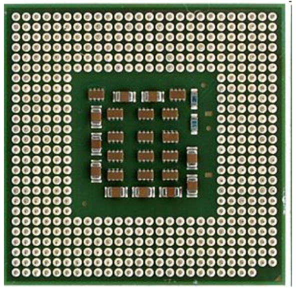
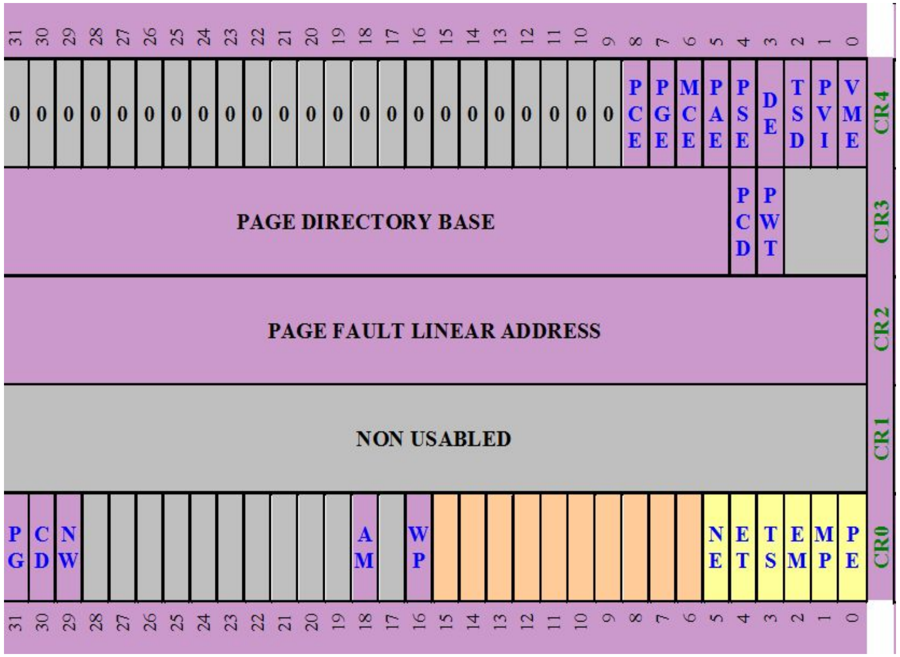
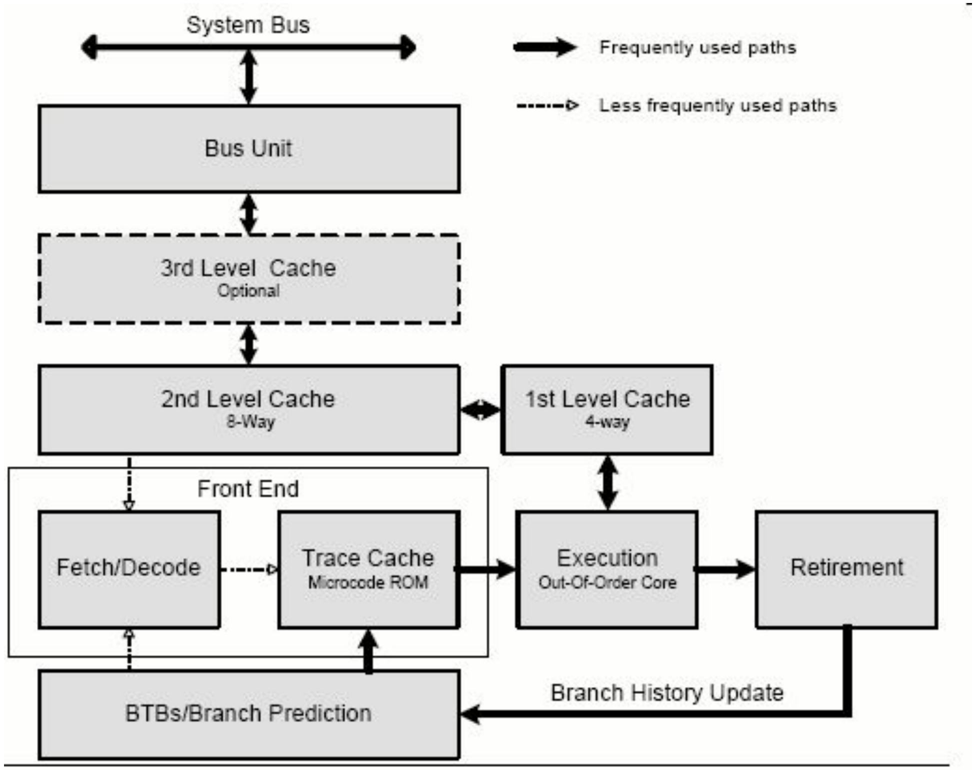


Lection
№*6*

Программная модель процессора: Регистры. Продолжение.



