Second Page

به نام خدا

- **فصل ٦ :**
  - حالت حفاظت شده در پردازنده پنتیوم
  - کتاب ریز پردازنده های پیشرفته از ۸۰۸۶ تا پنتیوم

- **استاد مربوطه :** دکتر جوادی مقدّم
- **تهیه کننده :** شاهین نباتی
- ترم بهمن ۹۹

مقدمه

- پردازنده های خانواده اینتل از۸۰۲۸۶ به بعد در دو حالت حقیقی و حفاظت شده عمل می نمایند.

- حالت حقیقی منطبق با ریزپردازنده ۸۰۸۶ می باشد اما حالت حفاظت شده مشخصات کاملاً متفاوتی دارد و بیشتر توانایی های ریزپردازنده های خانواده اینکه از جمله پردازنده پنتیوم مربوط به این حالت می شود.

- حالت حفاظت شده در پردازنده پنتیوم مشابه ۸۰۲۸۶ می‌باشد و توضیحاتی که در این فصل ارائه می‌شود حالت حفاظت شده در سایر ریزپردازنده های این خانواده را نیز در بر می‌گیرد.

٦-١) حالت حقیقی در پنتیوم

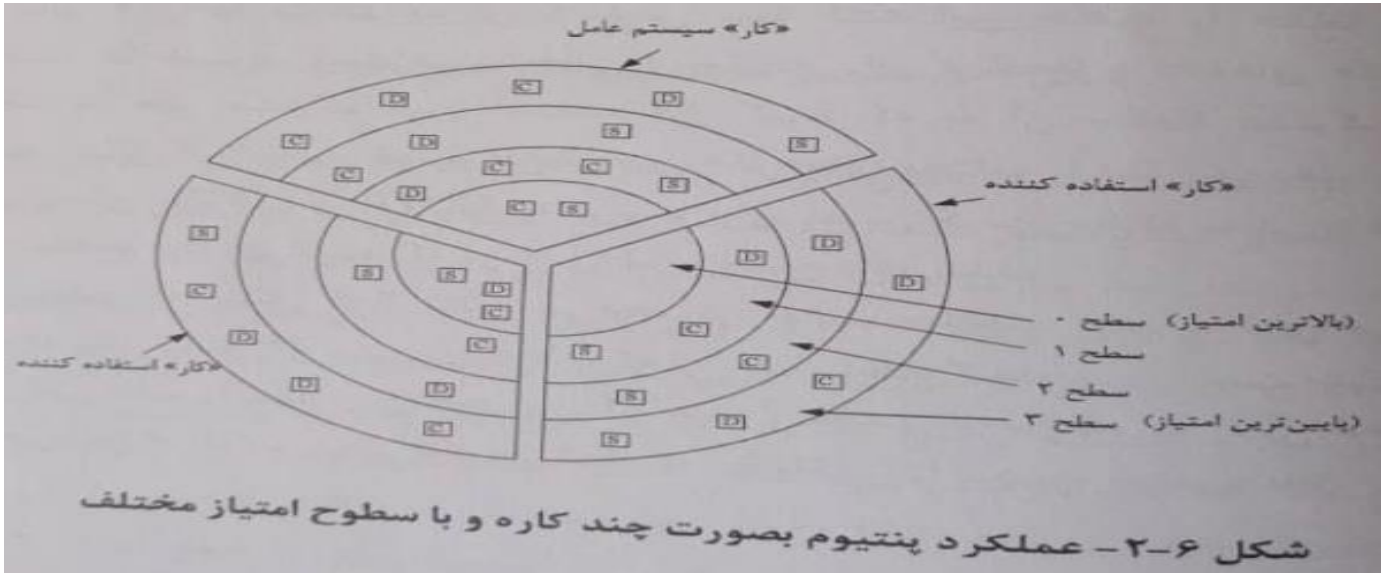
- توضیحاتی که در فصل های ۳ و ۴ دوستان ارئه کردن درمورد حالت حقیقی ریز پردازنده پنتیوم نیز کاملا معتبره به همین دلیل در اینجا از اونها خودداری میکنیم و تنها امکانات اضافه شده در این حالت را توضیح میدهیم.

- هنگامی که ریزپردازنده در حالت حقیقی قرار می‌گیرد به طور معمول صرفاً از ثبات های منطبق با ۸۰۸۶ استفاده می‌کند.

- پردازنده پنتیوم در حالت حقیقی به راحتی می‌توانند از دو ثبات سگمنت و GS که از نوع داده می باشد استفاده نماید.

