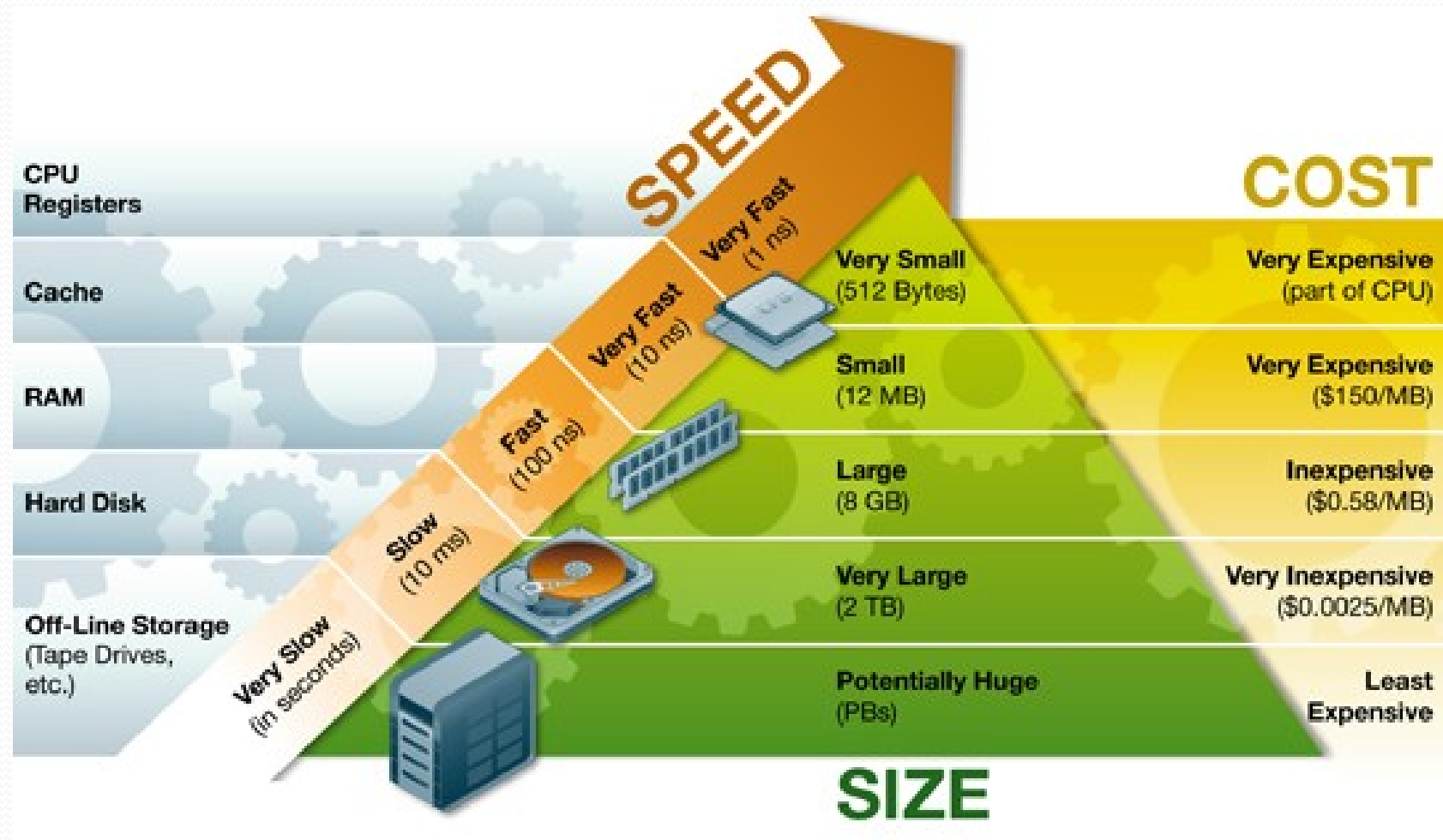


# Architektura počítačů

06

# Paměti

- Registry
- Cache
- Operační paměť
- Sekundární paměť
- Terciální paměť



# Základní parametry pamětí

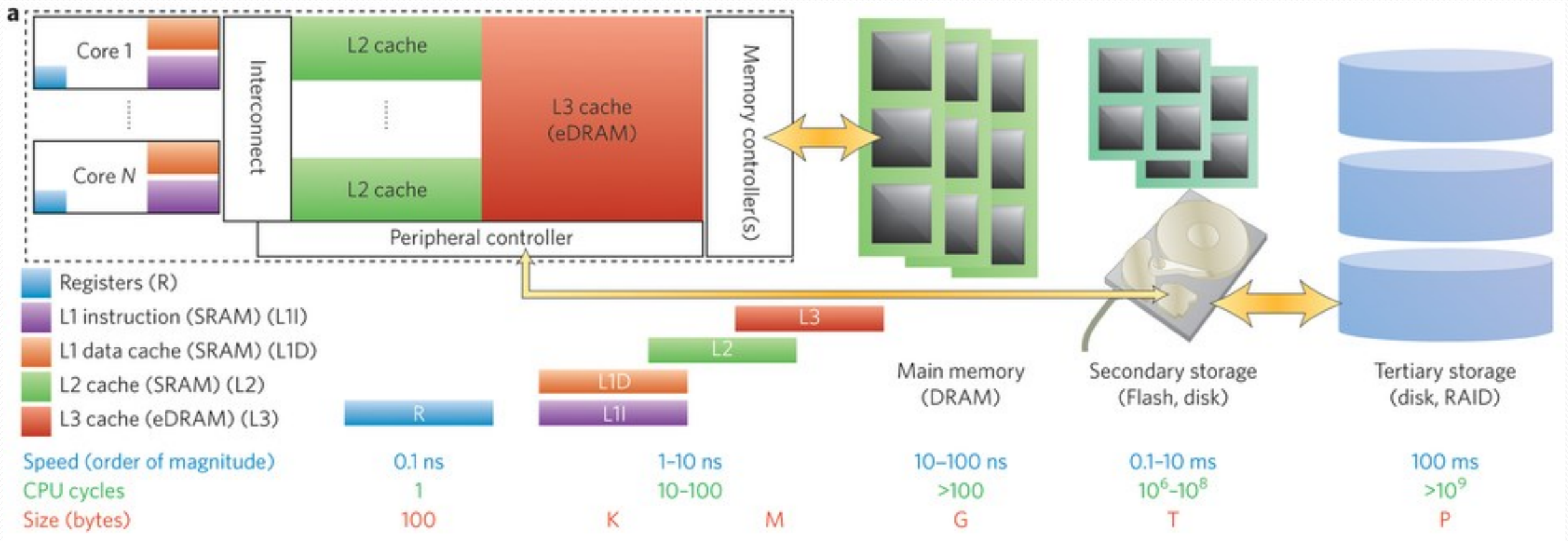
- kapacita
- přístupová doba
- přenosová rychlost
- statičnost / dynamičnost
- energetická závislost (Volatile/Non-volatile – závislé/nezávislé)
- přístup (sekvenční/přímý)
- destruktivnost při čtení
- spolehlivost
- cena za bit

# Parametry pamětí

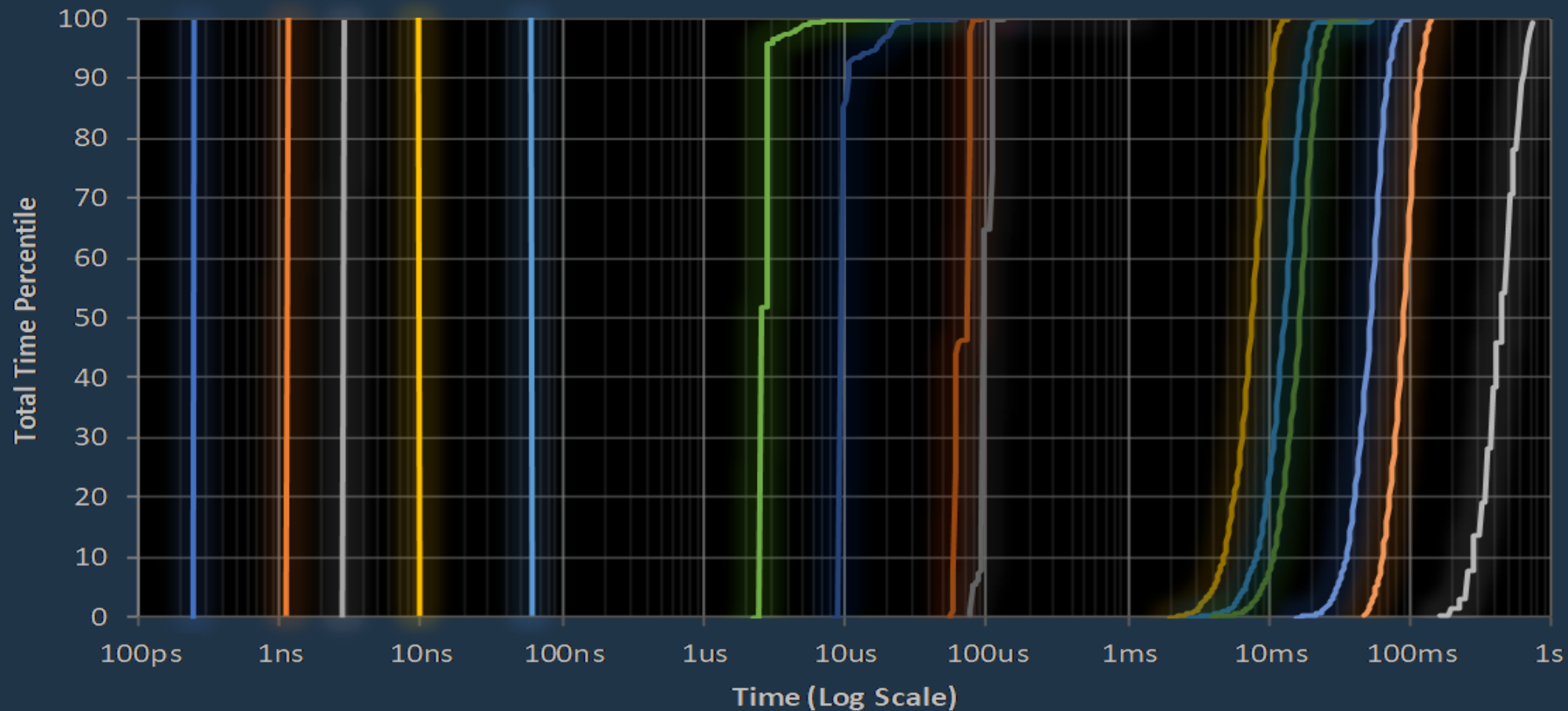
	registry	Vnitřní paměti	Vnější paměti
kapacita	Velmi malá	Výšší (MB)	Vysoká (GB)
přístupová doba	Nízká	nanosekundy	milisekundy
přenosová rychlost		Vysoká (GB/s)	Nižší (MB/s)
statičnost/ dynamičnost	Statické	Statické i dynamické	Statické
energetická závislost	Závislé	Závislé	Nezávislé
přístup	Přímý	Přímý	Přímý i sekvenční
destruktivnost při čtení	Nedestruktivní	Destruktivní i nedestruktivní	Nedestruktivní

# Hierarchie paměti

- Umístění/typ paměti/rychlost přístupu/kapacita



## Latency Percentile, 4KB Random Read - QD1



1 Clock Cycle (4 GHz)

L3 Cache (~100M IOPS)

Optane PCIe (100144 IOPS)

10K HDD (143 IOPS)

Zip 100 (20 IOPS)

L1 Cache (~800M IOPS)

DRAM (~17M IOPS)

NVMe SSD (14369 IOPS)

7.2K HDD (84 IOPS)

CD/DVD (10 IOPS)

L2 Cache (~333M IOPS)

RAMDISK (350682 IOPS)

SATA SSD (9939 IOPS)

5.4K HDD (65 IOPS)

Floppy (2 IOPS)



