

- Základní režim mikroprocesorů z rodiny x86.
- Název odvozen od skutečnosti, že adresy v reálném režimu odpovídají skutečným umístěním v paměti.
- Reálný režim neposkytuje podporu ochrany paměti, multitaskingu ani privilegovaný režim.

Vysvětlení

- Typickými vlastnostmi režimu reálných adres je segmentace paměti s 20bitovou adresací (tedy nanejvýš 1 MiB přímo adresovatelné paměti) a neomezený přímý přístup do celé paměti i ke všem periferiím.
- Nelze tedy zajistit spolehlivé fungování multitaskingu.

Použití

- V režimu reálných adres pracuje například BIOS a také v něm pracoval operační systém DOS (MS-DOS, DR-DOS, atd.) a dokonce i nejstarší verze Microsoft Windows (Windows 3.0 už běžel i v chráněném režimu).
- Prakticky všechny moderní operační systémy na osobních počítačích (unixové systémy v čele s Linuxem, OS/2, systémy Microsoft Windows z řady Windows NT a novější, atd.) vstupují do chráněného režimu hned při startu jádra operačního systému.

Adresace

- Adresa je v režimu reálných adres určena dvěma registry, a to segmentovým a offsetovým.
- Fyzická adresa je vypočítána jako součet hodnoty v segmentovém registru vynásobené 16 (tedy posunuté o 4 bity doleva) a hodnoty v offsetovém registru.
- Dík přenosu tak může být výsledek až 21bitové číslo: šestnáctkově 0xFFFF0 + 0xFFFF = 0x10FFEF.

- Pro 21. bit bylo do standardu IBM PC zavedeno rozšíření, které umožňovalo 21. adresní bit aktivovat řadičem klávesnice.
- Na procesorech Intel 80286 a novějších, které měly širší adresní sběrnici, bylo toto chování emulováno softwarově.
- Adresy nad hranicí 1 MiB (přesněji do adresy 1 MiB + 64 KiB – 16 B, tj. do adresy 1114095) byly označovány jako HMA (high memory area) a bylo do nich možné umístit například část systému DOS a uvolnit tak místo konvekční paměti.

Chráněný režim

Popis

= režim chráněné virtuální paměti

- Speciální operační režim mikroprocesorů rodiny x86.
- Umožňuje v počítači například zajistit, že spuštěný program (tj. proces) nemůže zasahovat mimo svůj vymezený prostor (tj. nemůže zasahovat ani do jiných procesů ani od jádra operačního systému).

Vysvětlení

- Chráněný režim přináší ve schopnostech mikroprocesorů několik nových vlastností, které dohromady umožňují naprogramovat moderní operační systém.
- Od moderních systémů provozovaných jako desktop nebo server se požaduje, aby zajistili:
    - Spolehlivý běh počítače
    - Podporu běhu více úloh najednou (multitasking)
    - Spuštěné procesy se nemohou navzájem ovlivňovat (ať už záměrně nebo kvůli programátorské chybě)
    - Jádro operačního systému má plnou kontrolu nad činností počítače (vynucuje dodržování přidělených oprávnění)
- **Ochrana paměti**
    - Umožňuje přidělit běžícímu procesu určitý úsek operační paměti a znemožnit, aby mohl zasahovat mimo tento vymezený prostor.
    - Umožňuje tak multitasking.
- **Privilegovaný režim**
    - Zajišťuje, aby neprivilegované procesy nemohly měnit nastavení, provedená v privilegovaném režimu.
    - Jádro OS běží v privilegovaném režimu, proto může přidělovat a odebírat systémové prostředky jednotlivým procesům.
- **Virtualizace paměti**
    - Uvnitř jednoho systému lze provozovat jiný systém, který bude mít dojem, že má počítač jen pro sebe.

Použití

- Mezi operační systémy, které chráněný režim používají, patří všechny verze Microsoft Windows z řady Windows NT, mac OS, Linux (i Android, pokud běží na mikroprocesoru od firmy Intel), tedy všechny plně 32bitové systémy.
- Systém DOS je 16bitový a chráněný režim nepodporuje, ale mohou ho využívat některé jeho součásti (např. EMM386) nebo aplikace (např. Hra Doom nebo starší verze Microsoft Windows).

Adresace

- Logická adresa je složena z 16bitového selektoru a 32bitového offsetu (tj.adresuje se 64 TB virtuální paměti). Tato adresa je algoritmem segmentační jednotky převedena na lineární adresu.

Porovnání

Reálný režim	Chráněný režim
Využívá fyzické adresy	Využívá logické adresy
Nepodporuje privilegovaný režim	Podporuje privilegovaný režim
Nepodporuje Multitasking	Podporuje Multitasking
BIOS, DOS, starší verze Windows	Windows, Linux, macOS (chráněný režim hned po aktivaci jádra)

Přerušení

Vnitřní

Vyvolané procesorem

- Stat half – přerušení činností z důvodu chyby, nebo přehřátí.
- TF – krokovací režim

Vyvolané programem

- Uložení paměti do zásobníku a změna registru SP.

Externí

Maskovatelné

- IMT – interapt [přerušení], při stisknutí klávesy, požadavek tiskárny

Nemaskovatelné

- NMI – nonmaskableinterapt [nemaskovatelné přerušení], chyba paritního součtu
- Vyšší priorita než IMT.