ویژگی های ریز پردازنده پنتیوم در حالت حفاظت شده

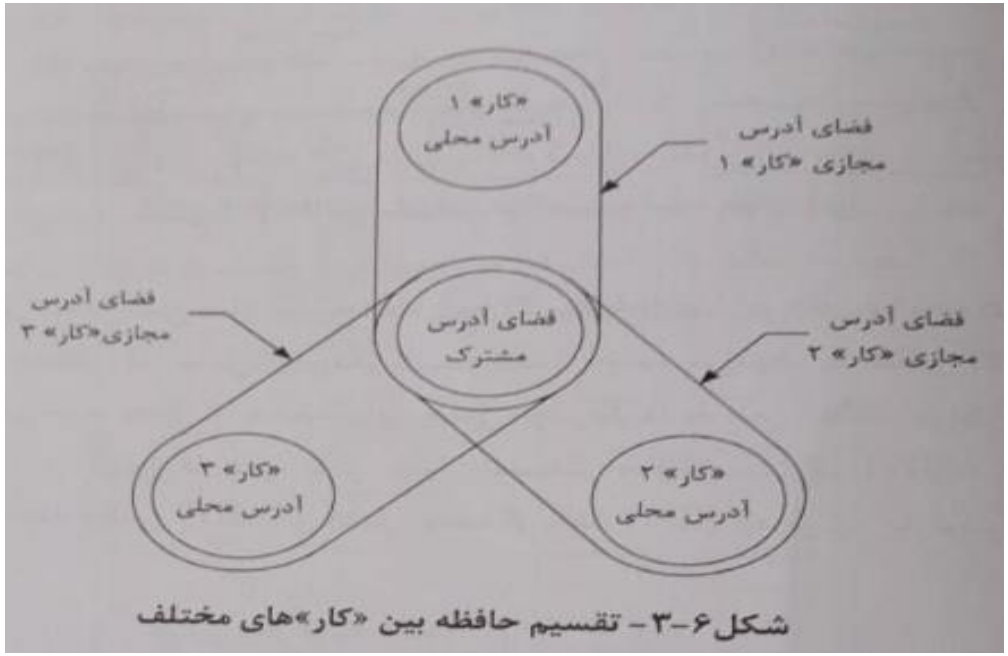
- در حالت حفاظت شده که به آن حالت آدرس دهی حفاظت شده نیز می گویند، عملکرد ریزپردازنده از جهات مختلف متفاوت و بسیار قوی‌تر از حالت حقیقی است.
- عمل کردن به صورت چند کاره از ویژگی‌های دیگر حالت حفاظت شده است.
- همانطور که در شکل زیر نشان داده شده است ریزپردازنده می‌تواند از چند کار مختلف تشکیل شود به عنوان مثال یکی از کارهای مربوط به برنامه های سیستم عامل و دو کار دیگر مربوط به دو استفاده کننده ی مختلف خواهد بود



شکل ۶-۲- عملکرد پنتیوم بصورت چند کاره و با سطوح امتیاز مختلف

۶-۳) نحوه ی آدرس کردن حافظه

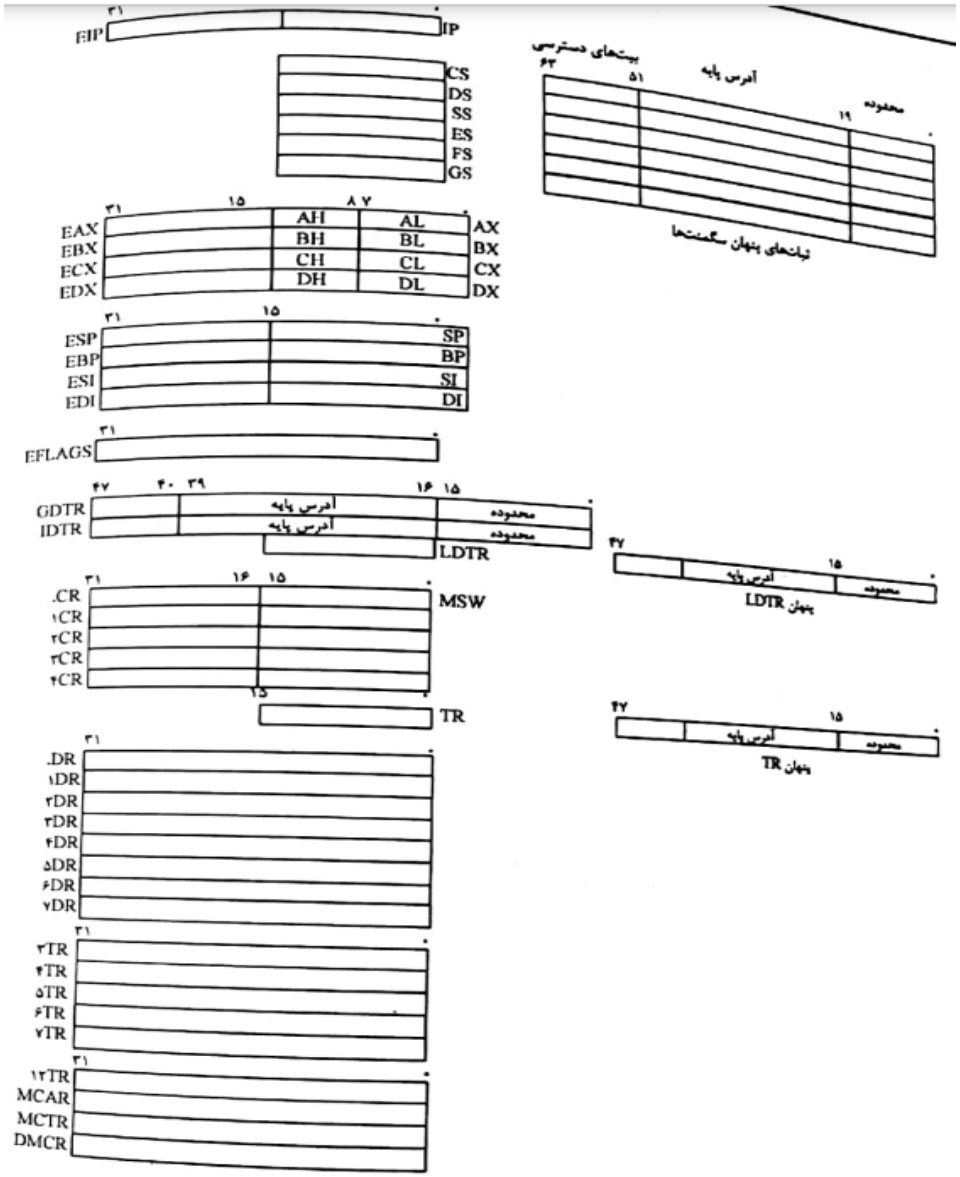
- که در حال حقیقی مانند روشی که در پردازنده ۸۰۸۶ دیدیم عمل می‌شود اما در حالت حفاظت‌شده روش کار کاملاً متفاوت است.
- در حالت حفاظت شده از آنجایی که ریزپردازنده به صورت چندکاره عمل می‌کند هر کار نیاز به یک حافظه مستقل دارد که سایر کارها نتوانند به آن دسترسی پیدا کنند.
- این حافظه را حافظه محلی می‌نامند. همانطور که در شکل نشان داده شده است در حالت حفاظت شده به ازای هر ثبات سگمنت یک ثبات ۶۴ بیتی وجود دارد که از دید استفاده کننده پنهان است.