# Registry

- Paměťové bloky s velmi malou kapacitou
- Omezený počet; Velikost 8, 16, 32 či 64 bitů, i více
- Slouží pro ukládání mezivýsledků a informací nutných pro řízení činnosti procesoru
- Jedná o paměť využívanou prakticky všemi instrukcemi
- Přístupová doba odpovídá rychlosti jádra procesoru
- Mohou sloužit jako rychlá vyrovnávací paměť



# Registry

- Uživatelsky přístupné registry
  - datové, adresové, obecné a příznakové
- Systémové registry
  - registr masky přerušení,
  - registr počáteční adresy tabulky stránek,
  - registr režimu supervizor/uživatel
- Speciální vnitřní registry
  - čítač instrukcí, registr instrukcí,
  - paměťový datový buffer,
  - paměťový adresový buffer

Některé registry se sdružují do tak zvaného stavového slova procesoru (program status word, **PSW** )- zachycují stav CPU

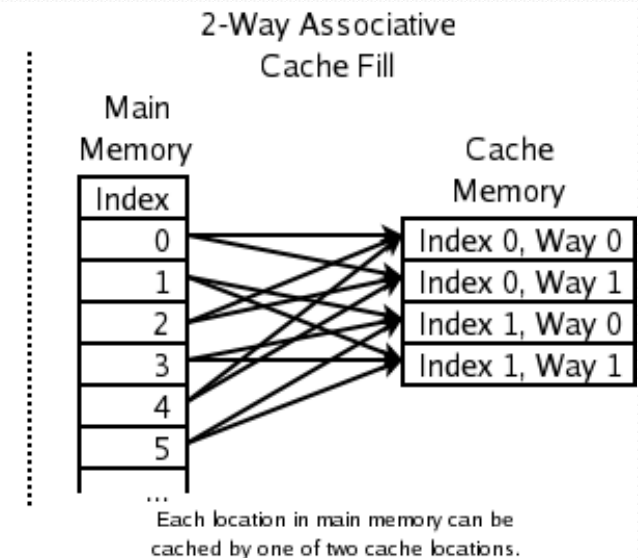
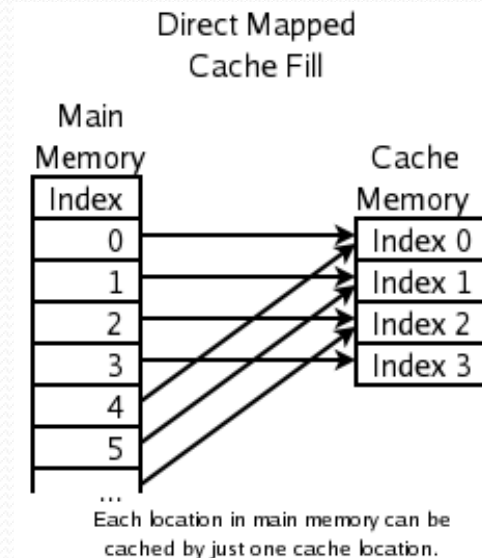


# Cache

- Paměť, která ukládá instrukce a/nebo data, aby mohly být budoucí požadavky obslouženy rychleji.
- V cache může být výsledek dřívějšího výpočtu nebo duplikát dat uložených jinde.
- Implementováno jako bloky paměti + tag (*cache lines*), např.  $64\text{B} \times 16384 = 1024\text{kiB}$
- základní přístupy zápisu:
  - **Write-through**: zápis se provádí synchronně jak do cache, tak do hlavní paměti.
  - **Write-back** (*write-behind*): zápis se provádí pouze do cache. Zápis do hlavní paměti je odložen, dokud nemají být data v cache nahrazena novým obsahem.
- cache hit - cache miss (Efektivita, Princip lokality)
- Asociativita vyrovnávací paměti (Přímo mapovaná, Asociativní, Dvoucestná, Čtyřcestná, ...)
- Úrovně vyrovnávací paměti
- Vyrovnávací paměť (Buffer vs. Cache)

# Asociativita cache

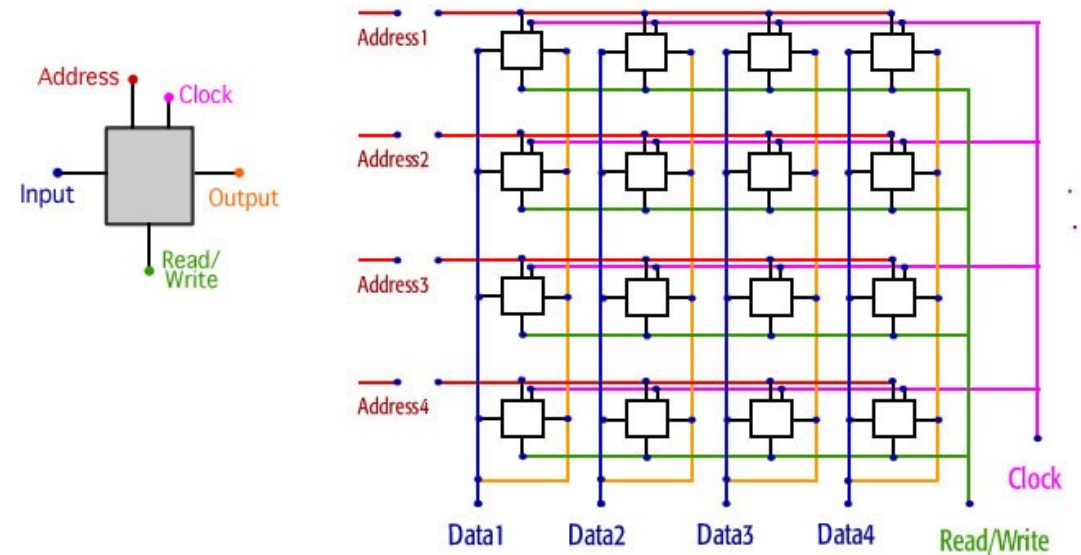
- Asociativita určuje způsob mapování bloků z RAM do *cache lines*.
  - Jakýkoli blok z RAM nemůže být obecně uložen kdekoli v cache.
- **přímo mapovaná** (*direct mapped cache*)
  - již přímo z indexu bloku (tj. nejvyšších bitů adresy) určuje, ve kterém místě se blok může nacházet - pozice bloku pevně dána jeho indexem.
- **Plně asociativní** (*fully associative cache*)
  - Blok se může nacházet kdekoliv
- **n-cestná** (*n-way set associative cache*)
  - n - je většinou 2, 4, 8, 16



# Vnitřní paměti

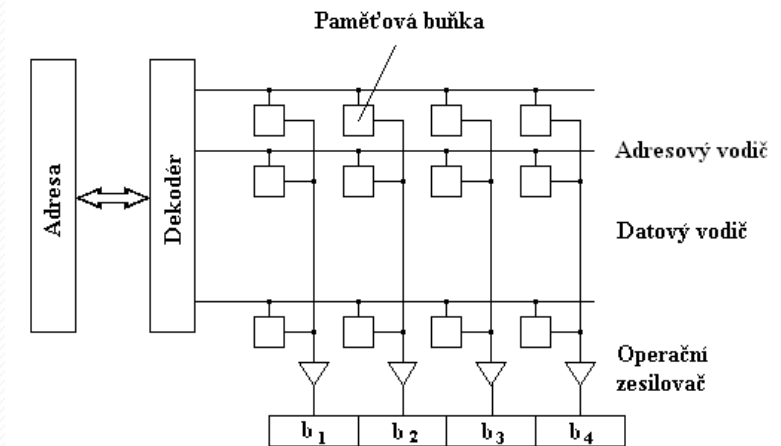
- matice paměťových buněk
  - Každá buňka má kapacitu jeden bit
    - hodnoty **log 1** a **log 0**
- Základní dělení vnitřních pamětí
  - RAM
    - SRAM
    - DRAM
  - ROM, PROM, EPROM, EEPROM, Flash EEPROM

## MEMORY MATRIX



# Přístup do paměti

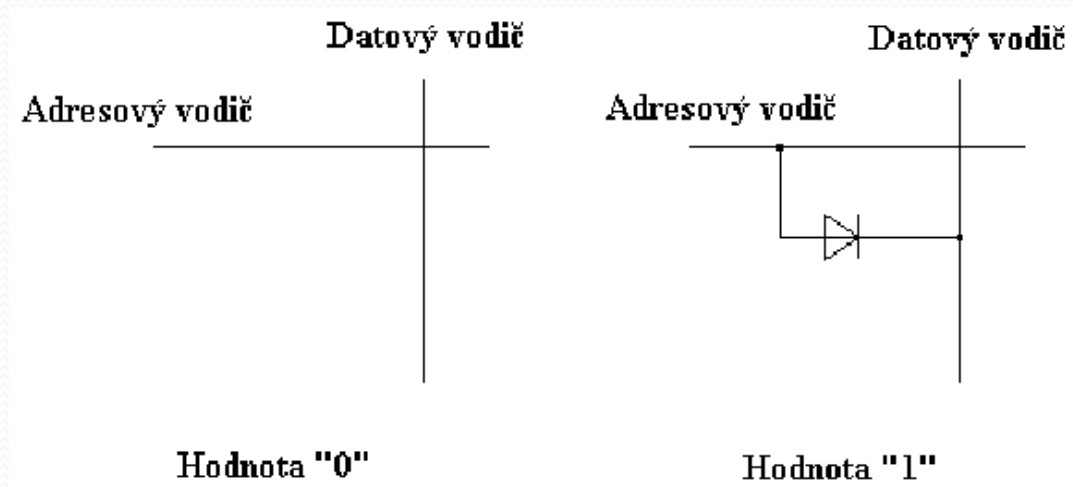
- Paměťové místo je adresováno
  - Adresa je přivedena na vstup dekodéru.
  - Dekodér pak podle zadané adresy vybere jeden z adresových vodičů a nastaví na něm hodnotu log 1.
  - Hodnota projde/neprojde paměťovou buňkou na datový vodič.
    - V případě, že hodnota logická jedna projde přes paměťovou buňku, obdržíme na výstupu hodnotu 1. V opačném případě je na výstupu hodnota 0.
- Jednotlivé typy pamětí se liší způsobem realizace buňky



# Paměti ROM

(Read Only Memory)

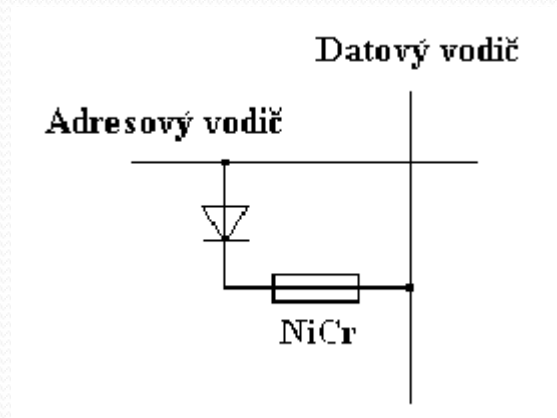
- určeny pouze pro čtení informací
- Informace pevně zapsány při jejich výroby
- potom již není možné obsah změnit



# Paměti PROM

(Programmable Read Only Memory)

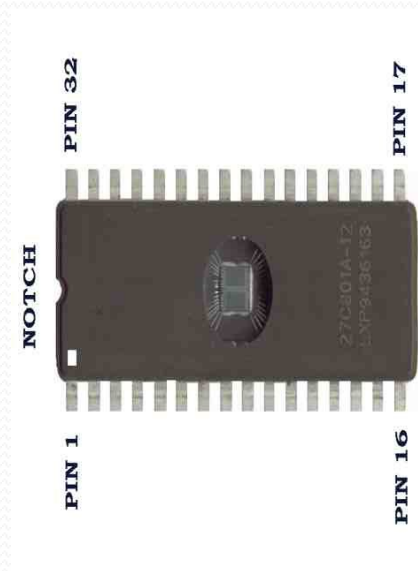
- Neobsahuje po vyrobení žádnou informaci
- Jedenkrát lze provést zápis informace
- poté paměť slouží stejně jako paměť ROM



