ОНЛАЙН-ОБРАЗОВАНИЕ

Меня хорошо слышно && видно?

Напишите в чат, если есть проблемы!

Ставьте + если все хорошо

OTUS

Защищенный режим

Сегментная/Страничная организация памяти

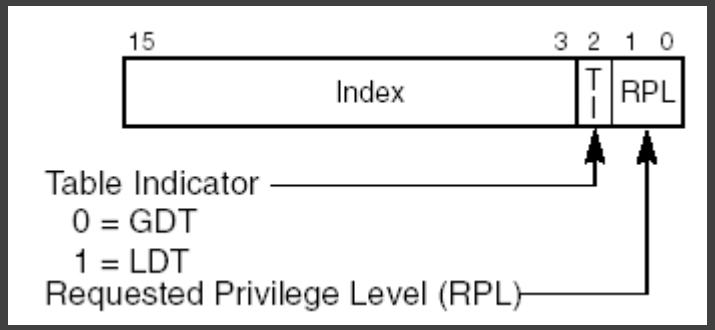
Пакулов Артур

1

Сегментная организация памяти

Селектор

Индекс дескриптора в GDT



TI = 0 → GDT

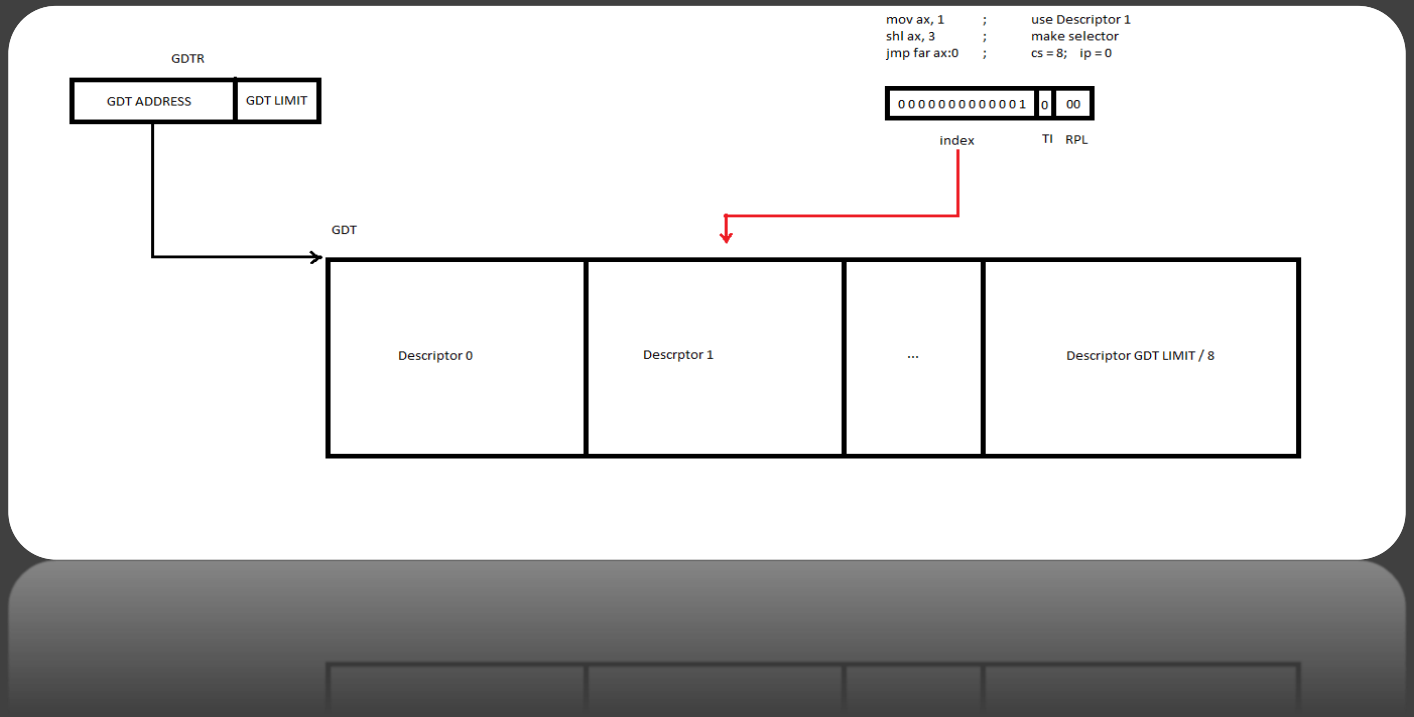
TI = 1 → LDT

RPL = 0 → режим ядра

RPL = 1 → режим пользователя

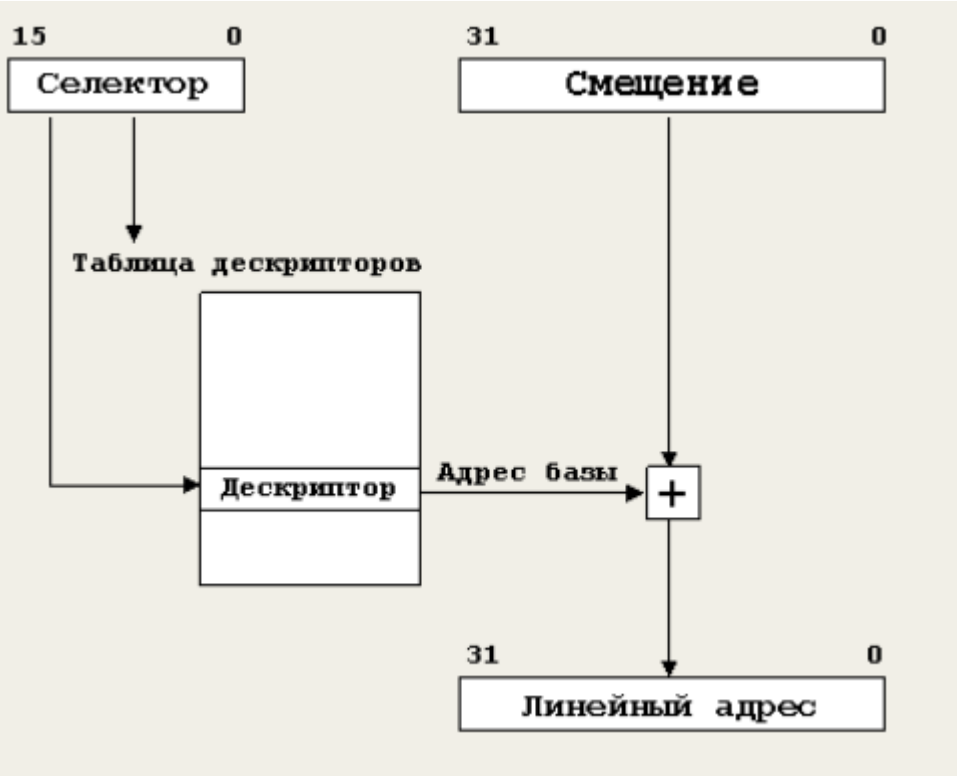
Селектор:Смещение

Селектор состоит из индекса сегмента в GDT, TI и RPL



Сегментная организация памяти

Преобразование логического адреса в линейный



Линейный адрес == Физическому!