شکل۶-۳- تقسیم حافظه بین «کار»های مختلف

توصیفگر ها

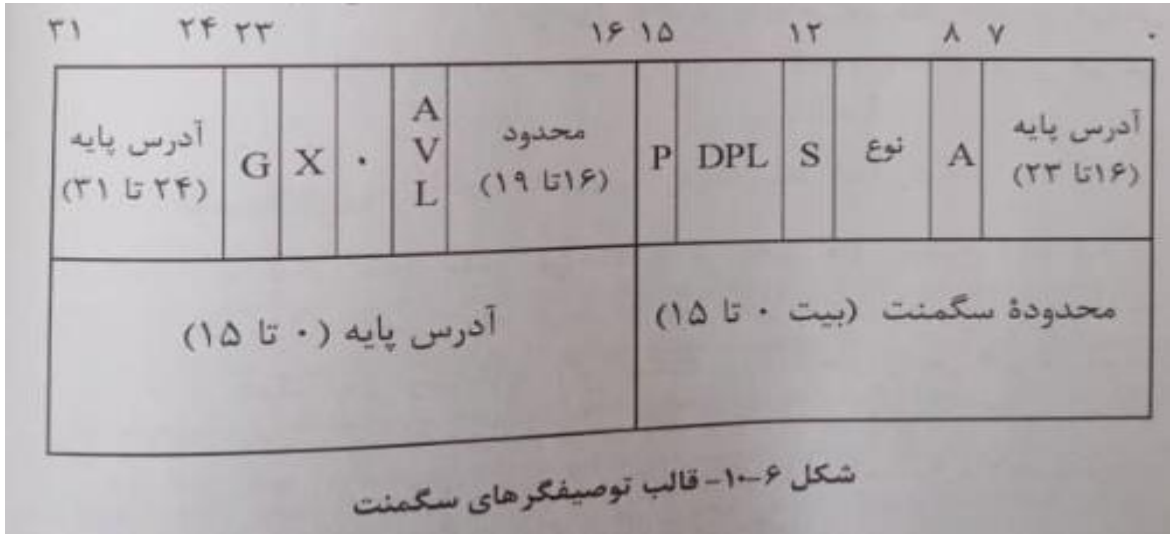
- ریزپردازنده به کمک این توصیفگر ها آدرس برنامه و داده را به دست می آورد و می تواند از دسترسی غیرمجاز کاربران به آنها جلوگیری نمایند.
-
- این توصیفگر ها به دو گروه ۱- توصیف گرهای سگمنت و ۲- توصیف گر های سیستم تقسیم می شوند که در زیر آنها را توضیح می دهیم.



شکل ۵-۲- ثبات‌های داخلی ریزپردازندهٔ پنتیوم

توصیفگر های سگمنت

- ریز پردازنده پنتیوم دارای شش ثبات سگمنت است.
- ثبات سگمنت برنامه که برای دسترسی به برنامه مورد استفاده قرار می گیرد و با دستورالعمل های CALL و JUMP تغییر می کند.
- ثبات انباره که برای دسترسی به انبار کاربرد دارد و چهار ثبات سگمنت داده که برای دسترسی به سگمنت های برنامه به کار می روند.
- هر یک از شش ثبات سگمنت فوق دارای یک توصیفگر ۶۴ بیتی است که در ثبات پنهان آن قرار می گیرد.