# Paměti EPROM

## Eraseable Programmable Read Only Memory

- Lze provést zápis
- Informace lze vymazat působením UV
- realizovány pomocí unipolárních tranzistorů
  - schopny na svém přechodu udržet elektrický náboj po dobu až několika let
- Paměti EPROM jsou charakteristické malým okénkem v pouzdře integrovaného obvodu

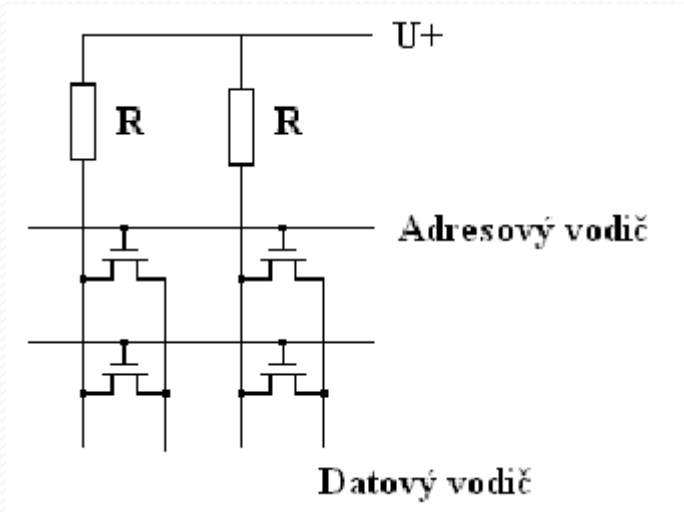




# Paměti EEPROM

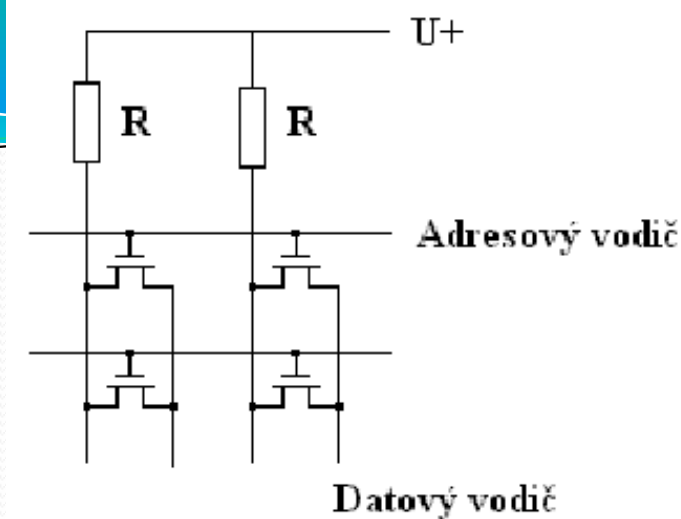
## Electrically EPROM

- podobné chování jako paměti EPROM
  - možné naprogramovat a později z ní informace vymazat
- vymazání se provádí elektricky



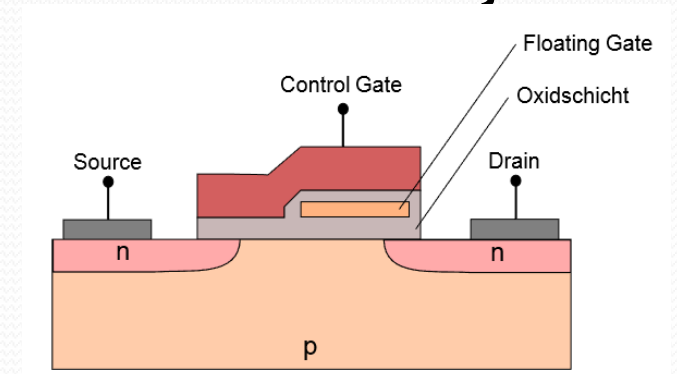
# Funkce EEPROM

- Zápis dat
  - přivede se na příslušný **adresový vodič** záporné napětí  $-U$
  - datový vodič buněk, do nichž se má zaznamenat hodnota 1, se uzemní.
    - Tranzistor se otevře a vznikne v něm náboj, který vytvoří **velké prahové napětí**.
- Čtení dat
  - přivede na adresový vodič záporný impuls.
  - Tranzistor s malým prahovým napětím se otevře a vede elektrický proud do datového vodiče, zatímco tranzistor s velkým prahovým napětím zůstane uzavřen.
- Vymazání paměti se provádí kladným napětím  $+U$ , které se přivede na adresové vodiče.
  - Tunelovaný náboj se tím zmenší a prahové napětí poklesne, čímž je paměť vymazána.

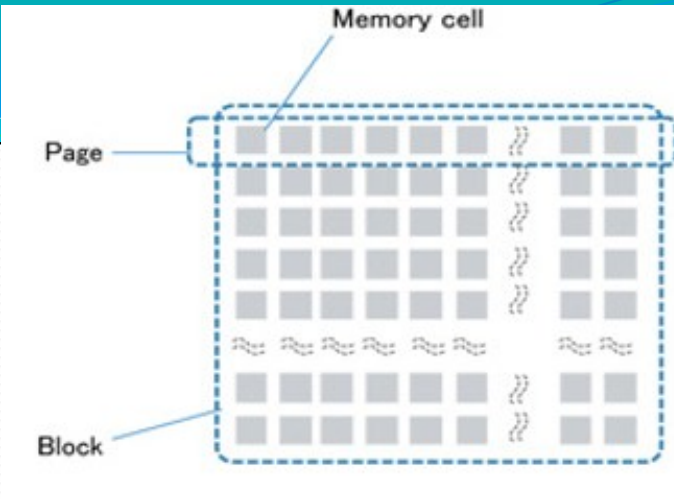
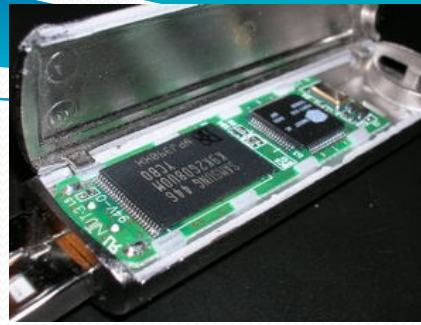


# Flash EEPROM

- Data jsou ukládána v poli unipolárních tranzistorů s plovoucími hradly, zvaných „buňky“ (cells)
- Ovládací hradlo (**CG** – control gate)
- Plovoucí hradlo (**FG** – floating gate)
  - Izolované od okolí vrstvou oxidu.
    - Všechny přivedené elektrony jsou zde „uvězněny“.
    - Tím je uložena informace.
- Elektrony na **FG**, modifikují (částečně ruší) elektrické pole přicházející z **CG**, což modifikuje prahové napětí ( $U_t$ ) buňky.
  - Čtení: el. napětí na **CG** -> průchod proudu překládáme jako Log 1



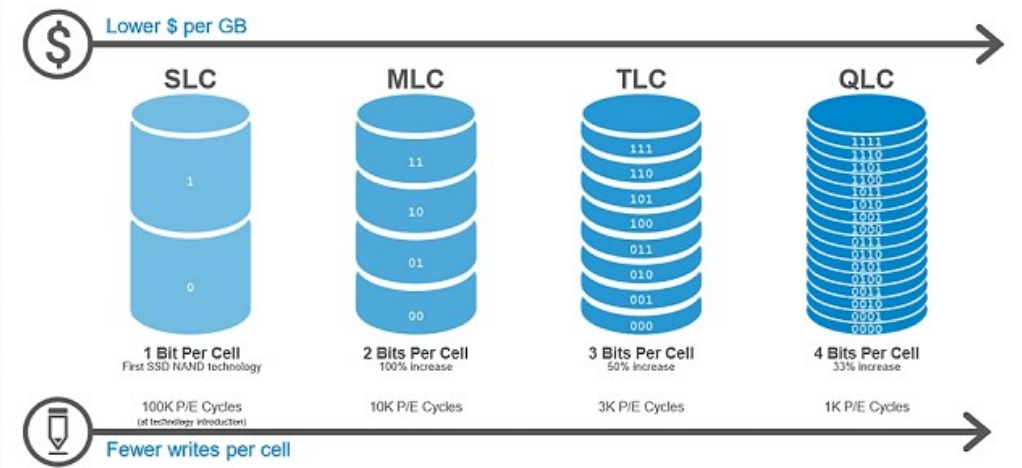
# Flash paměť



- **Obdoba pamětí EEPROM**

- Není možné přistupovat k jednotlivým buňkám (NAND)
- Zápis se provádí po celých stránkách (~2-16 kiB + ECC) a mazání po blocích (32-512 pages)
- Vymazání se provádí elektrickou cestou
  - přeprogramování je možné provést přímo v počítači

- **SLC - single-level cell** (pouze 1 bit)
- **MLC - multi-level cell** (2 bity)
- **TLC - triple-level cell** (3 bity)
- **QLC - quad-level cell** (4 bity)
  - Více úrovní elektrického náboje
    - 2 bity -> 4 stavy
    - 3 bit -> 8 stavů
    - 4 bit -> 16 stavů



<https://www.goplex.com/UploadFile/96972372091d42fb820a9e75454b79b7.jpg>

# Flash paměť - životnost

- SLC - single-level cell (pouze 1 bit)
  - MLC - multi-level cell (2 bity)
  - TLC - triple-level cell (3 bity)
  - QLC - quad-level cell (4 bity)
- 
- TBW (Terabytes Written)
  - Wear leveling

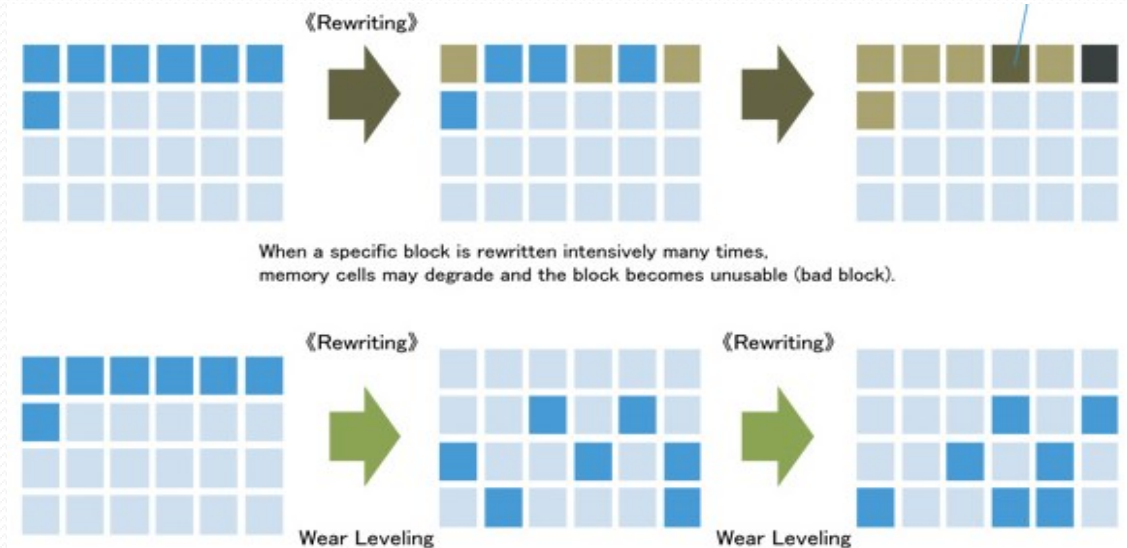
## počet přepisů

100 000

10 000

3 000

1 000



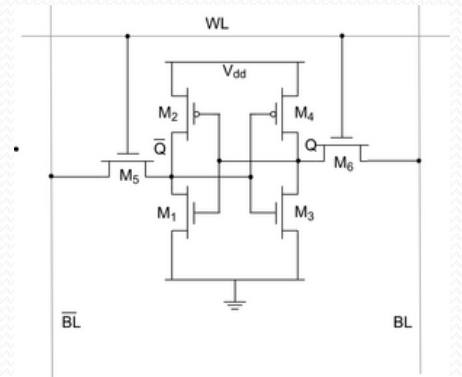
# Paměti RAM

## (Random Access Memory)

- Paměť s náhodným (přímým) přístupem
- **SRAM**
  - Static Random Access Memory
- **DRAM**
  - Dynamic Random Access Memory