2

Пример

Настраиваем **Bochs**

```
# configuration file generated by Bochs
plugin_ctrl: unmapped=1, biosdev=1, speaker=1, extfpuirq=1, parallel=1, serial=1, gameport=1, iodebug=1
config_interface: win32config
display_library: win32
memory: host=32, guest=32
romimage: file="D:\Program Files (x86)\Bochs-2.6.8/BIOS-bochs-latest"
vgaromimage: file="D:\Program Files (x86)\Bochs-2.6.8/VGABIOS-lgpl-latest"
boot: floppy
floppy_bootsig_check: disabled=0
floppya: type=1_44, 1_44="D:\Languages\fasm\programs\segmodel.bin", status=inserted, write_protected=0
floppyb: type=1_44, 1_44="D:\Languages\fasm\programs\floppy2.bin", status=inserted, write_protected=0
ata0: enabled=1, ioaddr1=0x1f0, ioaddr2=0x3f0, irq=14
ata0-master: type=none
ata0-slave: type=none
ata1: enabled=1, ioaddr1=0x170, ioaddr2=0x370, irq=15
ata1-master: type=none
ata1-slave: type=none
ata2: enabled=0
ata3: enabled=0
pci: enabled=1, chipset=i440fx
vga: extension=vbe, update_freq=5, realtime=1
cpu: count=1, ips=4000000, model=bx_generic, reset_on_triple_fault=1, cpuid_limit_winnt=0, ignore_bad_msrs=1, mwait_is_nop=0
cpuid: level=6, stepping=3, model=3, family=6, vendor_string="GenuineIntel", brand_string="                Intel(R) Pentium(R) 4 CPU        "
cpuid: mmx=1, apic=xapic, simd=sse2, sse4a=0, misaligned_sse=0, sep=1, movbe=0, adx=0
cpuid: aes=0, sha=0, xsave=0, xsaveopt=0, x86_64=1, 1g_pages=0, pcid=0, fsgsbase=0
cpuid: smep=0, smap=0, mwait=1, vmx=1
print_timestamps: enabled=0
debugger_log: -
magic_break: enabled=1
port_e9_hack: enabled=0
private_colormap: enabled=0
clock: sync=none, time0=local, rtc_sync=0
# no cmosimage
# no loader
log: -
logprefix: %t%e%d
debug: action=ignore
info: action=report
error: action=report
panic: action=ask
keyboard: type=mf, serial_delay=250, paste_delay=100000, user_shortcut=none
mouse: type=ps2, enabled=0, toggle=ctrl+mbutton
sound: waveoutdrv=win, waveout=none, waveindrv=win, wavein=none, midioutdrv=win, midiout=none
speaker: enabled=1, mode=sound
parport1: enabled=1, file=none
parport2: enabled=0
com1: enabled=1, mode=null
com2: enabled=0
com3: enabled=0
com4: enabled=0
```

Настраиваем **Bochs**

```
Регистры CPU: r

Сегментные регистры: sreg

Дамп памятя (10 байт): x /10bx 0x7c00

Вывод стека (4 элемента): print-stack 4
```

[консольные команды дебагера bochs]

Настраиваем **Bochs**

Если параметр magic_break включен:

```
magic_break: enabled=1
```

То, можно в любое место кода вставить команду

```
xchg bx, bx
```

Тогда, bochsdbg брякнется на этой команде

[консольные команды дебагера bochs]

Прямая запись в видеопамять

```
;clrscr
mov ax,3
int 10h
mov ax, 0xb800
mov es, ax
lea si, str
xor di, di
mov ah, 7   ;абтибут
L:
  lodsb
  stosw     ;!пишем вместе с атрибутом
  test al, al
  jnz L
str db 'hello', 0
INT 19h
```