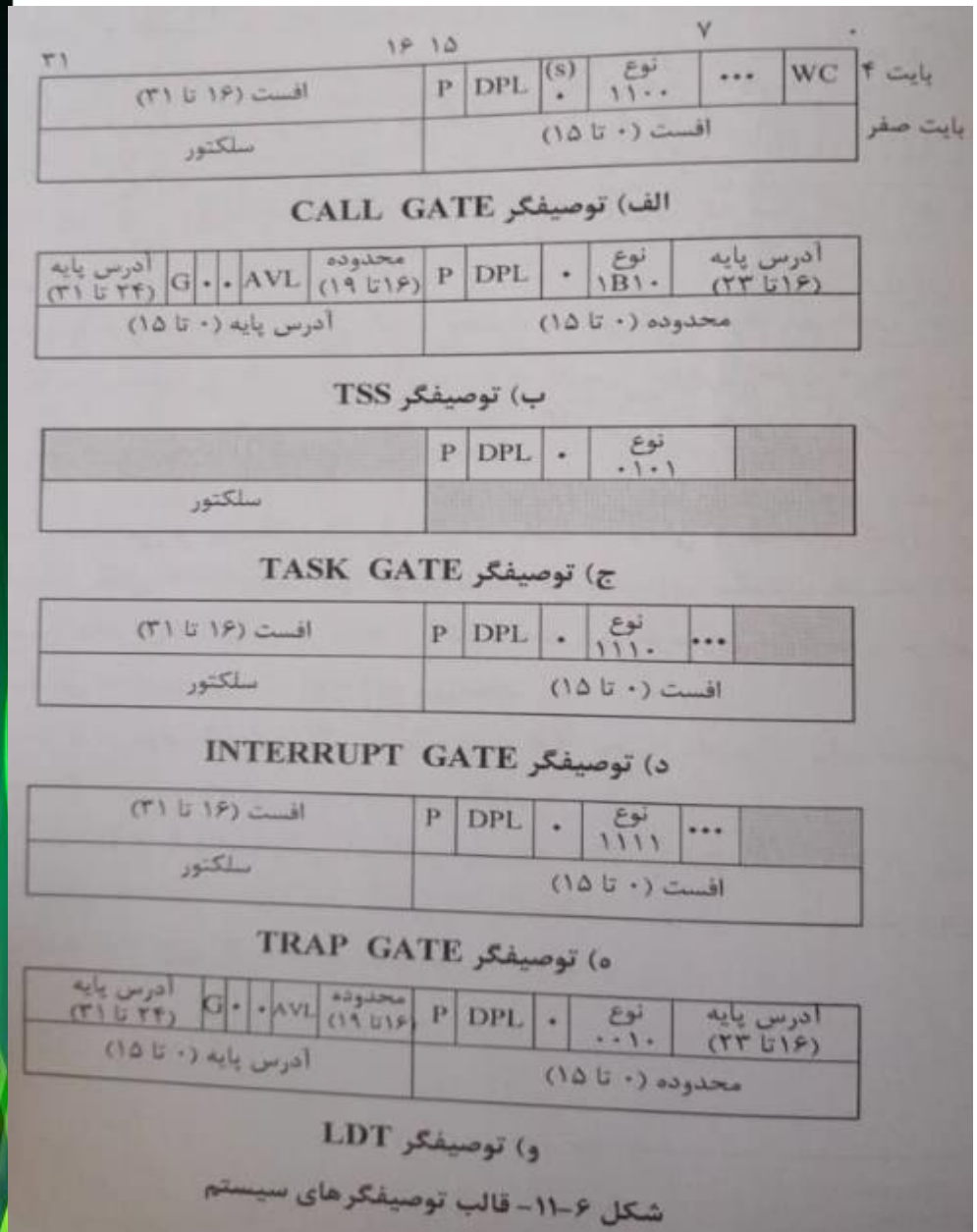


شکل ۶-۱۰- قالب توصیفگرهای سگمنت

توصیفگر های سیستم

- توصیفگر های سیستم یا توصیفگرهای سگمنت سیستم مستقیماً برای دسترسی به برنامه و داده مورد استفاده قرار نمی گیرند بلکه ریزپردازنده از این توصیفگر ها برای اجرای عملیات مربوط به سیستم مانند اجرای ریز برنامه‌های وقفه و تغییر کار استفاده می کند.

- شکل رو به رو قالب توصیفگرهای سیستم که در در پنتیوم مورد استفاده قرار می گیرد را نشان می دهد:



۳۱ ۱۶ ۱۵ ۷ ۰

بایت ۴: WC | ... | نوع ۱۱۰۰ | (S) ۰ | DPL | P | افست (۱۶ تا ۳۱)

بایت صفر: افست (۰ تا ۱۵) | سلکتور

الف) توصیفگر CALL GATE

آدرس پایه (۲۴ تا ۳۱) | G | ۰ | ۰ | AVL | محدوده (۱۶تا ۱۹) | P | DPL | ۰ | نوع ۱B۱۰ | آدرس پایه (۱۶تا ۲۳)

آدرس پایه (۰ تا ۱۵) | محدوده (۰ تا ۱۵)

ب) توصیفگر TSS

P | DPL | ۰ | نوع ۰۱۰۱

سلکتور

ج) توصیفگر TASK GATE

افست (۱۶ تا ۳۱) | P | DPL | ۰ | نوع ۱۱۱۰ | ...

سلکتور | افست (۰ تا ۱۵)

د) توصیفگر INTERRUPT GATE

افست (۱۶ تا ۳۱) | P | DPL | ۰ | نوع ۱۱۱۱ | ...

سلکتور | افست (۰ تا ۱۵)

ه) توصیفگر TRAP GATE

آدرس پایه (۲۴ تا ۳۱) | G | ۰ | ۰ | AVL | محدوده (۱۶تا ۱۹) | P | DPL | ۰ | نوع ۰۰۱۰ | آدرس پایه (۱۶تا ۲۳)

آدرس پایه (۰ تا ۱۵) | محدوده (۰ تا ۱۵)