# SRAM

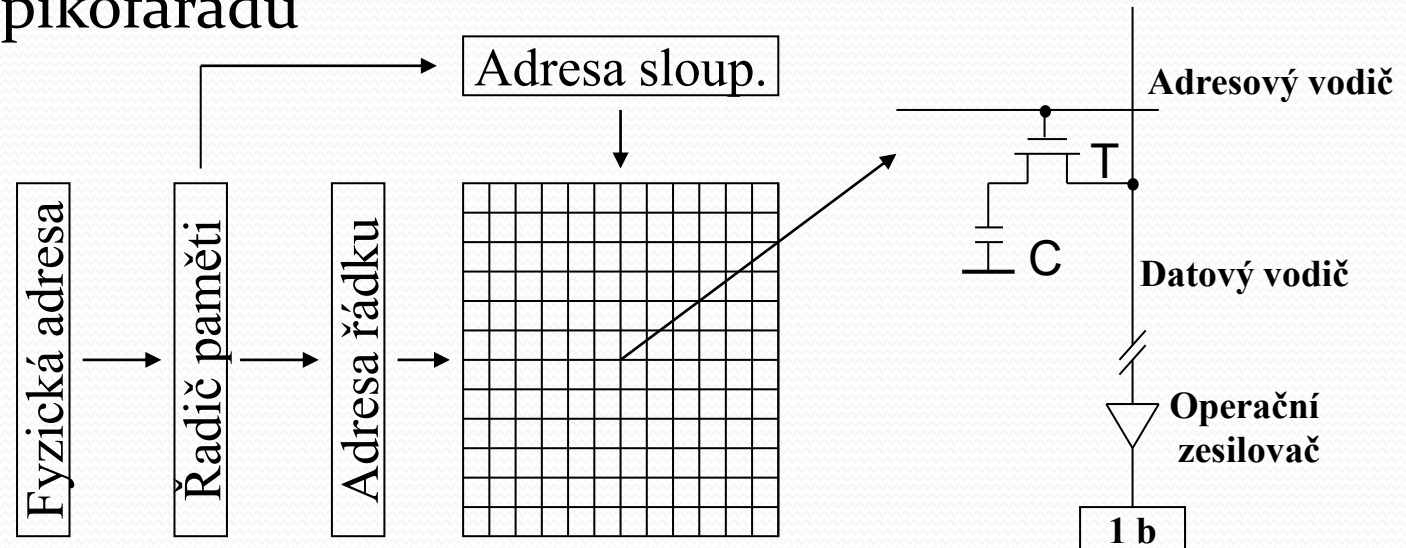
- Statická RAM (technologie CMOS)
- *Statická* - jednou zapsaný bit je v buňce držen po celou dobu
  - pokud se nepřeruší napájení čtení nebývá destruktivní
- bistabilní klopný obvod
  - Jeden ze dvou stavů - **log 1** nebo **log 0**
- nutnost použití 4-6 tranzistorů pro jednu paměťovou buňku
  - vyšší cena za jeden bit i větší plocha





# DRAM

- Dynamická RAM
- Každá buňka vytvořena z tranzistoru a kondenzátoru.
- Uchování informace pomocí náboje v kondenzátoru
  - (konkrétně na parazitní (Müllerově) kapacitě řídicího tranzistoru)
  - kapacita v řádu desetin pikofaradů



# Paměti DRAM

## Dynamic Random Access Memory

- Nabití kondenzátoru odpovídá uložení jednoho bitu
- Po přivedení Log 1 na řádkový vodič se všechny tranzistory v řádku matice otevřou a je možné zapisovat do paměťových buněk informace (nabíjet kondenzátory), popř. informace z buněk číst.
  - Při čtení se náboj přenesení do záchytných registrů
    - Kondenzátory se vybíjí, čtení je destruktivní operací.
    - Zápis je rychlejší jak čtení
- náboj má tendenci se vybíjet i v době, kdy je paměť připojena ke zdroji napájení
  - nutnost periodicky provádět tzv. **refresh**, tj. ožiování paměťové buňky - speciální obvod (při obnově je paměť nedostupná), 64 ms
    - Provádí se po celých řádcích
      - paralelně sejmuty obsahy buněk na řádku, v budiči zesíleny a opět zapsány na původní místo

# Typy DRAM

- Paměti typu **FPM** (Fast Page Mode)
- Paměti typu **EDO** (Extended Data Out)
- Paměti typu **Burst EDO** (BEDO)
- Paměti typu **RDRAM** (Ramubus)
- Paměti typu **SDRAM**
  - Synchronnous Dynamic RAM
- Paměti typu **DDR SDRAM**
  - Double Data Rate SDRAM
- Paměti typu **DDR<sub>2</sub> SDRAM**
- Paměti typu **DDR<sub>3</sub> SDRAM**
- Paměti typu **DDR<sub>4</sub> SDRAM**

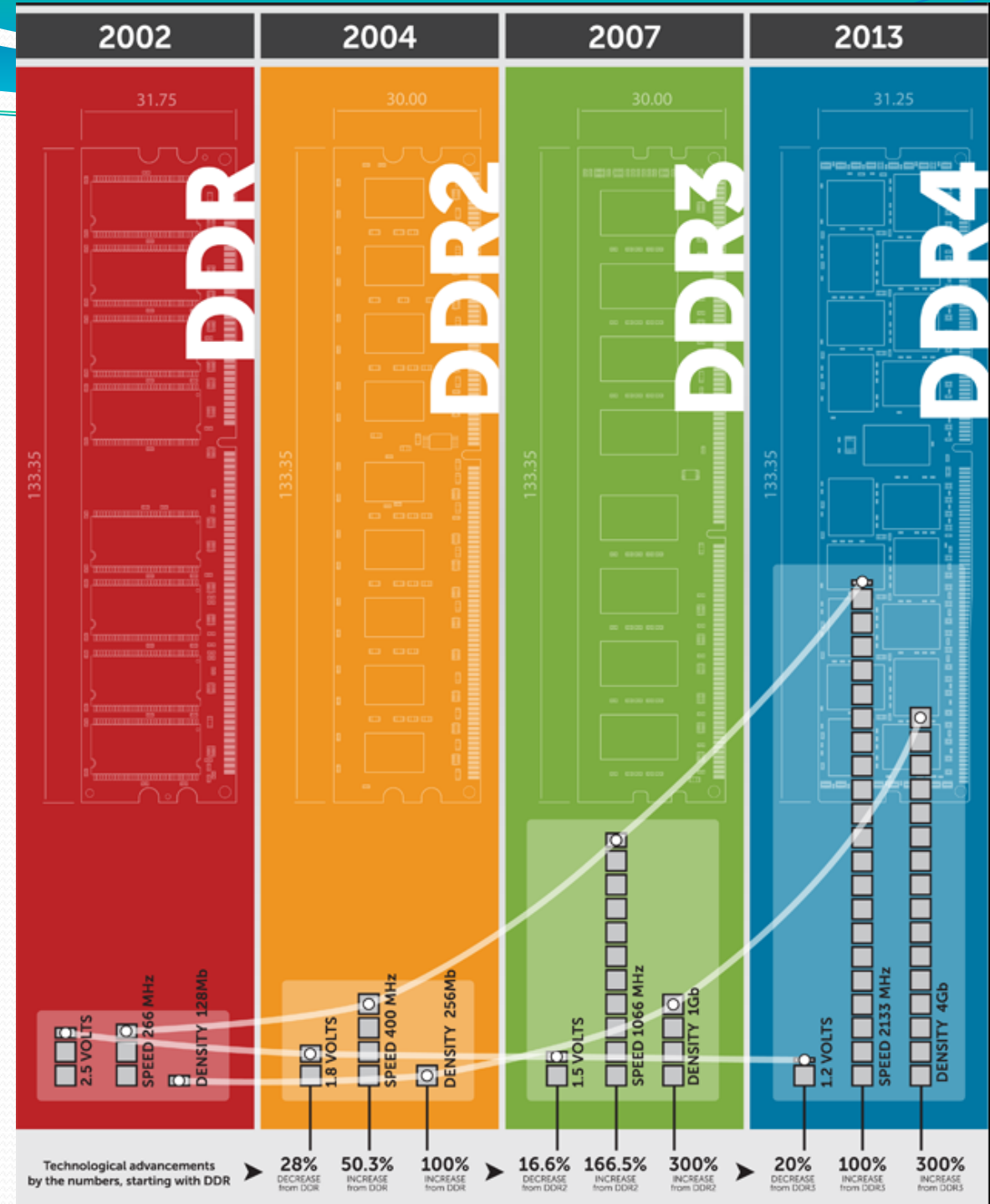
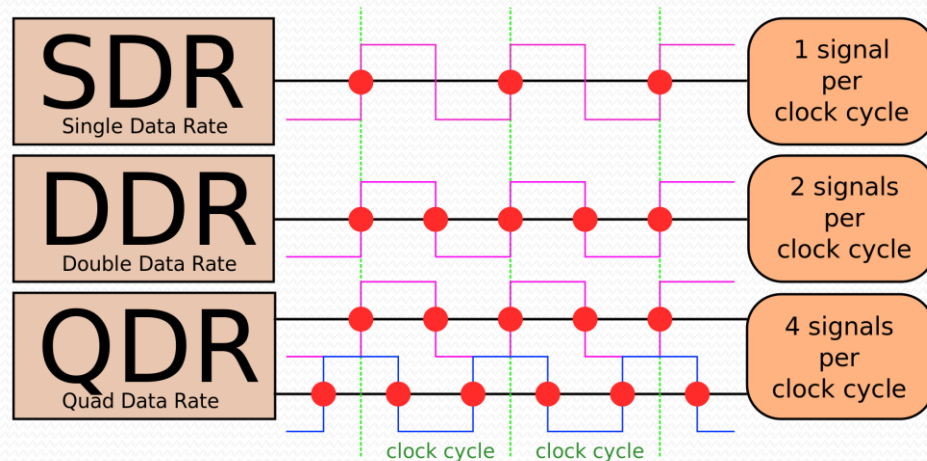
Memory Type	Years Popular	Desktop Module Type	Laptop Module Type	Voltage	Max. Clock Speed	Max. Throughput Single-Channel	Max. Throughput Dual-Channel	Max. Throughput Triple-Channel
Fast Page Mode (FPM) DRAM	1987–1995	30/72-pin SIMM	72/144-pin SODIMM	5V	22MHz	177MBps	N/A	N/A
Extended Data Out (EDO) DRAM	1995–1998	72-pin SIMM	72/144-pin SODIMM	5V	33MHz	266MBps	N/A	N/A
Single Data Rate (SDR) SDRAM	1998–2002	168-pin DIMM	144-pin SODIMM	3.3V	133MHz	1,066MBps	N/A	N/A
Double Data Rate (DDR) SDRAM	2002–2005	184-pin DIMM	200-pin SODIMM	2.5V	400MTps	3,200MBps	6,400MBps	N/A
DDR2 SDRAM	2005–2009	240-pin DDR2 DIMM	200-pin SODIMM	1.8V	1,066MTps	8,533MBps	17,066MBps	N/A
DDR3 SDRAM	2009–2015	240-pin DDR3 DIMM	204-pin SODIMM	1.5V	2,133MTps	17,066MBps	34,133MBps	51,200MBps
DDR4 SDRAM	2015+	284-pin DDR4 DIMM	256-pin SODIMM	1.2V	4,266MTps	34,133MBps	68,266MBps	102,400MBps

# SDRAM (Synchronní dynamické RAM)

- Synchronní paměti používají hodinový signál a podpůrné obvody
  - Asynchronní paměti - všechno běželo svou maximální rychlostí
- Paměťový čip má svoji vlastní „inteligenci“
  - rozšiřuje se protokol použitý pro přenosy dat z/do paměti
    - čipy většinou dokáží automaticky provádět obnovu (*refresh*) dat
- Burst režim – přenos většího bloku dat
  - Díky hodinovému signálu je možné pouze inicializovat přenos, nastavit adresu řádku i adresu sloupce a po prvotním zpoždění způsobeném výběrem řádku je v každém taktu provedeno přečtení/zápis jedné hodnoty.