31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0	
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	PCE	PGE	MCE	PAE	PSE	DE	TSD	PVI	VME	CR4
PAGE DIRECTORY BASE																											PCD	PWT				CR3
PAGE FAULT LINEAR ADDRESS																																CR2
NON USABLED																																CR1
PG	CD	NW											AM		WP											NE	ET	TS	EM	MP	PE	CR0
31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0	



Управляющие регистры

Регистр cr0 содержит системные флаги, управляющие режимами работы микропроцессора и отражающие его состояние глобально, независимо от конкретных выполняющихся задач.
Назначение системных флагов:

pe (Protect Enable), бит 0 — разрешение защищенного режима работы.
Состояние этого флага показывает, в каком из двух режимов — реальном (pe=0) или защищенном (pe=1) — работает микропроцессор в данный момент времени.

mp (Math Present), бит 1 — наличие сопроцессора. Всегда 1.

ts (Task Switched), бит 3 — переключение задач. Процессор автоматически устанавливает этот бит при переключении на выполнение другой задачи.

am (Aligment Mask), бит 18 — маска выравнивания. Этот бит разрешает (am = 1) или запрещает (am = 0) контроль выравнивания.

cd (Cache Disable), бит 30, — запрещение кэш-памяти. С помощью этого бита можно запретить (cd = 1) или разрешить (cd = 0) использование внутренней кэш-памяти (кэш-памяти первого уровня).

pg (PaGing), бит 31, — разрешение (pg = 1) или запрещение (pg = 0) страничного преобразования. Флаг используется при страничной модели организации памяти.

Регистр CR0 является расширением регистра MSW процессора в котором были определены лишь биты PE, MP, EM и TS. Для обеспечения программной совместимости команды LMSW и SMSW, предназначавшиеся для процессоров , затрагивают только эти младшие 4 бита.

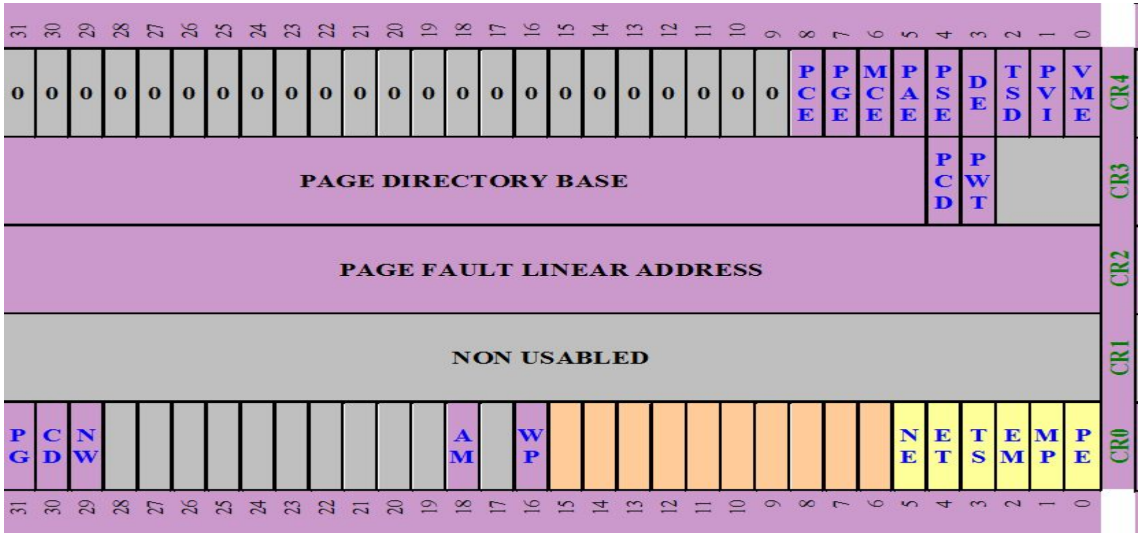
Регистры(CR[0÷3]) хранят признаки состояния процессора, общие для всех задач.

Регистр CR1 не используется.

Регистр CR2 (Page Fault Linear Address) хранит 32-битный линейный адрес, по которому был получен последний отказ страницы памяти.

Регистр CR3 (Page Directory Base Register) в старших 20 битах хранит физический базовый адрес таблицы каталога страниц. Из младших 12 бит в процессорах используются следующие:

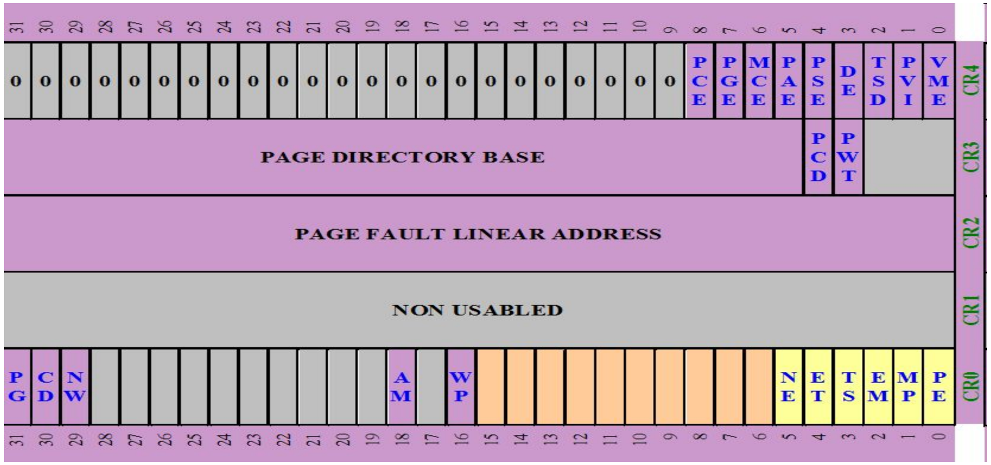
- PCD (Page-Level Cache Disable) — запрет кэширования страницы (один из источников аппаратного сигнала PCD для управления внешним кэшем);
- PWT (Page-Level Writes Trough) — кэширование страницы со сквозной записью (один из источников аппаратного сигнала PWT для управления внешним кэшем).



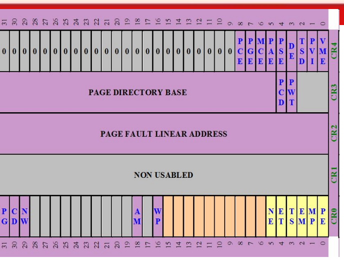
31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0	
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	PCE	PGE	MCE	PAE	PSE	DE	TSD	PVI	VME	CR4
PAGE DIRECTORY BASE																											PCD	PWT				CR3
PAGE FAULT LINEAR ADDRESS																																CR2
NON USABLED																																CR1
PG	CD	NW											AM		WP											NE	ET	TS	EM	MP	PE	CR0
31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0	

Регистр cr2 используется при страничной организации оперативной памяти для регистрации ситуации, когда текущая команда обратилась по адресу, содержащемуся в странице памяти, отсутствующей в данный момент времени в памяти. В такой ситуации в микропроцессоре возникает исключительная ситуация с номером 14, и линейный 32-битный адрес команды, вызвавшей это исключение, записывается в регистр cr2. Имея эту информацию, обработчик исключения 14 определяет нужную страницу, осуществляет ее подкачку в память и возобновляет нормальную работу программы;

Регистр cr3 также используется при страничной организации памяти.
Это так называемый регистр каталога страниц первого уровня. Он содержит 20-битный физический базовый адрес каталога страниц текущей задачи. Этот каталог содержит 1024 32-битных дескриптора, каждый из которых содержит адрес таблицы страниц второго уровня. В свою очередь каждая из таблиц страниц второго уровня содержит 1024 32-битных дескриптора, адресующих страничные кадры в памяти. Размер страничного кадра — 4 Кбайт.



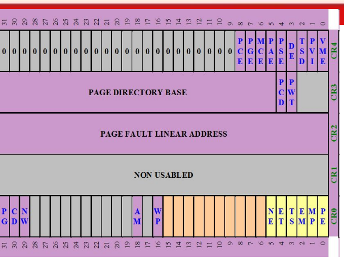
Регистр CR4 содержит биты разрешения архитектурных расширений



CR4: назначения битов

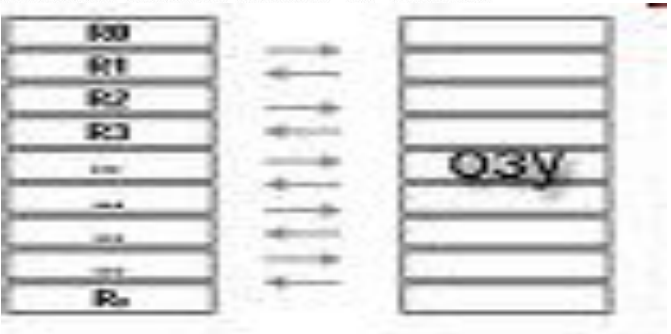
Регистр CR4 (присутствует в процессорах Pentium и выше) содержит биты разрешения архитектурных расширений. Назначение бит регистра CR4 представлено ниже.

- VME (Virtual-8086 Mode Extensions) — разрешение использования виртуального флага прерываний в режиме V86, что позволяет повысить производительность за счет сокращения лишних вызовов монитора виртуальных машин.
- PVI (Protected-Mode Virtual Interrupts) — разрешение использования виртуального флага прерываний в защищенном режиме.
- TSD (Time Stamp Disable) — превращение инструкции RDTSC (чтение счетчика меток реального времени) в привилегированную.
- DE (Debugging Extensions) — расширение возможностей отладки (разрешение точек останова на инструкциях обращения к заданным портам ввода-вывода).
- PSE (Page Size Extension) — расширение размера страницы (4 Кбайт и 4 Мбайт).
- PAE (Physical Addres Extension) — расширение физического адреса (страницы 4 Кбайт и 2 Мбайт, 36-битная адресация).
- MCE (Machine-Check Enable) — разрешение машинного контроля (выработки исключения #MC по машинной ошибке) (P5+).