و) توصیفگر LDT

شکل ۶-۱۱- قالب توصیفگرهای سیستم

نحوه حفاظت از برنامه و داده

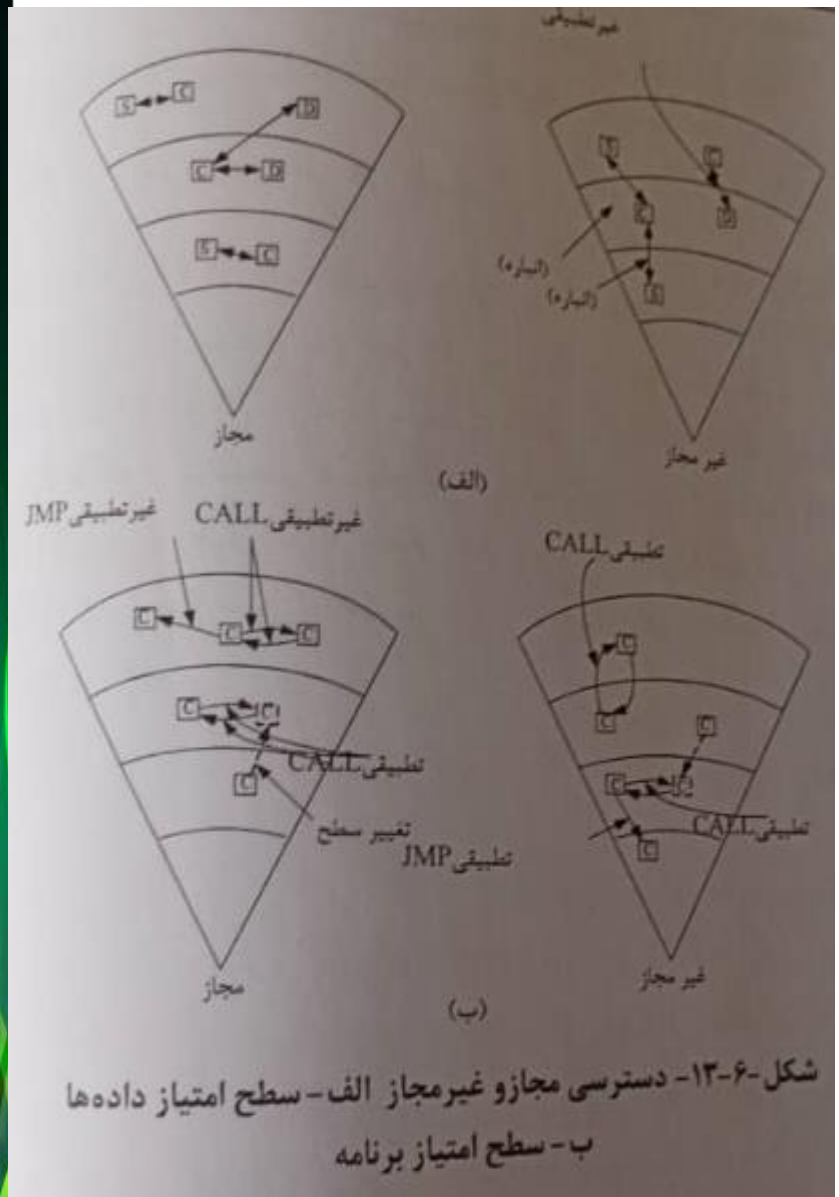
- در اسلاید های گذشته در مورد نحوه آدرس کردن حافظه در حالت حفاظت شده و توصیفگر های مورد استفاده گفته شد.
- در این بخش نحوه ی حفاظت از برنامه و داده ها و چگونگی استفاده از توصیفگر هارا می گوییم :

- مهمترین اقدامی که ریزپردازنده برای حفاظت انجام می دهد بررسی سطح امتیاز برنامه و یا داده است.
- به این منظور سه شاخصه سطح امتیاز یعنی RPL,CPL,DPL باید با یکدیگر مقایسه شوند.
- مقایسه این سه شاخص همیشه یکسان نمی باشد بلکه به شرایط و حالت های تعریف شده برای این پردازنده و نوع توصیفگر بستگی دارد در بخش های بعد به او می پردازیم.

کارهای با یک سطح امتیاز

- در این بخش نحوه حفاظت از برنامه ها و داده ها در حالتی که تمام سگمنت های برنامه در یک سطح امتیاز هستند را توضیح می دهیم :

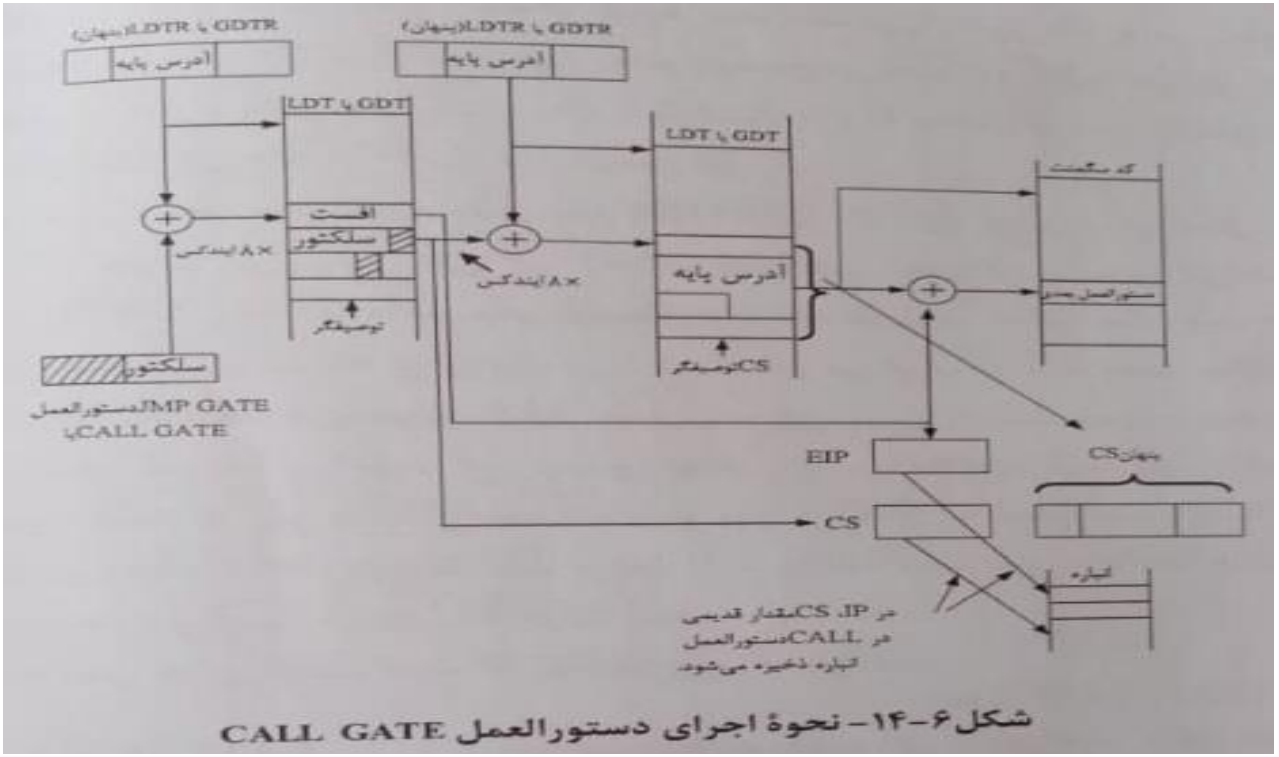
- در این حالت به عنوان مثال اگر برنامه در حال اجرا در سطح امتیاز ۲ قرار داشته باشد تنها می‌تواند از برنامه‌هایی در همین سطح امتیاز استفاده نماید و استفاده از برنامه هایی در سطح امتیاز بالاتر و پایین تر مجاز نمی باشد