# DDR (Double Data Rate)

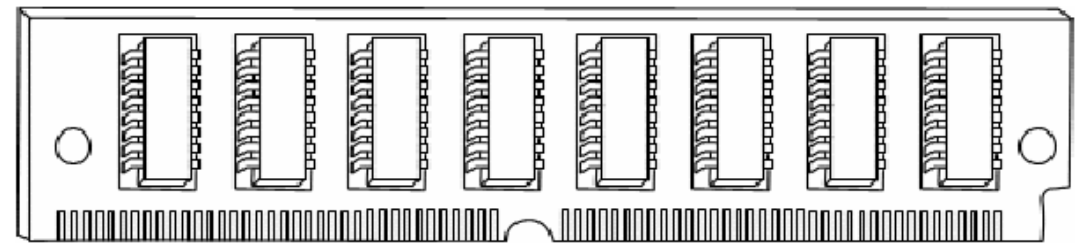
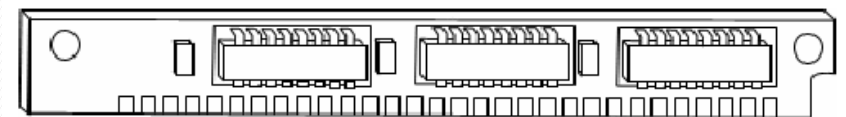
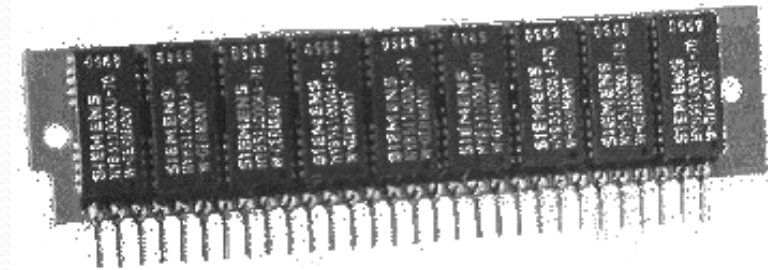
- Lepší využití hodinového signálu
- Používá se vzestupná i sestupná hrana hodinového signálu.
- Použití této techniky u sběrnic a pamětí
- DDR neznamená automaticky typ paměti, ale způsob přenosu





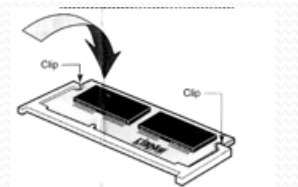
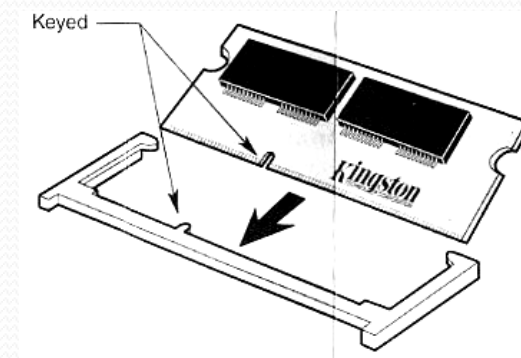
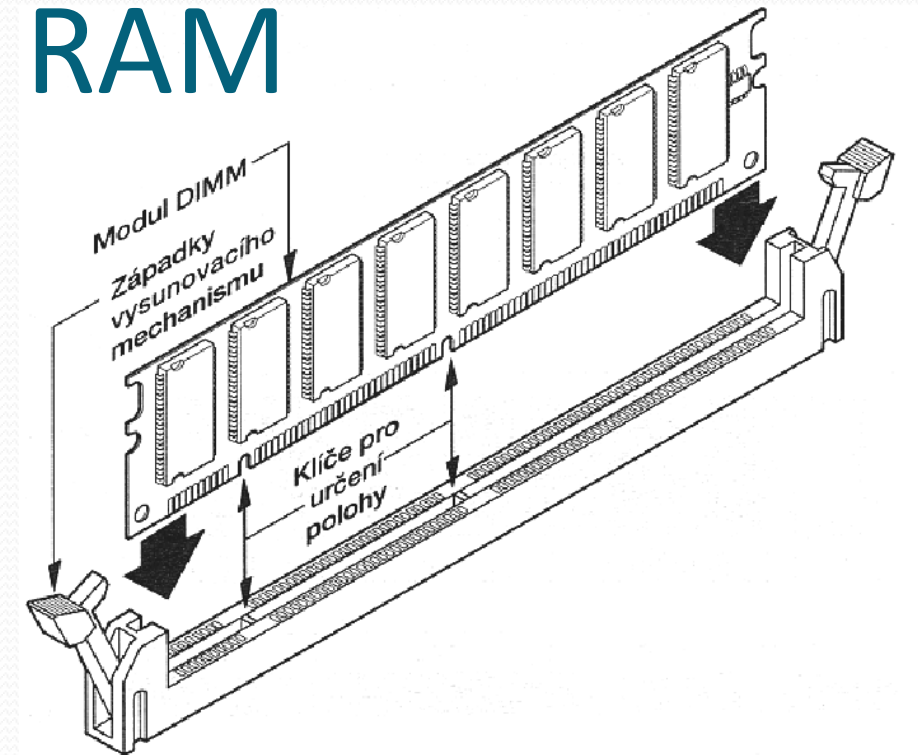
# Fyzické uspořádání paměti RAM

- DIP
- SIPP (Single Inline Pin Package)
- SIMM (Single Inline Memory Module)
  - 30-pin SIMM
  - 72-pin SIMM



# Fyzické uspořádání paměti RAM

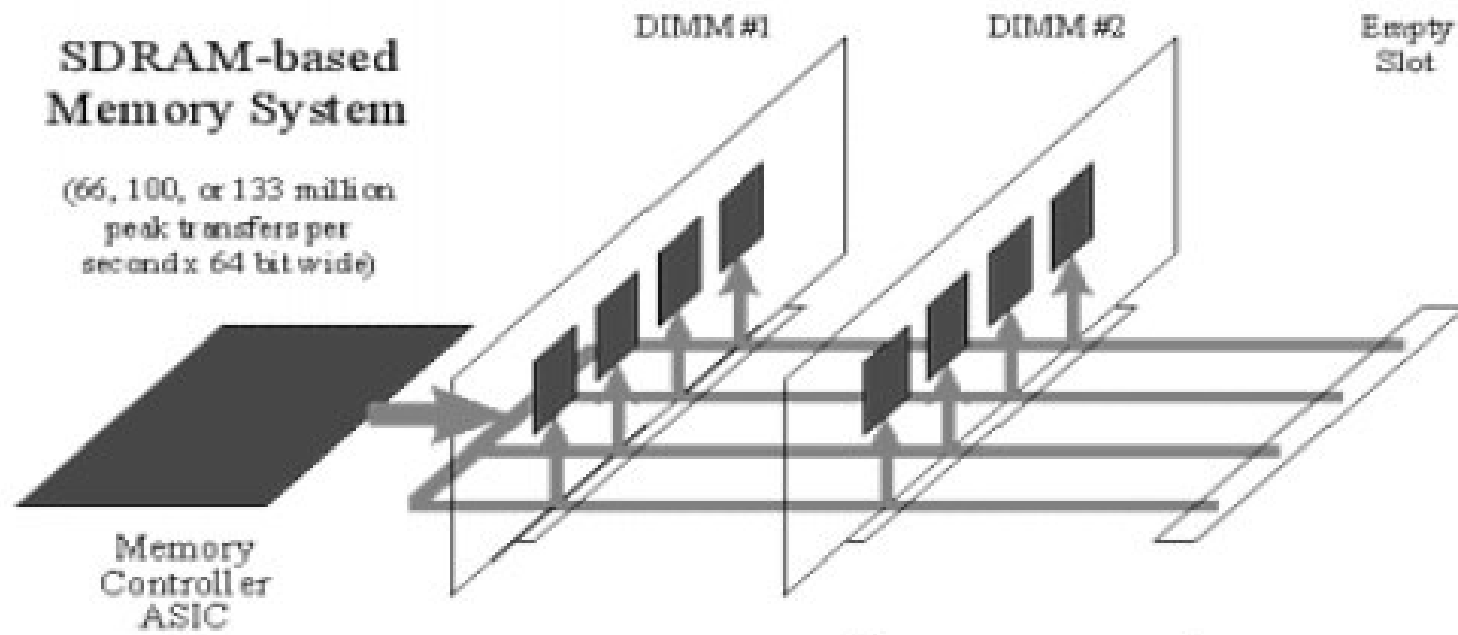
- DIMM (Dual Inline Memory Module)
  - SODIMM (Small Outline DIMM)
- DDR DIMM (Double Data Rate DIMM)
  - DDR SODIMM
- DDR<sub>2</sub> DIMM
  - DDR<sub>2</sub> SODIMM
- DDR<sub>3</sub> DIMM
  - DDR<sub>3</sub> SODIMM
- DDR<sub>4</sub> DIMM
  - DDR<sub>4</sub> SODIM
- RIMM (Rambus Inline Memory Module)





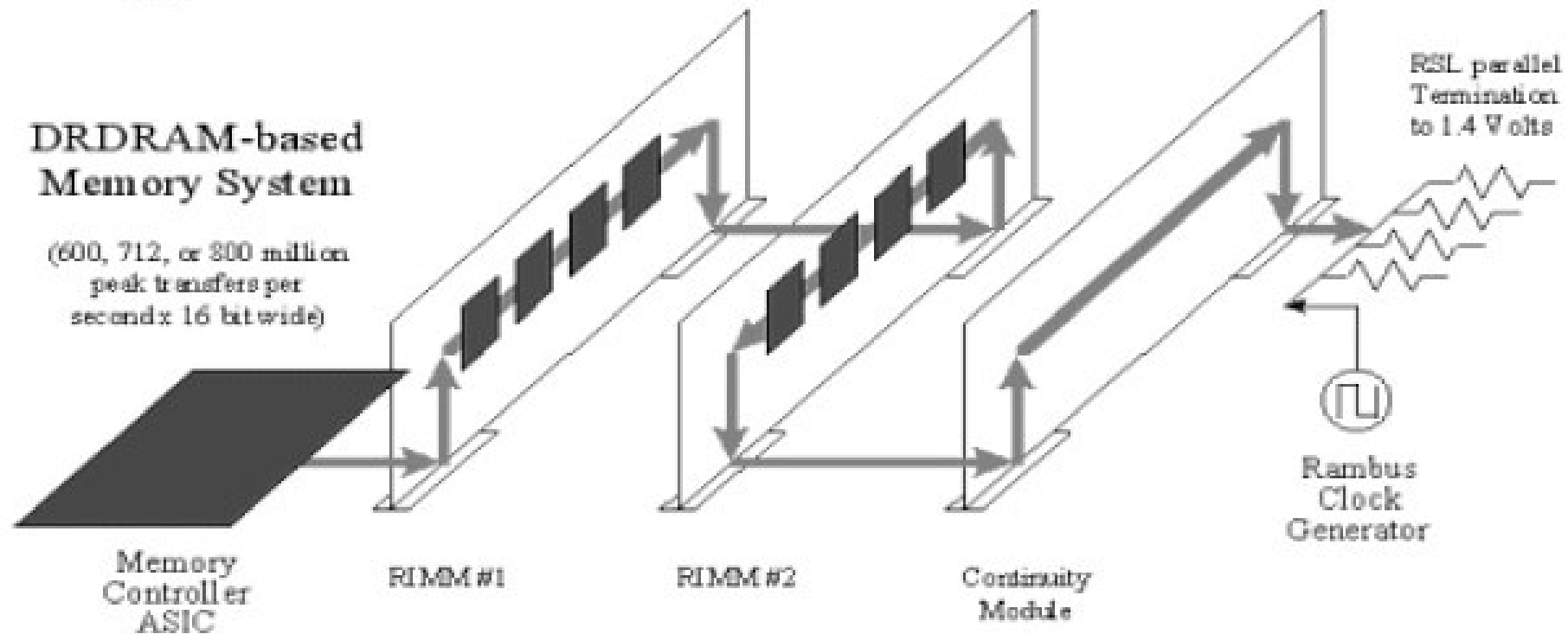
## SDRAM-based Memory System

(66, 100, or 133 million peak transfers per second x 64 bit wide)



## DDRDRAM-based Memory System

(600, 712, or 800 million peak transfers per second x 16 bit wide)



# Časování paměti

$$t_{CL}-t_{RCD}-t_{RP}-t_{RAS}$$

Výběr(zápis) – adresace řádku – počáteční ustálení – aktivní adresace

- DRAM pracují v jednotkách nanosekund
  - Nutno rozdělit čtení a zápis na suboperace
- **RAS precharge** - zpoždění po výběru paměti do adresace řádku
  - Ustálení stavu signálů před adresováním
- **RAS to CAS** - zpoždění mezi výběrem řádků a adresací sloupce
  - Adresace řádku
- **CAS nebo CL (CAS Latency)** – Adresace sloupce
  - zpoždění na vstupu nebo výstupu
  - Poté lze data číst nebo zapisovat.
- **tRAS** – Doba nutná na ponechání aktivní adresace řádku než se může přejít na adresaci dalšího řádku.
- Čím jsou zpoždění menší, tím je reálná propustnost dat vyšší.