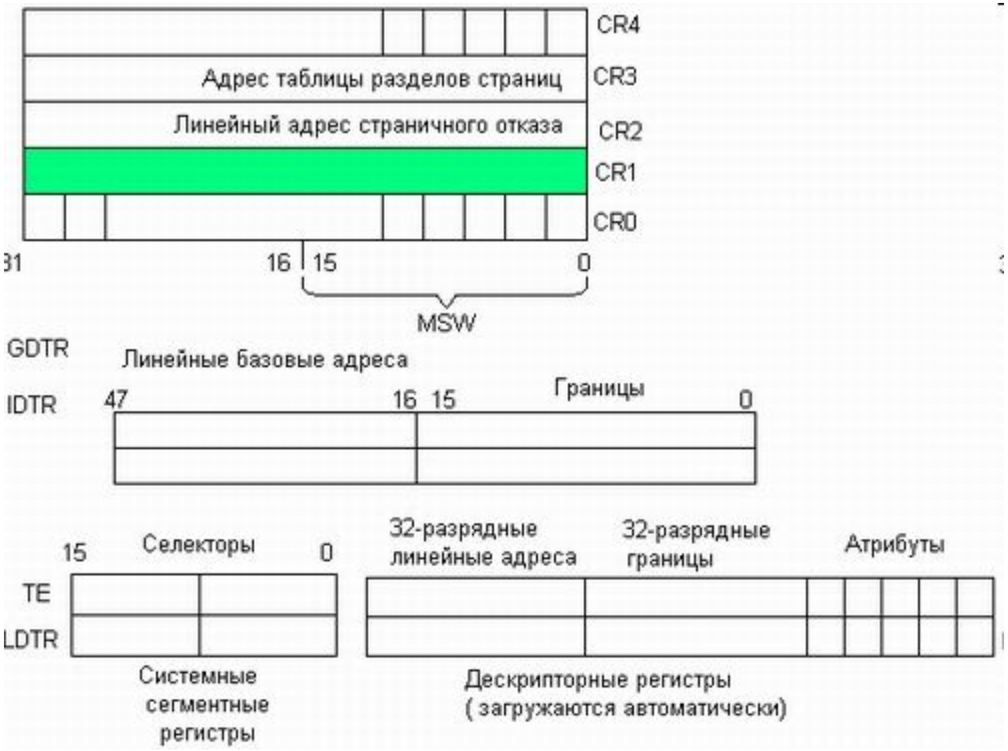


CR4: назначения битов

- `PGE` (Paging Global Extensions) — разрешение глобальности в страничной переадресации. При `PGE = 1` по команде `MOV CR3` в TLB очищаются только вхождения с неустановленным битом глобальности `G` (P6+).
- `PCE` (Performance-monitoring Counter Enable) — разрешение обращения к счетчикам событий (инструкция `RDPMC`) на любом уровне привилегий.
- `OSFXSR` — флаг использования инструкций `FXSAVE/FXRSTOR` для быстрого сохранения и восстановления состояния FPU/MMX при переключении контекста. При инициализации процессора флаг обнуляется; он может быть установлен операционной системой, если она эти инструкции использует, а процессор их поддерживает. Признак поддержки инструкций — бит `FXSR (EDX.24)` после вызова `CPUID(1)` (P6+).
- `OSXMMEXCPT` — флаг поддержки операционной системой исключений от блока XMM (SIMD-инструкций с плавающей точкой).



Регистры системных адресов



Эти регистры еще называют регистрами управления памятью. Они предназначены для защиты программ и данных в мультизадачном режиме работы микропроцессора.

При работе в защищенном режиме микропроцессора адресное пространство делится на: глобальное — общее для всех задач; локальное — отдельное для каждой задачи.