شکل-۶-۱۳- دسترسی مجازو غیرمجاز الف- سطح امتیاز داده‌ها
ب- سطح امتیاز برنامه

کارهای با چند سطح امتیاز

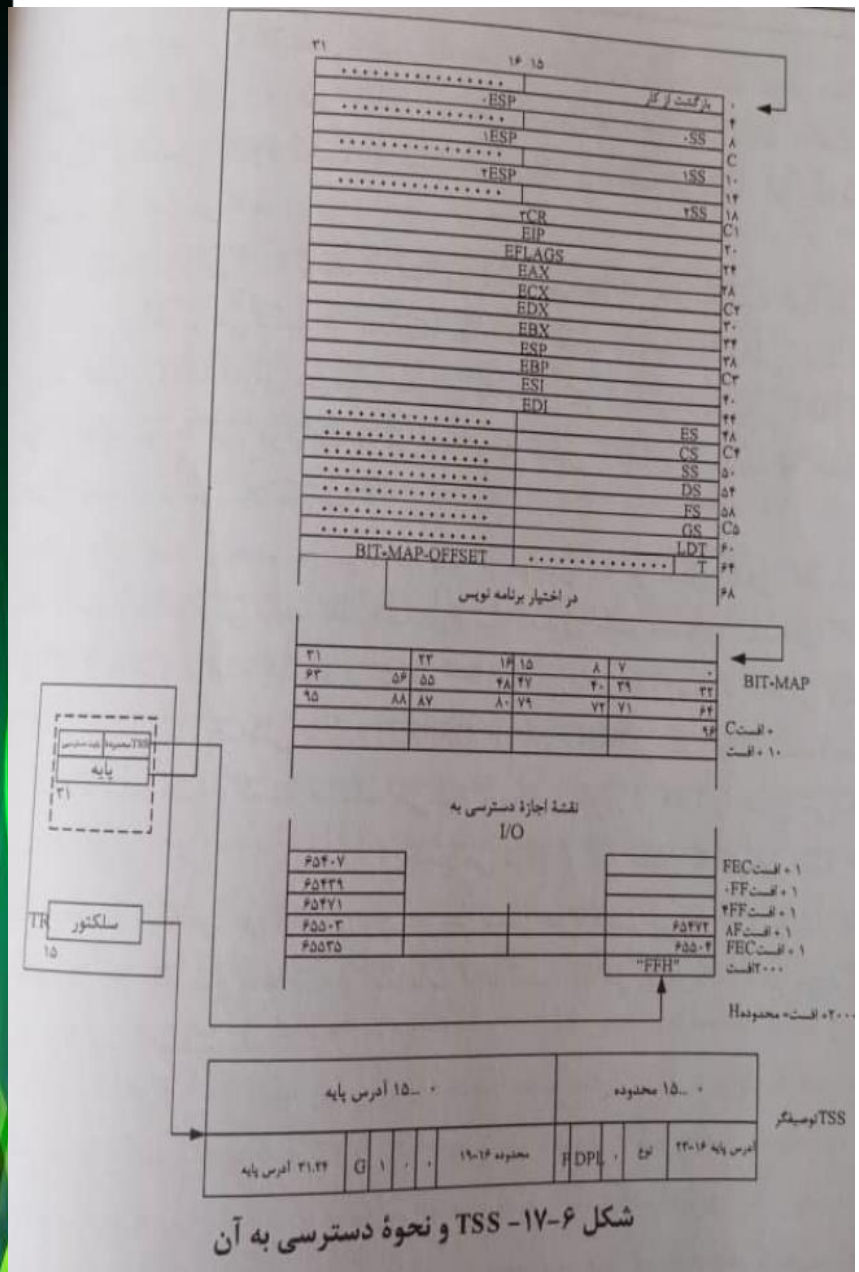
- در این قسمت می خواهیم بگوییم که چگونه می‌توان به برنامه‌های با سطوح بالاتر هم رفت و یا از آنها استفاده کرد یا به عبارت دیگر کارهای با چند سطح امتیاز می‌تواند در اختیار برنامه نویس نیز قرار گیرد.
- این عمل توسط توصیفگر جدیدی به نام CALL GATE و اجرای دستورالعملی با همین نام صورت می گیرد.
- شکل زیر قالب این توصیف کرده را نشان میدهد :