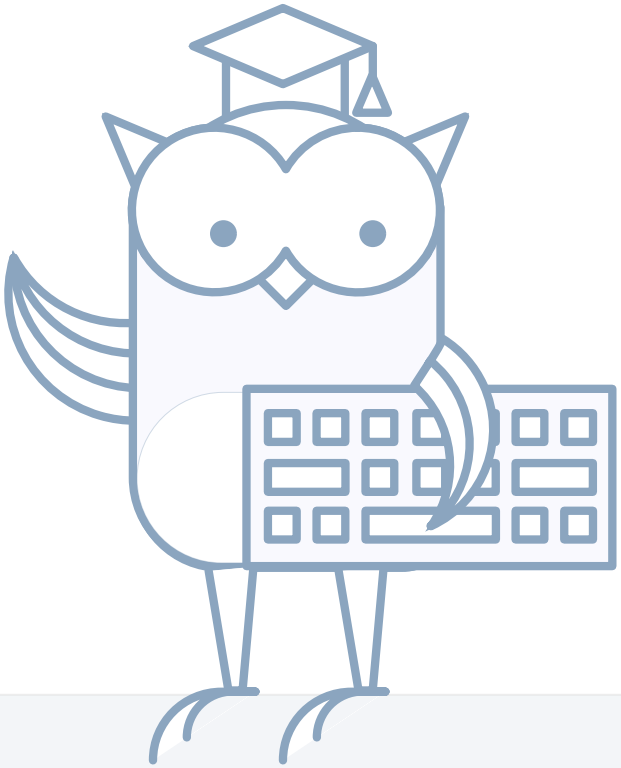
Таблица атрибутов

Атрибут состоит из x:y: x - цвет фона, y - цвет символа

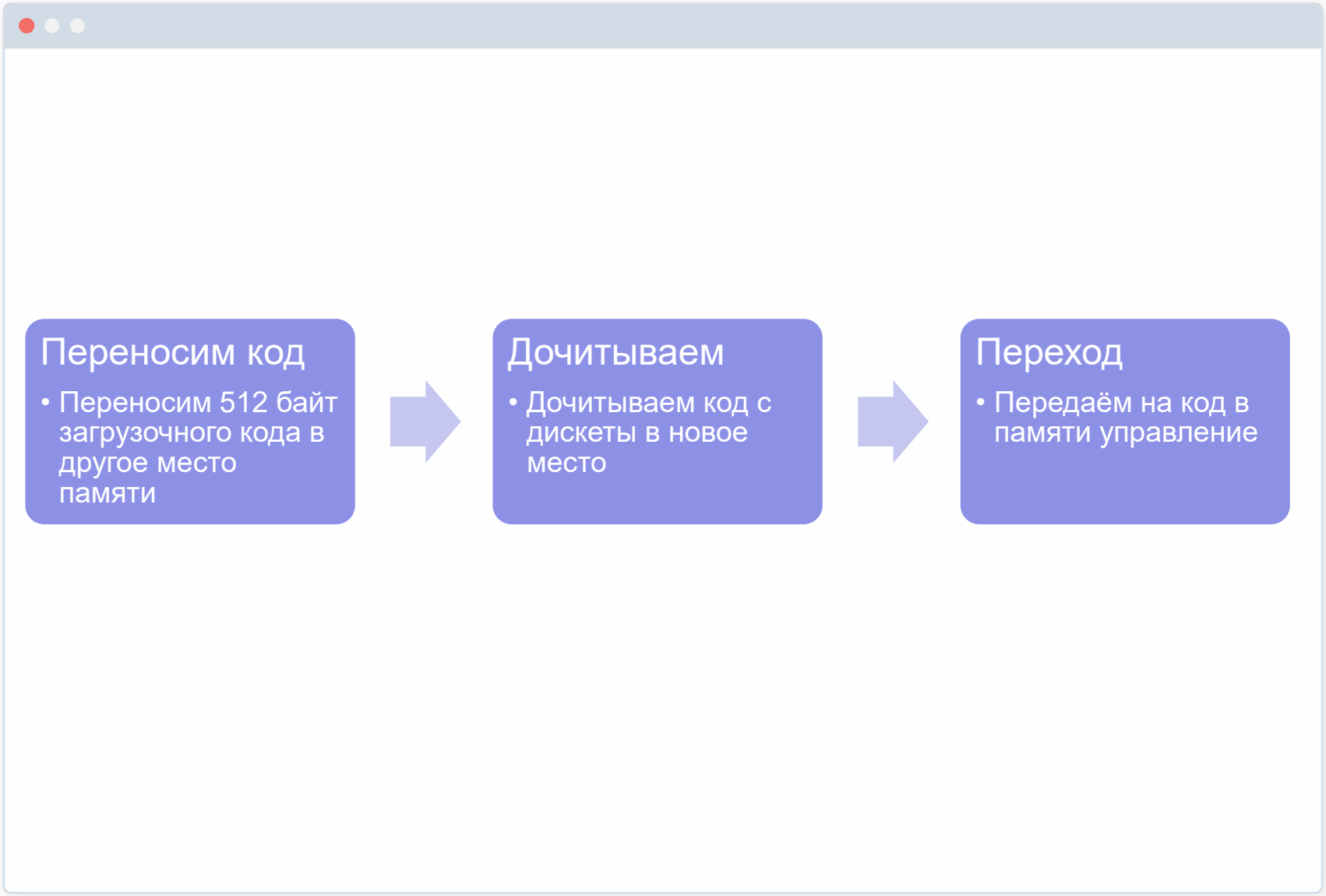
Код	Цвет	Код	Цвет
0h	Черный	8h	Серый
1h	Синий	9h	Голубой
2h	Зеленый	0Ah	Салатовый
3h	Бирюзовый	0Bh	Светло-бирюзовый
4h	Красный	0Ch	Розовый
5h	Фиолетовый	0Dh	Светло-фиолетовый
6h	Коричневый	0Eh	Желтый
7h	Белый	0Fh	Ярко-белый