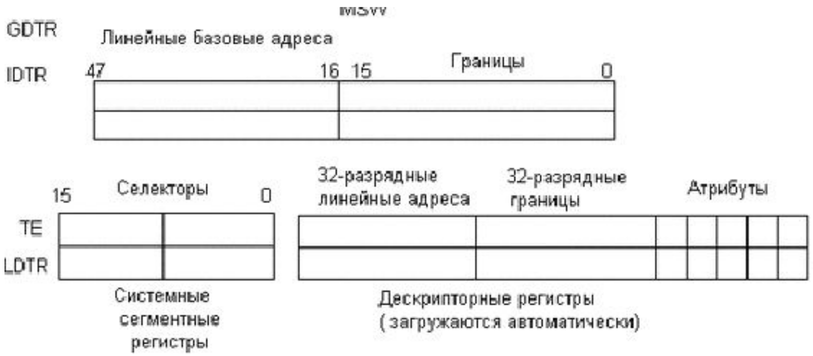
Регистры системных адресов

Разделением и объясняется присутствие в архитектуре микропроцессора следующих системных регистров:
регистра таблицы глобальных дескрипторов gdtr (Global Descriptor Table Register) имеющего размер 48 бит и содержащего 32-битовый (биты 16—47) базовый адрес глобальной дескрипторной таблицы GDT и 16-битовое (биты 0—15) значение предела, представляющее собой размер в байтах таблицы GDT;
регистра таблицы локальных дескрипторов ldtr (Local Descriptor Table Register) имеющего размер 16 бит и содержащего так называемый селектор дескриптора локальной дескрипторной таблицы LDT. Этот селектор является указателем в таблице GDT, который и описывает сегмент, содержащий локальную дескрипторную таблицу LDT;

Регистры системных адресов

Регистр таблицы дескрипторов прерываний idtr (Interrupt Descriptor Table Register) имеющего размер 48 бит и содержащего 32-битовый (биты 16–47) базовый адрес дескрипторной таблицы прерываний IDT и 16-битовое (биты 0—15) значение предела, представляющее собой размер в байтах таблицы IDT;

16-битового регистра задачи tr (Task Register), который подобно регистру ldtr, содержит селектор, то есть указатель на дескриптор в таблице GDT. Этот дескриптор описывает текущий сегмент состояния задачи (TSS — Task Segment Status). Этот сегмент создается для каждой задачи в системе, имеет жестко регламентированную структуру и содержит контекст (текущее состояние) задачи. Основное назначение сегментов TSS — сохранять текущее состояние задачи в момент переключения на другую задачу.



Регистры отладки

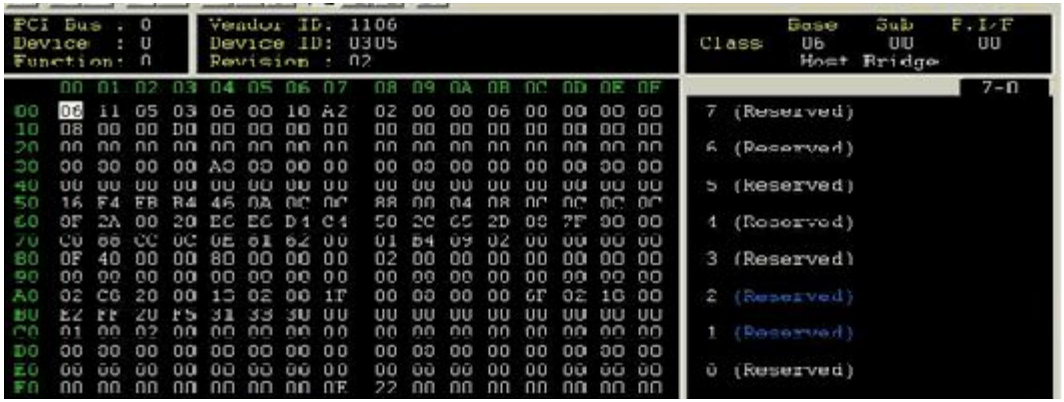
Регистры отладки (Debug Register) предназначены для задания и управления отладочными точками останова.

Регистры DR0...DR3 (Linear Breakpoint Address 0...3) хранят 32-битные линейные адреса точек останова.

Регистры DR4, DR5 в процессорах 80386 и 486 не используются, обращение к ним эквивалентно обращению к регистрам DR6, DR7. В процессоре Pentium при включенном расширении отладки обращение к этим регистрам вызывает исключение недопустимого кода операции (#UD).

Регистр DR6 (Breakpoint Status) отражает состояние контрольной точки.

Регистр DR7 (Breakpoint Control) управляет установкой контрольных точек.



```
PCI Bus  : 0     Vendor ID: 1106              Base   Sub   P.I/F
Device   : 0     Device ID: 0305       Class   06     00     00
Function: 0      Revision : 02                 Host Bridge

    00 01 02 03 04 05 06 07  08 09 0A 0B 0C 0D 0E 0F          7-0
00  06 11 05 03 06 00 10 A2  02 00 00 06 00 00 00 00    7 (Reserved)
10  08 00 00 D0 00 00 00 00  00 00 00 00 00 00 00 00
20  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00    6 (Reserved)
30  00 00 00 00 A0 00 00 00  00 00 00 00 00 00 00 00
40  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00    5 (Reserved)
50  16 F4 EB B4 46 0A 0C 0C  88 00 04 08 0C 0C 0C 0C
60  0F 2A 00 20 EC EC D4 C4  50 2C C5 2D 03 7F 00 00    4 (Reserved)
70  C0 66 CC 0C 0E 61 62 00  01 B4 09 02 00 00 00 00
80  0F 40 00 00 80 00 00 00  02 00 00 00 00 00 00 00    3 (Reserved)
90  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
A0  02 C6 20 00 13 02 00 1F  00 00 00 00 6F 02 10 00    2 (Reserved)
B0  E2 FF 20 F5 31 33 30 00  00 00 00 00 00 00 00 00
C0  01 00 02 00 00 00 00 00  00 00 00 00 00 00 00 00    1 (Reserved)
D0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
E0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00    0 (Reserved)
F0  00 00 00 00 00 00 00 0E  22 00 00 00 00 00 00 00
```