شکل۶-۱۴- نحوهٔ اجرای دستورالعمل CALL GATE

عمل با چند کار

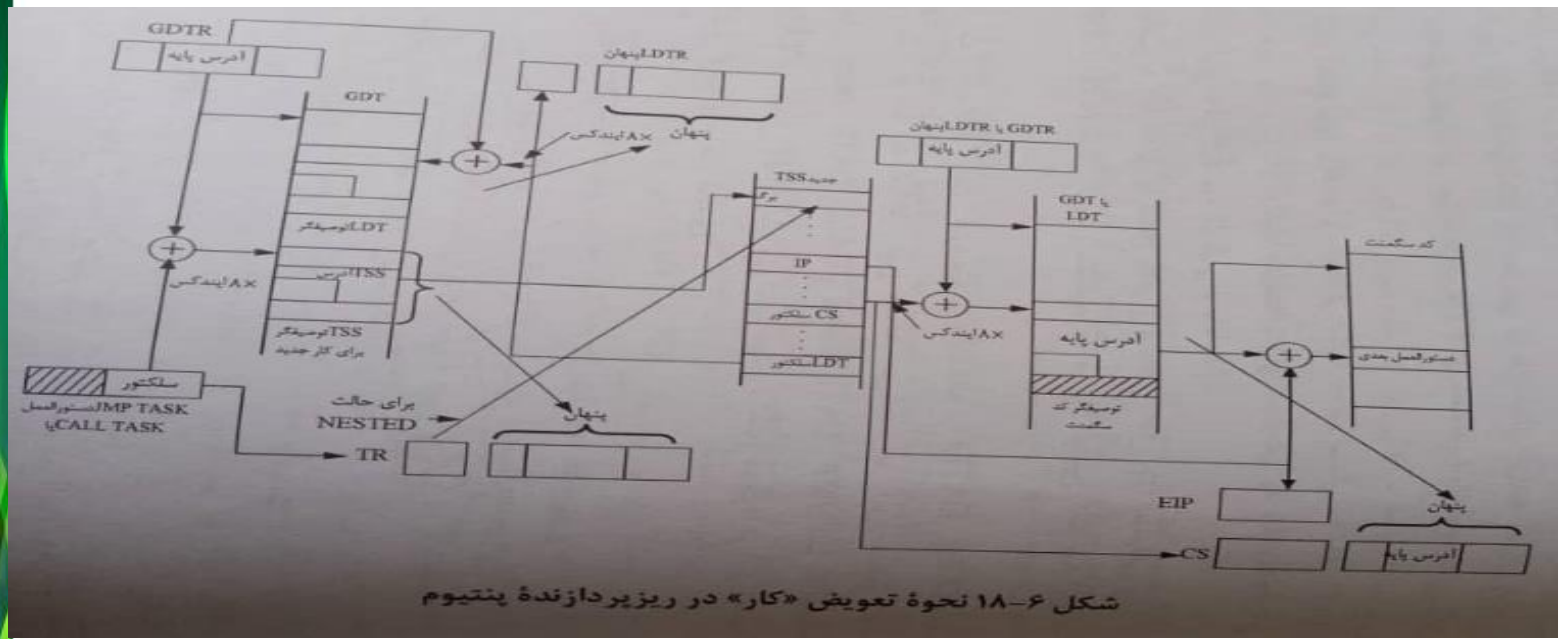
- تاکنون همه توضیحات مربوط به عمل در یک کار بود در اینجا نحوه عمل در چند کار را توضیح می دهیم :
- به منظور تغییر کار برای هر کار بخشی به نام سگمنت وضعیت کار در جدول GDT در نظر گرفته شده است.
- جدول TSS به دوقسمت ایستا و پویا تقسیم می شود :
- ۱- قسمت ایستا در ابتدای کار برای یک بار برنامه نویسی شده و در طول کار سیستم ثابت می‌ماند
- ۲- قسمت پویا در هنگام تعویض کار تغییر می‌کند ۴ بایت اول از TSS مربوط به بازگشت از کار است این قسمت به صورت پویا عمل می کند.



شکل ۶-۱۷- TSS و نحوهٔ دسترسی به آن

عمل با چند کار

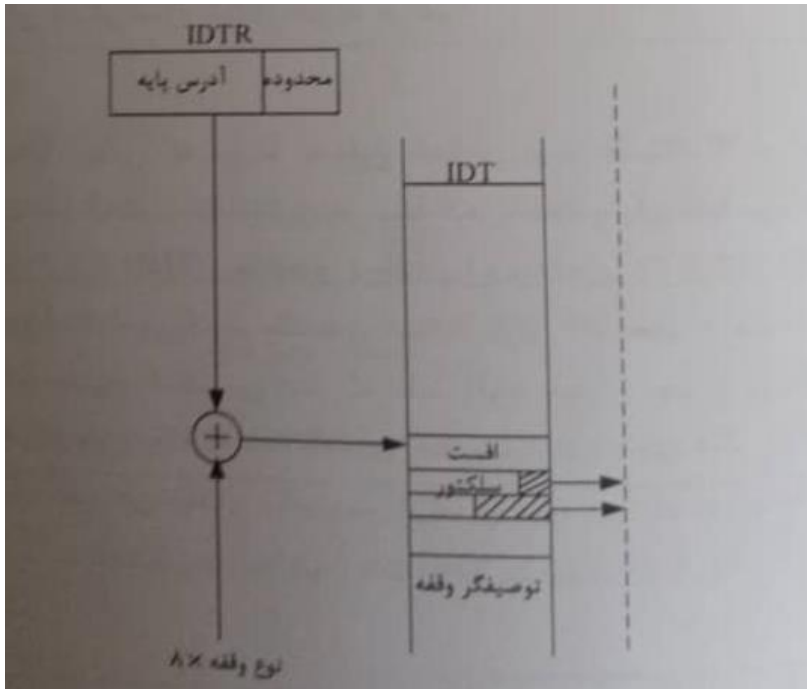
- شرکل زیر مراحل مختلف تغییر کار را نشان می‌دهد که در زیر به توضیح این مراحل می پردازیم :
- ۱- محتوای کلیه ثبات ها در کار فعلی در خانه مربوط در TSS ذخیره می گردد.
- ۲- ۲ بایت دوم عملوند دستورهای CALL و یا JMP در ثبات TR قرار گرفته
- ۳- محتوای توصیفگر TSS در ثبات پنهان TR قرار می‌گیرد وجدول TSS آدرس می‌شود
- ۴- مقدار ثبات TR قبلی که مربوط به کار قبل می‌شود در خانه اول TSS ذخیره می شود
- ۵- با قرار گرفتن مقادیر جدید در ثبات های CS و IP مراحل بعد مانند اجرای دستورالعمل CALL و یا JMP معمولی می باشد