# Časování pamětí

	PC-3200 (DDR-400)				PC2-6400 (DDR2-800)				PC3-12800 (DDR3-1600)			
	Typical		Fast		Typical		Fast		Typical		Fast	
	cycles	time	cycles	time	cycles	time	cycles	time	cycles	time	cycles	time
$t_{CL}$	3	15 ns	2	10 ns	5	12.5 ns	4	10 ns	9	11.25 ns	8	10 ns
$t_{RCD}$	4	20 ns	2	10 ns	5	12.5 ns	4	10 ns	9	11.25 ns	8	10 ns
$t_{RP}$	4	20 ns	2	10 ns	5	12.5 ns	4	10 ns	9	11.25 ns	8	10 ns
$t_{RAS}$	8	40 ns	5	25 ns	16	40 ns	12	30 ns	27	33,75 ns	24	30 ns

$t_{CL}-t_{RCD}-t_{RP}-t_{RAS}$

Výběr(zápis) – adresace řádku – počáteční ustálení – aktivní adresace

# Ochrana operační paměti

- Kontrola Parity
  - Kód ECC - Error Correcting code
  - Technologie Chipkill
- 
- Hot Swap, Hot Add
  - Hot Spare Memory
  - Memory Scrubbing
  - Technologie ProteXion

# Kontrola parity

- modul musí mít dodatečné paměťové čipy, do kterých se ukládá paritní bit
- Paritní bit je kontrolou pro dalších 8 bitů
- Kontrola parity neznamená možnost opravy chyb
- Doplnění jednoho bitu tak, aby byl
  - sudý počet jedniček (sudá parita)
  - lichý počet jedniček (lichá parita)

# Kód ECC

## (Error Correcting code)

- Detekce a korekce 1 chybného bitu na 64b.
  - 64b. – šířka datové sběrnice
- Umožňuje i detekci dvou chybných bitů
  - v tomto případě již není možná oprava
- Nutnost navýšit počet bitů (1 chip navíc), 64b. -> 72b.
- Mírné snížení výkonu: 0,5-2%

# ChipKill

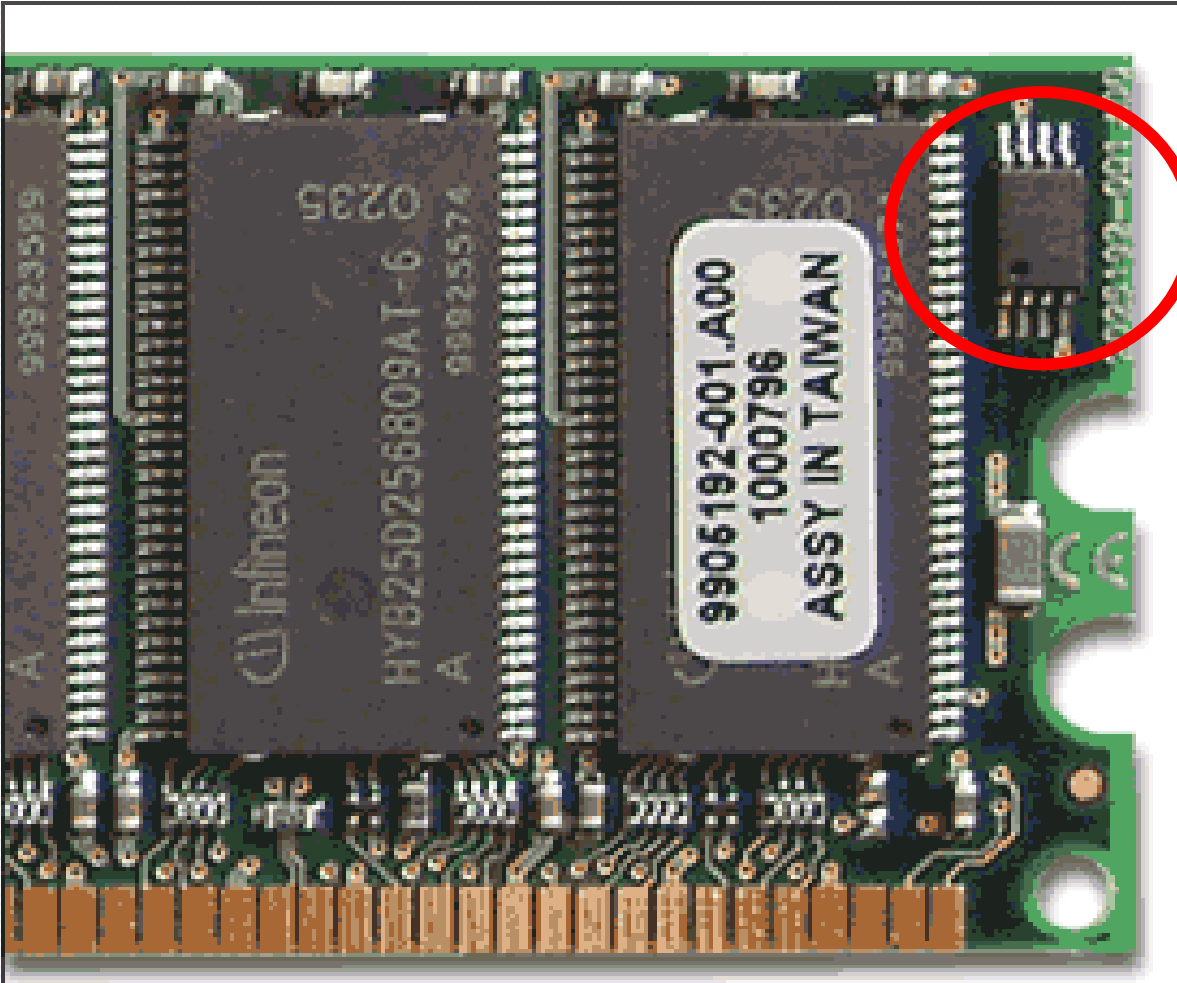
- Extended ECC, Advanced ECC (a další názvy podle firmy, která vyrábí)
- Vyvíjena původně pro NASA
  - (výzkum Marsu)
- Rozpozná chybu v 8 bitech
- Korekce chyby až ve 4 bitech
- Nevyžaduje speciální moduly
  - Stačí ECC paměť
- Funkce závisí na podpoře chipsetu a BIOSu



# Chyby paměťových modulů

- **Fyzické chyby** - obvykle je jediná možná oprava – výměna celého modulu.
- **Logické chyby** - většinou dočasné chyby, které se mohou náhodně objevovat
  - Poruchy napájení.
  - Nesprávný typ modulu nebo nevhodná rychlost modulu.
  - Rušení radiovými signály – v důsledku indukce mohou vznikat falešné elektrické signály.
  - Statické výboje.
  - Výpadky časování – příčinou jsou pomalé paměťové moduly nebo přetaktované procesory

# SPD chip (Serial Presence Detect Chip)



# Nastavení paměti

Memory Timing Setting		
Parameters	Setting	Current Value
Memory Timing Setting	[Expert]	
tCL (CAS Latency)	[Auto(7)]	7
tRCD	[Auto(7)]	7
tRP	[Auto(7)]	7
tRAS	[Auto(20)]	20
Command Per Clock (CMD)	[Auto(1T)]	1T
** Advanced Memory Settings **		
tRRD	[Auto(4)]	4
tRC	[Auto(27)]	27
tWR	[Auto(10)]	10
tWTR	[Auto(14)]	14
tFAW	[Auto(21)]	21
tREF	[Auto]	7.7uS

# Lavalys EVEREST Cache & Memory Benchmark

	Read	Write	Copy	Latency
Memory	6138 MB/s	4815 MB/s	5263 MB/s	74.2 ns
L1 Cache	42645 MB/s	42490 MB/s	84996 MB/s	1.1 ns
L2 Cache	19502 MB/s	15074 MB/s	21379 MB/s	5.1 ns
L3 Cache				
CPU Type	DualCore Intel Core 2 Duo E6700 (Conroe, LGA775)			
CPU Clock	2666.6 MHz (original: 2667 MHz)			
CPU FSB	266.7 MHz (original: 266 MHz)			
CPU Multiplier	10.0x	CPU Stepping		B2
Memory Bus	333.3 MHz	DRAM:FSB Ratio		10:8
Memory Type	Dual Channel DDR2-667 SDRAM (5-5-15 CR2)			
Chipset	Intel Broadwater P965			
Motherboard	Gigabyte GA-965P-DS4			

# Lavalys EVEREST Cache & Memory Benchmark

	Read	Write	Copy	Latency
Memory	6311 MB/s	5407 MB/s	4951 MB/s	80.5 ns
L1 Cache	47979 MB/s	47814 MB/s	95645 MB/s	1.0 ns
L2 Cache	22511 MB/s	17369 MB/s	24327 MB/s	4.9 ns
L3 Cache				
CPU Type	DualCore Intel Core 2 Duo E6700 (Conroe, LGA775)			
CPU Clock	3000.0 MHz (original: 2667 MHz, overclock: 12%)			
CPU FSB	300.0 MHz (original: 266 MHz, overclock: 13%)			
CPU Multiplier	10.0x	CPU Stepping		B2
Memory Bus	375.0 MHz	DRAM:FSB Ratio		10:8
Memory Type	Dual Channel DDR2-750 SDRAM (5-6-6-18 CR2)			
Chipset	Intel Broadwater P965			
Motherboard	Gigabyte GA-965P-DS4			

# Lavalys EVEREST Cache & Memory Benchmark

	Read	Write	Copy	Latency
Memory	20515 MB/s	16946 MB/s	22088 MB/s	22.9 ns
L1 Cache	59987 MB/s	59958 MB/s	119879 MB/s	1.1 ns
L2 Cache	39998 MB/s	36487 MB/s	46426 MB/s	2.7 ns
L3 Cache	29199 MB/s	24833 MB/s	30460 MB/s	3.3 ns
CPU Type	QuadCore Intel Bloomfield (Bloomfield / Gainestown, LGA1366)			

	Read	Write	Copy	Latency
Memory	50781 MB/s	50867 MB/s	45355 MB/s	77.3 ns
L1 Cache	994.24 GB/s	498.64 GB/s	994.06 GB/s	1.0 ns
L2 Cache	772.35 GB/s	452.27 GB/s	698.27 GB/s	5.2 ns
L3 Cache	411.72 GB/s	365.00 GB/s	491.59 GB/s	18.7 ns
L4 Cache				
CPU Type	OctalCore AMD Ryzen 7 1700 (Summit Ridge, Socket AM4)			
CPU Stepping	ZP-B1			
CPU Clock	4001.7 MHz			
CPU FSB	133.4 MHz (original: 100 MHz, overclock: 33%)			
CPU Multiplier	30x	North Bridge Clock		
Memory Bus	1800.7 MHz	DRAM:FSB Ratio		54:4
Memory Type	Dual Channel DDR4-3600 SDRAM (17-17-17-38 CR1)			
Chipset	AMD X370, AMD K17 SCH, AMD K17 IMC			

# Adresování operační paměti reálný režim

- **Princip adresování paměti - mikroprocesor i8086**
  - Plně 16bitový procesor. 16 bitová vnitřní architektura
    - možnost zpracovat maximálně 16bitové číslo (tj. číslo o až  $(2^{16}-1)$  neboli 0 až 65535).
- Adresová sběrnice – 20 bitů
  - možnost adresovat paměťový prostor o kapacitě max. 1 MB (odpovídá  $2^{20}$  B = 1048576 B).
- **Důležité: pro vytvoření 20 bitové adresy jsou k dispozici pouze 16 bitové registry.**
- Adresa je tvořena dvěma šestnáctibitovými složkami –
  - **segment** a **offset**, které se sečtou posunuty o 4 bity
  - (posunutí o 4 bity = vynásobení 16).
    - Tím je vytvořena výsledná 20bitová adresa.