Регистры тестирования

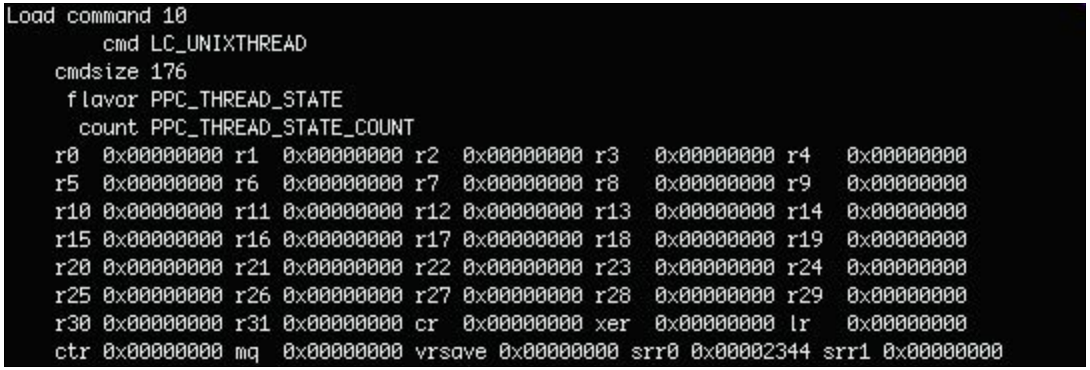
Состав *регистров тестирования* (Test Register) варьируется в зависимости от типа процессора. Процессоры имели только два регистра, предназначенных для тестирования кэша страничной переадресации — TR6 и TR7, для процессора состав регистров расширен: TR3 — регистр данных внутреннего кэша, TR4 — тестовый регистр состояния кэша, TR5 — управляющий регистр тестирования кэша, TR6 (Test Control) — управляющий регистр для теста кэширования страниц, TR7 (Test Status) — регистр данных для теста кэширования страниц.

В процессорах Pentium и выше тестовые регистры входят в группу модельно-специфических регистров MSR. Для этих процессоров обращение к регистрам TRx вызывает исключение #UD недопустимого кода операции.

Модельно-специфические регистры

Модельно-специфические регистры `MSR` (Model-Specific Registers) предназначены для управления расширениями отладки, мониторингом производительности, машинным контролем, кэшированием областей физической памяти и другими функциями. Их назначение привязывается к микроархитектуре конкретного процессора, состав меняется от модели к модели, доступ привилегирован. Инструкции обмена с этими 64-битными регистрами подразумевают, что данные находятся в паре `EDX:EAX`, а номер указывается в регистре `ECX`, что позволяет неограниченно (до 4 миллиардов) увеличивать число этих регистров.

Доступность регистров различных групп зависит от режима работы процессора и уровня привилегий задачи. В табл. показана возможность загрузки (занесения значения в регистр) различных регистров и сохранения их в памяти в трех режимах работы процессора.

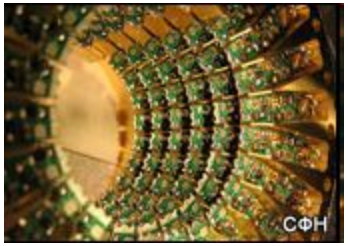


```
Load command 10
        cmd LC_UNIXTHREAD
    cmdsize 176
     flavor PPC_THREAD_STATE
      count PPC_THREAD_STATE_COUNT
    r0  0x00000000 r1  0x00000000 r2  0x00000000 r3   0x00000000 r4   0x00000000
    r5  0x00000000 r6  0x00000000 r7  0x00000000 r8   0x00000000 r9   0x00000000
    r10 0x00000000 r11 0x00000000 r12 0x00000000 r13  0x00000000 r14  0x00000000
    r15 0x00000000 r16 0x00000000 r17 0x00000000 r18  0x00000000 r19  0x00000000
    r20 0x00000000 r21 0x00000000 r22 0x00000000 r23  0x00000000 r24  0x00000000
    r25 0x00000000 r26 0x00000000 r27 0x00000000 r28  0x00000000 r29  0x00000000
    r30 0x00000000 r31 0x00000000 cr  0x00000000 xer  0x00000000 lr   0x00000000
    ctr 0x00000000 mq  0x00000000 vrsave 0x00000000 srr0 0x00002344 srr1 0x00000000
```