Задача

Переключить процессор в защищённый режим с сегментной организацией памяти



Этапы


Переносим код
• Переносим 512 байт загрузочного кода в другое место памяти
Дочитываем
• Дочитываем код с дискеты в новое место
Переход
• Передаём на код в памяти управление

Структура кода

Первые 512 байт

- 16-разрядный код
- Копируют данные дискеты в новое место
- Переводят процессор в PM

Вторые 512 кода

- 32 разрядный код
- Тестовое использование селекторов

```
    mov ax,3
    int 10h
        cld
        xor ax, ax

        mov ds, ax
        mov si, CURRENT_OFFSET

        mov di, ax
        mov ax, NEW_SEG
        mov es, ax

        mov cx, 0x200
        mov bx, cx
        rep movsb

        mov ah, 2
        mov al, 1
        mov dx, 0
        mov cx, 2
        int 13h

        push NEW_SEG
        push NEW_OFFSET-CURRENT_OFFSET
        retf

NEW_OFFSET:
```

Перевод в **PM**

```
NEW_OFFSET:
        in al, 0x92
        or al, 2
        out 0x92, al

        cli
        mov al, 0x8F
        out 0x70, al
        in al, 0x71

xchg bx, bx
        mov eax, NEW_SEG
        shl eax, 4                          ;phisical addres = segmeng*0x10 + offset
        add eax, GDT-CURRENT_OFFSET
        mov [(GDTR-CURRENT_OFFSET) + 2], eax    ;phisical address of GDT table

        lgdt fword [GDTR-CURRENT_OFFSET]
        mov eax, cr0
        or al, 1
        mov cr0, eax

xchg bx, bx
        jmp fword 8: pm_Main-CURRENT_OFFSET
```

Пишем в видеопамять

```
use32
pm_Main:
        mov ax, 0x10
        mov ds, ax
        mov fs, ax
        mov ss, ax
        mov esp, -1
        mov ax, 18h
        mov gs, ax

        mov esi, Hello-CURRENT_OFFSET
        call print
        hlt
        jmp $

print:
        pushad
        mov ah, 7
        xor ebx, ebx
        xchg ebx, ebx
puts:
        mov al, byte [cs:esi+ebx]
        mov [gs:(ebx*2)], ax
        inc ebx
        test al, al
        jnz puts
        popad
        hlt
        ret

Hello db 'pm_Main', 0
```

ДЗ

Наладить работу со стеком, проверить лимит в **GDTR**

3

Страничная организация памяти

Типы адресов

Три вида адреса:

- Логический (виртуальный)
- Линейный
- Физический

Линейныё адрес != физическому

Включается установкой PG бита в Cr0

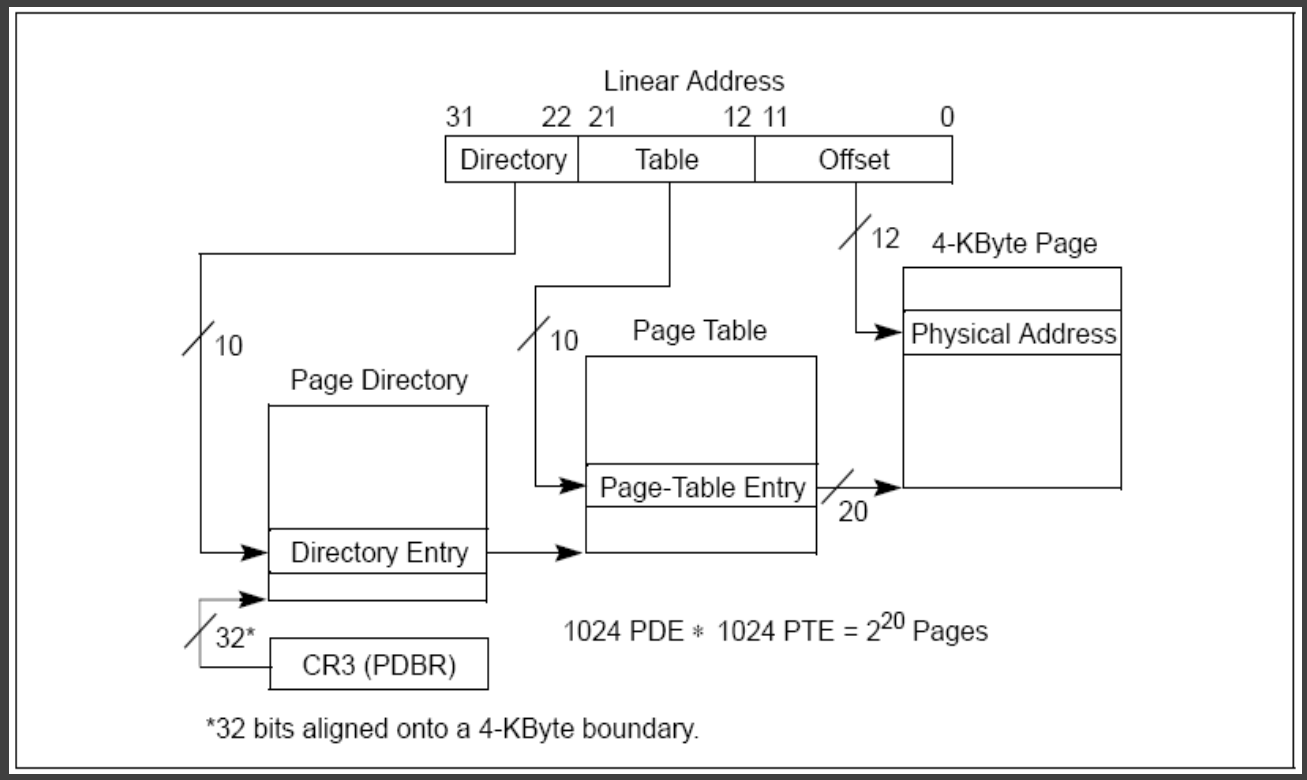
Поддержка ВАП

Осуществляется благодаря:

- ✓ Каталогу страниц
- ✓ Таблице страниц
- ✓ Странице

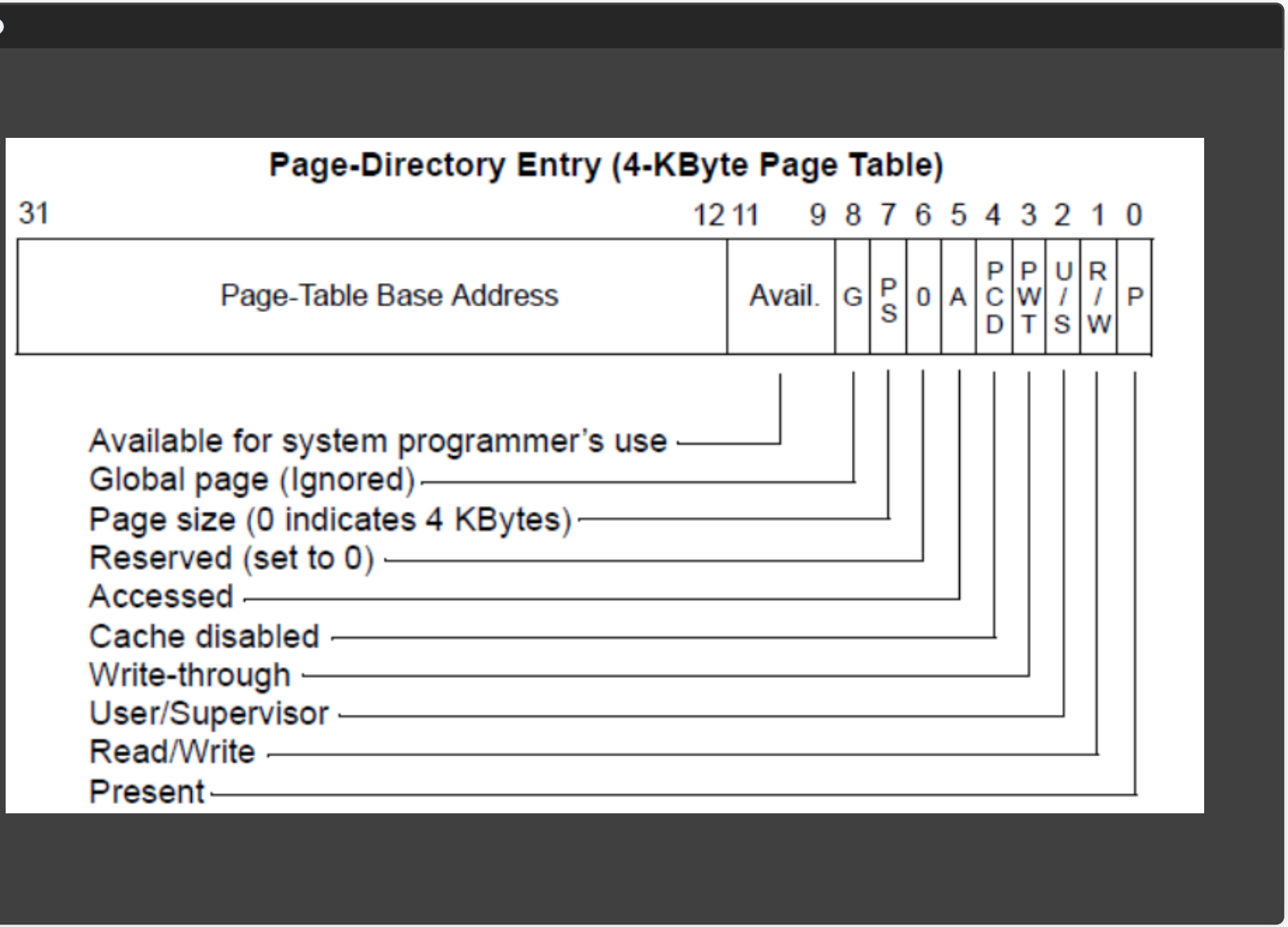
У каждого процесса – свой каталог страниц ➔ свой набор страниц

Преобразование линейного адреса в физический

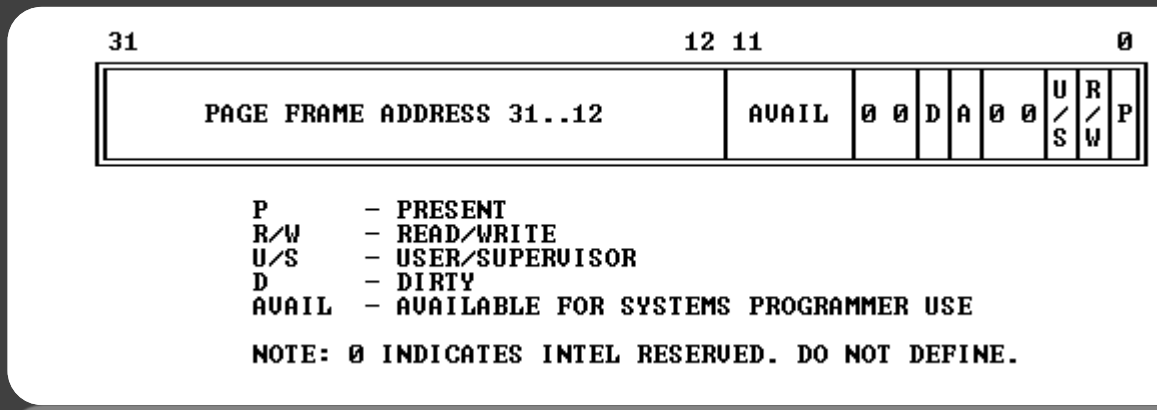


PAE выключен

Структура **PDE**



Структура **PTE**



Поддержка ВАП

Текущий каталог страниц находится в регистре Cr3

У каждого процесса – свой каталог страниц ➔ свой набор страниц

OTUS

Вопросы???

Пакулов Артур

A.Pakulov.Otus@Gmail.com

Спасибо
за внимание!