# Adresování operační paměti

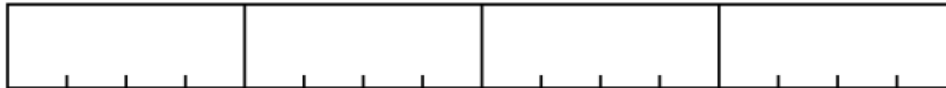
## Příklad

- Původní binární kombinace:
- **1101** – desítkově 13
- Posunutí o 4 bity doleva a doplnění zprava nulami: **1101 0000**
  - Desítkově  $16 + 64 + 128 = 208$
- Stejný výsledek dostaneme, když původní číslo vynásobíme 16:
  - $13 \times 16 = 208$
- Adresa se v reálném režimu počítá podle vztahu:  
 $16 \times \text{segment} + \text{offset}.$

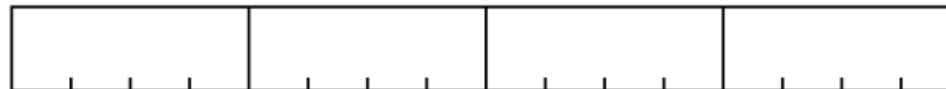
# Adresování operační paměti

reálný režim

**Segment: 16 bitů**

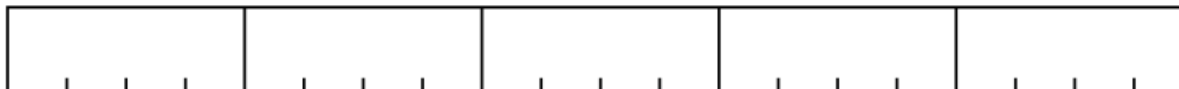


**Offset: 16 bitů**



---

**Adresa: 20 bitů**





# Adresování operační paměti

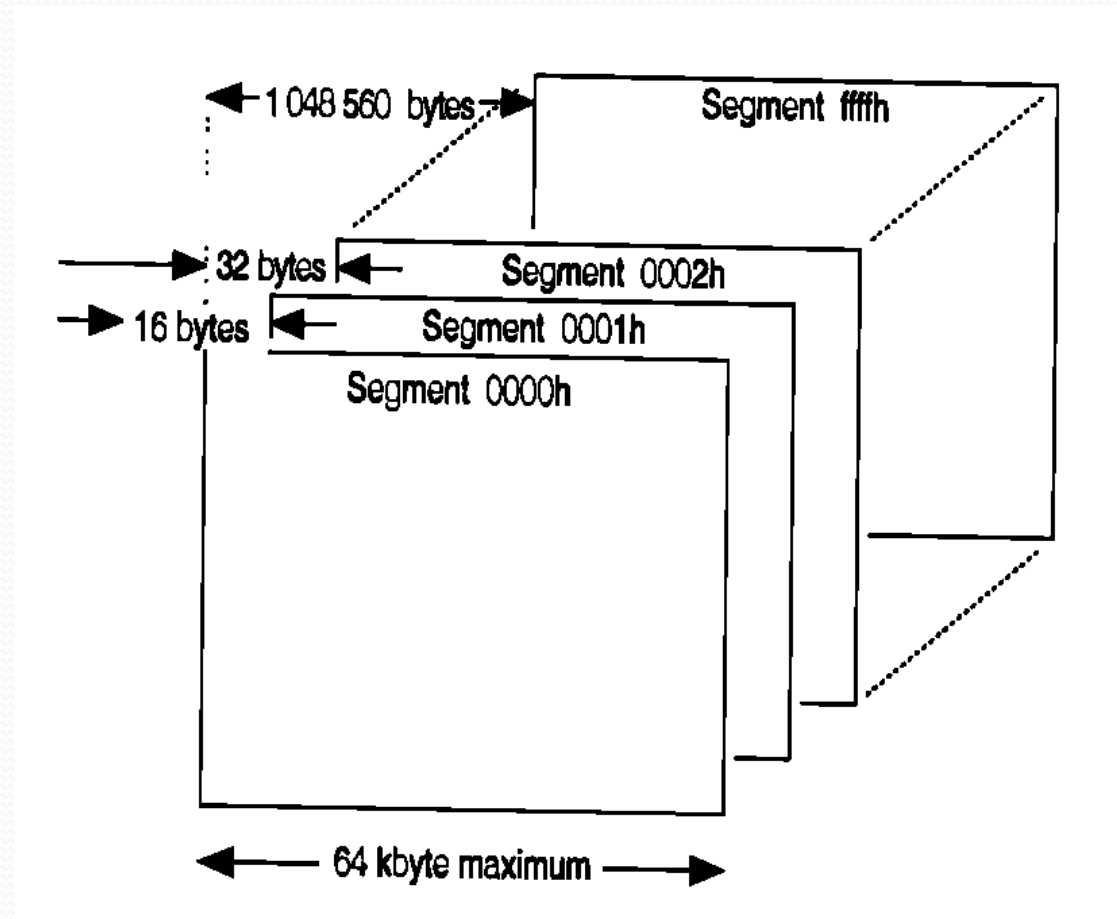
## Příklad

- Adresa se zapisuje ve tvaru **segment:offset**
  - Např. **4000:B000** značí adresu **4B000** (hexadecimálně), tj. **307200** (dekadicky).
- Zápis **1F36:0A5D** reprezentuje segment **1F36**, offset **0A5D**
  - adresa je:  $1F36 \times 16 + 0A5D = 7990 \times 16 + 2653 = 130\,493$ .
- **Praktická realizace součtu:**
- Vynásobení čísla segmentu 16 = posunutí čísla segmentu o 4 bity doleva
  - $1F360 + 0A5D = 1FDBD = 130\,493$
- **Velikost jednoho segmentu**, v jehož rámci je možné se pohybovat pouze pomocí změny hodnoty offsetu, je **64kB**.
  - **Zdůvodnění:** registry jsou 16 bitové, takže je možné v rámci segmentu adresovat pouze  $2^{16}$  slabik (64 kB).
- Registr pro uložení segmentu je 16bitový
  - $2^{16}$  možností adresy segmentu (začátku segmentu kapacity 64 kB).

# Adresování operační paměti

- **Důležité:**
- Segment může začínat na libovolné adrese dané kombinací uloženou v registru segmentu
  - nikoliv na adresách začínajících hranicích 64kB bloků (každých 16 B může začínat nový segment).
- Zvýšení adresy segmentu o 1 – adresa začátku segmentu se zvýší o 16
  - (souvisí s principem adresace v reálném režimu – posunutím o 4 bity doleva).
- Zvýšení offsetu o 1 – adresa se zvýší o 1

# Adresování operační paměti



# Adresování operační paměti chráněný režim

- **mikroprocesor i80286** Šířka sběrnic: 16 bitů, 24 bitů adresa(16 MB).
  - 1MB (reálný režim) – nedostatečné ...
- **Princip**
  - pracuje se zase se 16 bitovými registry, ty jsou však pouze ukazateli na lokality, kde je teprve uložena celá 24bitová adresa.
- Nový režim je neslučitelný s 8086

# Adresování operační paměti chráněný režim

- Procesor v tomto režimu poskytuje **ochranu** mezi jednotlivými spuštěnými programy a **různé úrovně oprávnění přístupu** k prostředkům počítače.
- Procesor v tomto režimu také používá jiný model pro vytváření adresy – dvě 16bit složky nazývané **selektor** a **offset** za pomoci tzv. **tabulek deskriptorů**.
- Adresa je 24b (pro i286)
  - umožňuje procesoru adresovat maximálně  $2^{24}$  B = 16 MB operační paměti.

# Adresování operační paměti chráněný režim – i286

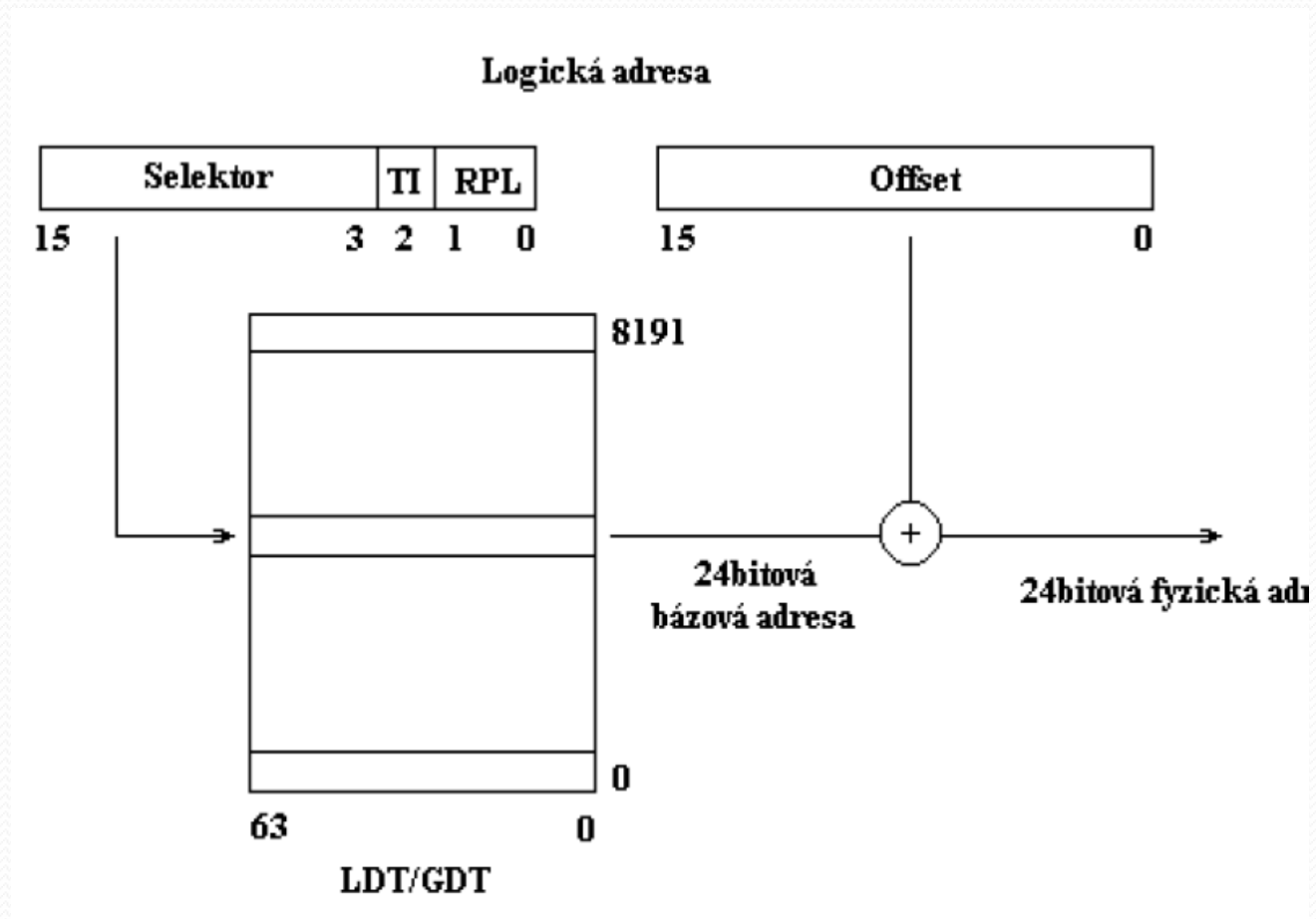
- První část logické adresy zvaná selektor je rozdělena na tři části:
  - Nejnižší dva bity jsou nazývány **RPL** (Requested Privilege Level)
    - určují požadovanou úroveň oprávnění k segmentu paměti
      - podpora 4 úrovní oprávnění.
  - Bit 2 - **TI** (Table Index) - určuje, zda při tvorbě adresy bude použita lokální tabulka deskriptorů (**LDT** – Local Descriptor Table) nebo globální tabulka deskriptorů (**GDT** - Global Descriptor Table).
    - **LDT** - určen pro umístování jedinečných dat
    - **GDT** - ukazuje, kde jsou umístěny LDT, základní globální a systémové věci. Jsou zde programy nebo proměnné přístupné více uživatelům.
  - **Nejvyšších třináct bitů potom slouží jako index do příslušné tabulky deskriptorů.**
- Jedna položka tabulky deskriptorů má 64 bitů, ze kterých je vybráno 24 bitů sloužících jako tzv. **bázová adresa**. K této bázové adrese se potom přičte 16b offset uložený v registru (přičtení je provedeno přímo bez jakéhokoliv posunutí).