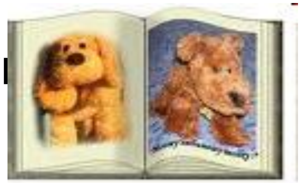
Доступность регистров процессора

Режим	**Реальный**		**Защищенный**		**Виртуального 8086**	
Регистры	**Загрузка**	**Сохранение**	**Загрузка**	**Сохранение**	**Загрузка**	**Сохранение**
Общего назначения	Да	Да	Да	Да	Да	Да
Сегментов	Да	Да	Да	Да	Да	Да
Флагов	Да	Да	Да	Да	IOPL[1]	IOPL[1]
Управляющие	Да	Да	PL=0	PL=0	Нет	Да
GDTR, IDTR	Да	Да	PL=0	Да	Нет	Да
LDTR, TR	Нет	Нет	PL=0	Да	Нет	Нет
Отладки	Да	Да	PL=0	PL=0	Нет	Нет
Тестирования	Да	Да	PL=0	PL=0	Нет	Нет
MSR	PL=0	PL=0	PL=0	PL=0	Нет	Нет

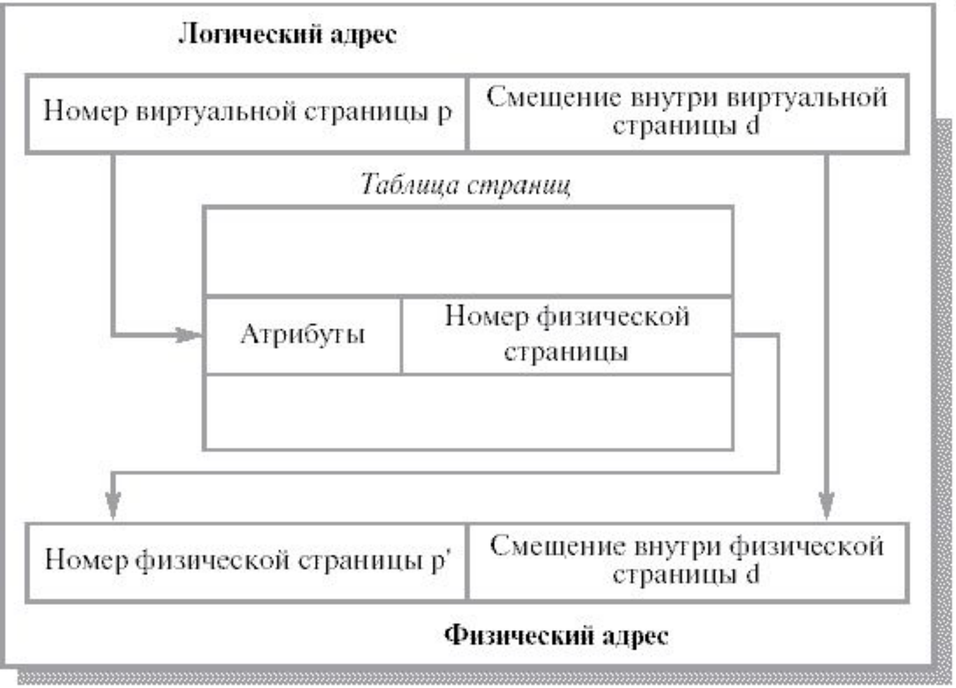
[1] PUSHF и POPF чувствительны к уровню привилегий.



Используемая литература:



- Книга «Ассемблер. Учебник для ВУЗов», авторы Михаил Гу Юров
- Книга «Архитектура ЭВМ»,автор Мюллер
- *http://www.studfiles.ru/dir/cat32/subj79/file970/view1954.html*
- http://adept7.narod.ru/library/programming/asm/guide/text/cpumodel.htm
- http://www.intuit.ru/department/hardware/mpbasics/13/4.html
- http://www.studfiles.ru/dir/cat32/subj58/file8417
- http://bhv.ru/books/full_contents.php?id=14006