# Adresování operační paměti chráněný režim – i286

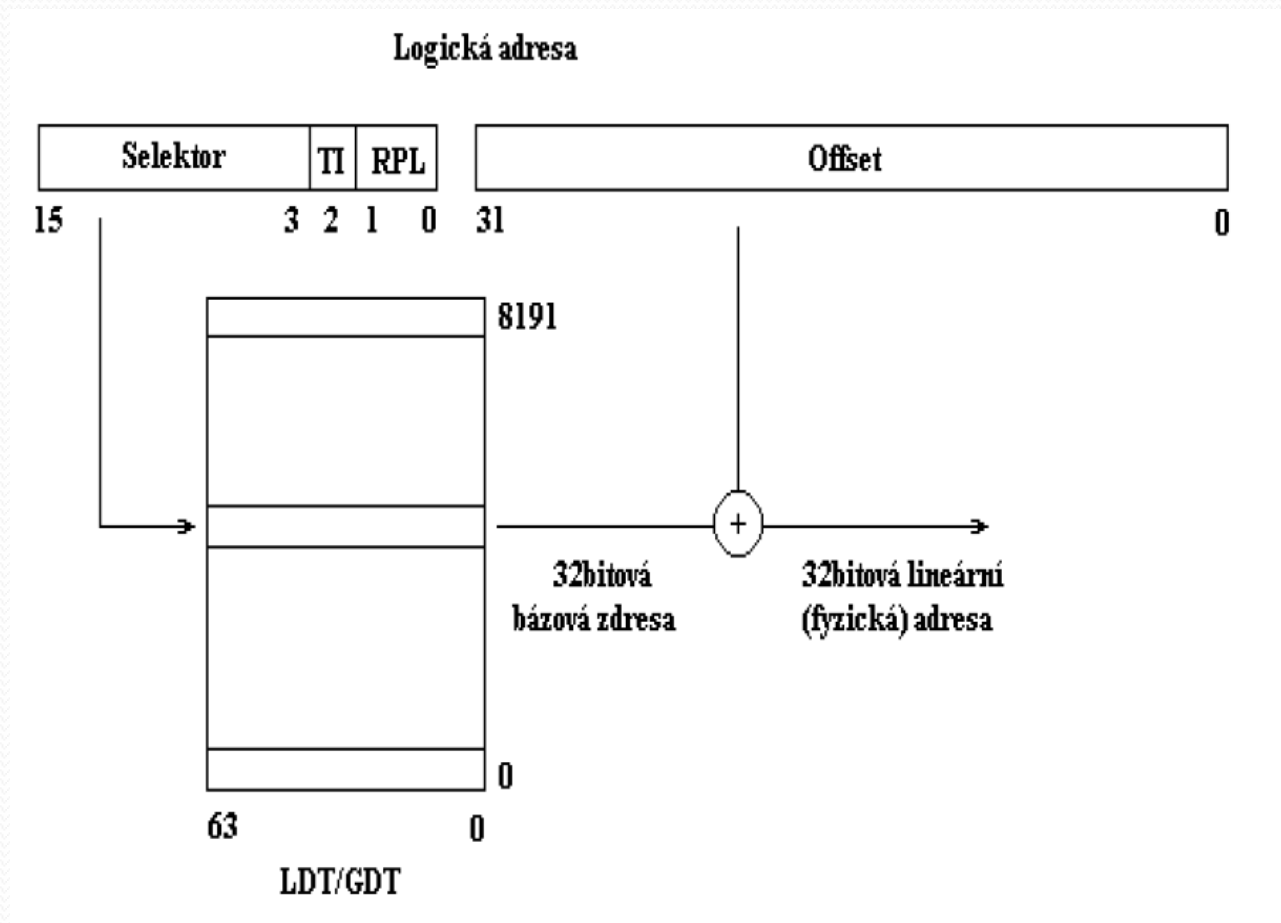
- Výsledkem je 24 bitová **fyzická adresa**, pomocí které je možno adresovat maximálně 16 MB operační paměti (**plná adresovací kapacita procesoru 80286**).
- Jedna položka tabulky deskriptorů obsahuje:
  - **bázovou adresu segmentu** (24 bitů), tj. adresu, na které segment začíná.
  - **přístupová práva** k segmentu (8bitů).
  - **limit segmentu** (16 bitů), který určuje maximální velikost segmentů
  - zbývající bity deskriptoru jsou nastaveny vždy na nulu (kvůli kompatibilitě s procesorem 80386)
- **Velkou nevýhodou** tohoto procesoru je stále **16bitový offset**, který nedovoluje větší segment než 64 kB.



# Adresování operační paměti chráněný režim – i286



# Adresování operační paměti chráněný režim – i386



# 80386 - adresace

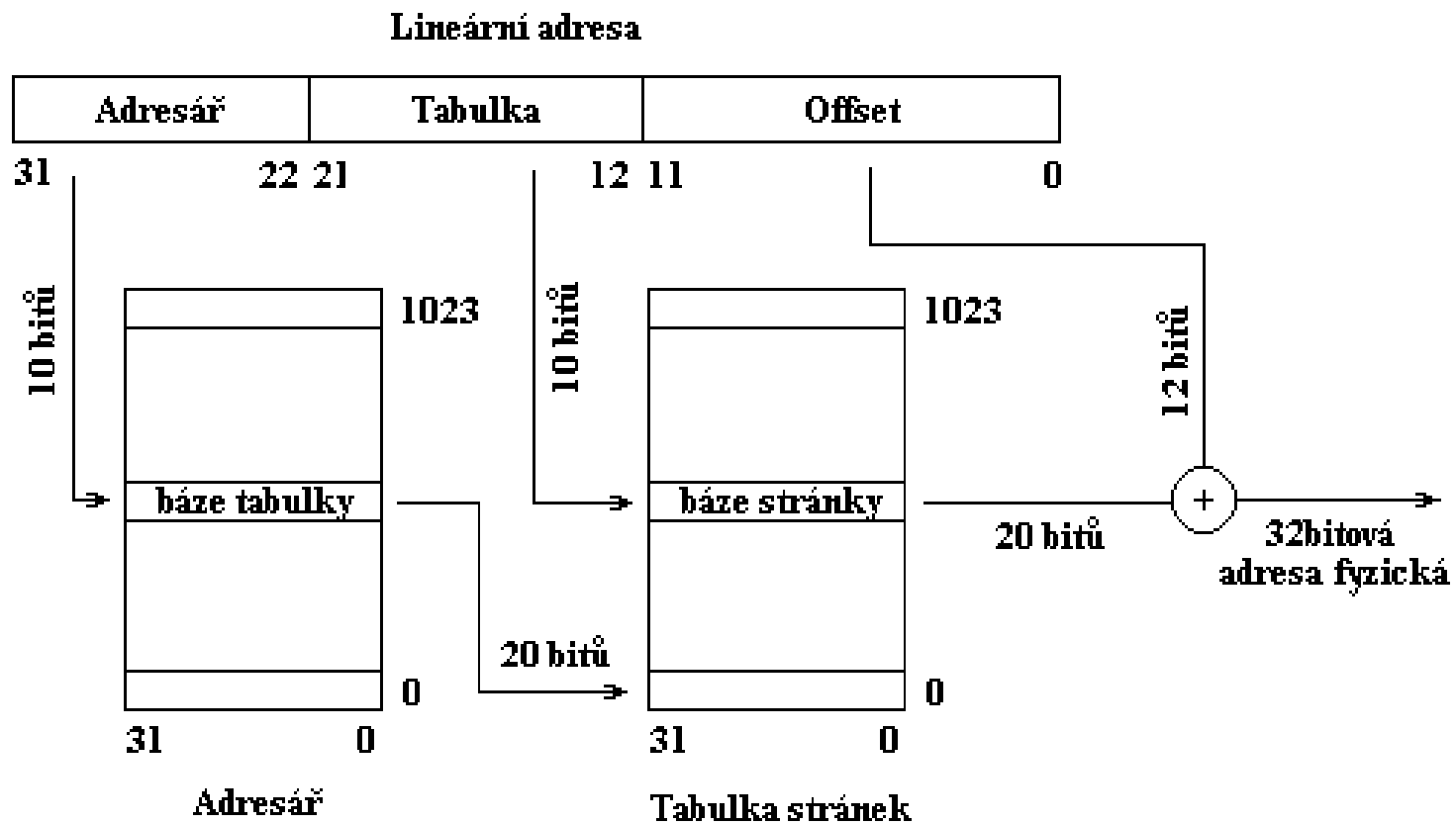


Schéma stránkovacího mechanismu procesoru 80386

**TLB** (Translation Lookaside Buffer)

# Adresování operační paměti chráněný režim – i386


- Vnitřní sběrnice procesoru je 32 bitová,
- Vnitřní registry procesoru jsou také 32b.
- Tento mechanismus umožňuje, aby vytvořená adresa byla 32 bitová.
- Bázová adresa, která se vybírá z tabulky deskriptorů, je 32bitová.
- Velikost offsetu - 32 bitů.
- Procesor 80386 adresoval až 4 GB ( $2^{32}$ B) operační paměti
- Max. velikost jednoho segmentu je 4GB (protože registr, v němž byla uložena hodnota segmentu, je 32b).

# Adresování operační paměti chráněný režim – i386

- **Procesory I80386 a vyšší: možnost adresace tzv. oblasti HMA (High Memory Area)** – oblast prvních 64 kB nad 1 MB paměti (zkrácených o 16 B).
- Jak taková adresa vznikne:
  - Adresu paměti v rámci 1 MB tvoří bity **A0- A19**.
  - Pokud sečtením čísla segmentu a offsetu nastane **přetečení do bitu A20**, pak se dostaneme do oblasti nad 1 MB (oblast HMA).
- **Příklad:**

Segment x 16	FFFF0H	
Offset		FFFFH
Fyzická adresa	10FFEFH	

Důsledek: vznikla tak adresa sestávající z 21 bitů.
- Využití této techniky v MS DOSu - mohl v reálném režimu rozšířit původních 640 kB o 10 %, přesněji o kapacitu **64 kB** a tuto oblast využít pro uložení částí operačního systému a ovladačů
  - podpora v MS DOSu potřebnými příkazy
    - (pokyn pro uložení těchto částí do oblasti HMA).
- Bit A20 bylo možné ignorovat nebo zohledňovat (nastavení v setupu) – hardwarově to zařizoval řadič klávesnice.

- 
- Forthcoming non-volatile memory technologies include FeRAM, CBRAM, PRAM, SONOS, RRAM, racetrack memory, NRAM, 3D XPoint, and millipede memory.