Логический адрес

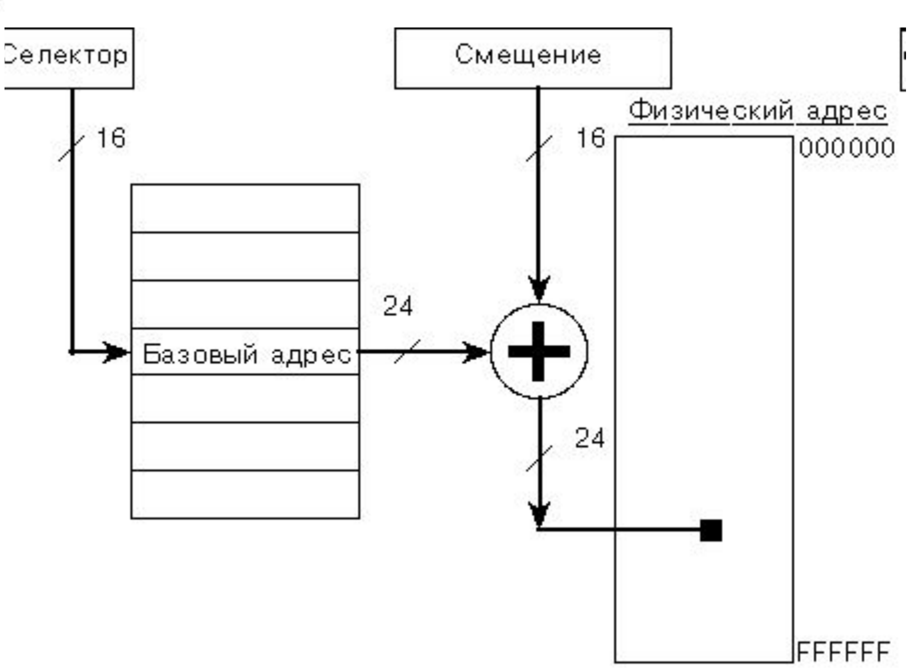
Номер виртуальной страницы p | Смещение внутри виртуальной страницы d

Таблица страниц

Атрибуты | Номер физической страницы

Номер физической страницы p' | Смещение внутри физической страницы d

Физический адрес

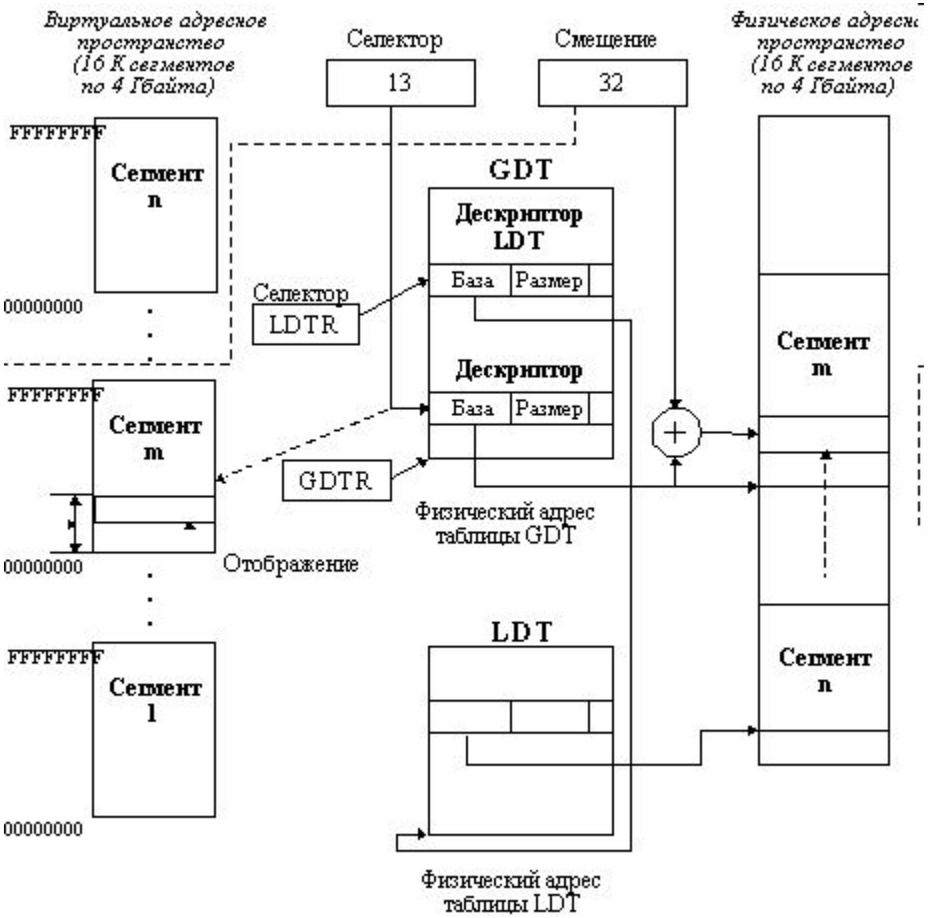


Селектор

Смещение

Физический адрес

Базовый адрес


Виртуальное адресное пространство (16 К сегментов по 4 Гбайта)
Селектор
13
Смещение
32
Физическое адресн
пространство (16 К сегментов по 4 Гбайта)
FFFFFFFF
Сегмент n
00000000
GDT
Дескриптор LDT
База
Размер
Селектор
LDTR
Дескриптор
База
Размер
FFFFFFFF
Сегмент m
GDTR
Физический адрес таблицы GDT
00000000
Отображение
Сегмент m
LDT
FFFFFFFF
Сегмент l
00000000
Сегмент n
Физический адрес таблицы LDT