شکل ۶-۱۸ نحوهٔ تعویض «کار» در ریزپردازندهٔ پنتیوم

وقفه در حالت حفاظت شده

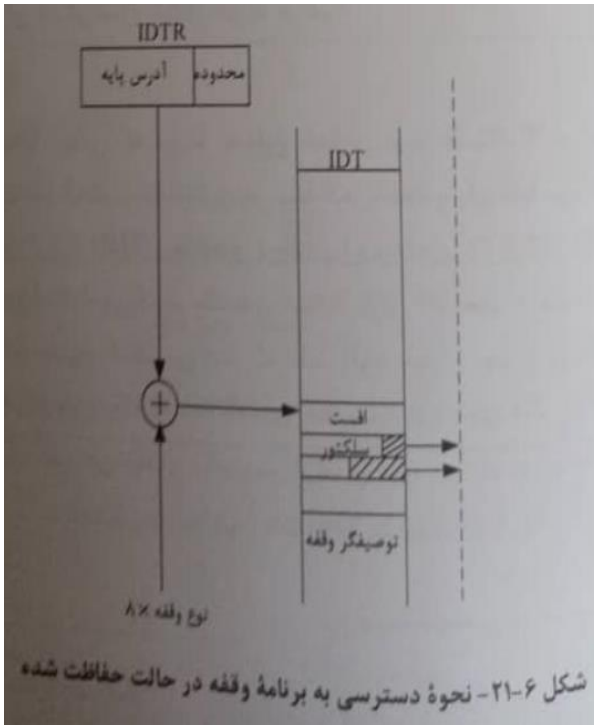
- وقف در پردازنده پنتیوم در دو حالت انجام می‌شود :
- ۱- در حالت حقیقی مانند ریزپردازنده ۸۰۸۶ است که در فصل سوم دوستان آن را توضیح دادند
- ۲- وقفه در حالت حفاظت شده و تفاوت های جزئی وقفه در حال حقیقی را شرح می دهیم



شکل ۶-۲۱- نحوهٔ دسترسی به برنامهٔ وقفه در حالت حفاظت شده

نحوه دسترسی به برنامه وقفه

- در حالت حفاظت شده مانند حالت حقیقی جمعا می توانیم تا ۲۵۶ وقفه داشته باشیم.
- در اینجا برای دسترسی به برنامه هر وقفه به یک توصیفگر آدرس در جدول قرار داده شده است مانند سایر توصیفگر ها در اینجا نیز هر توصیفگر از ۸ بایت تشکیل شده است.
- شکل زیر نحوه دسترسی به توصیفگرهای جدول IDT و در نهایت آدرس برنامه وقفه را نشان می‌دهد.
- همانطور که میبینید به دنبال ارسال هر وقفه، نوع وقفه نیز از داخل و خارج از پردازنده در یک بایت مشخص می گردد.

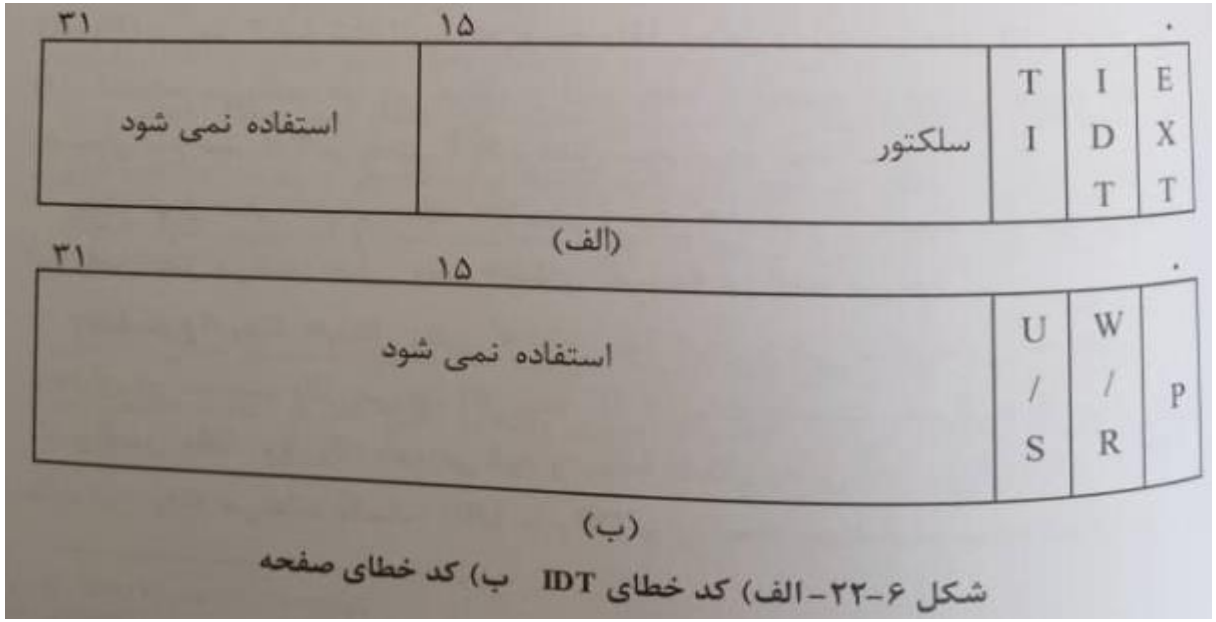


شکل ۶-۲۱- نحوهٔ دسترسی به برنامهٔ وقفه در حالت حفاظت شده

کد خطا

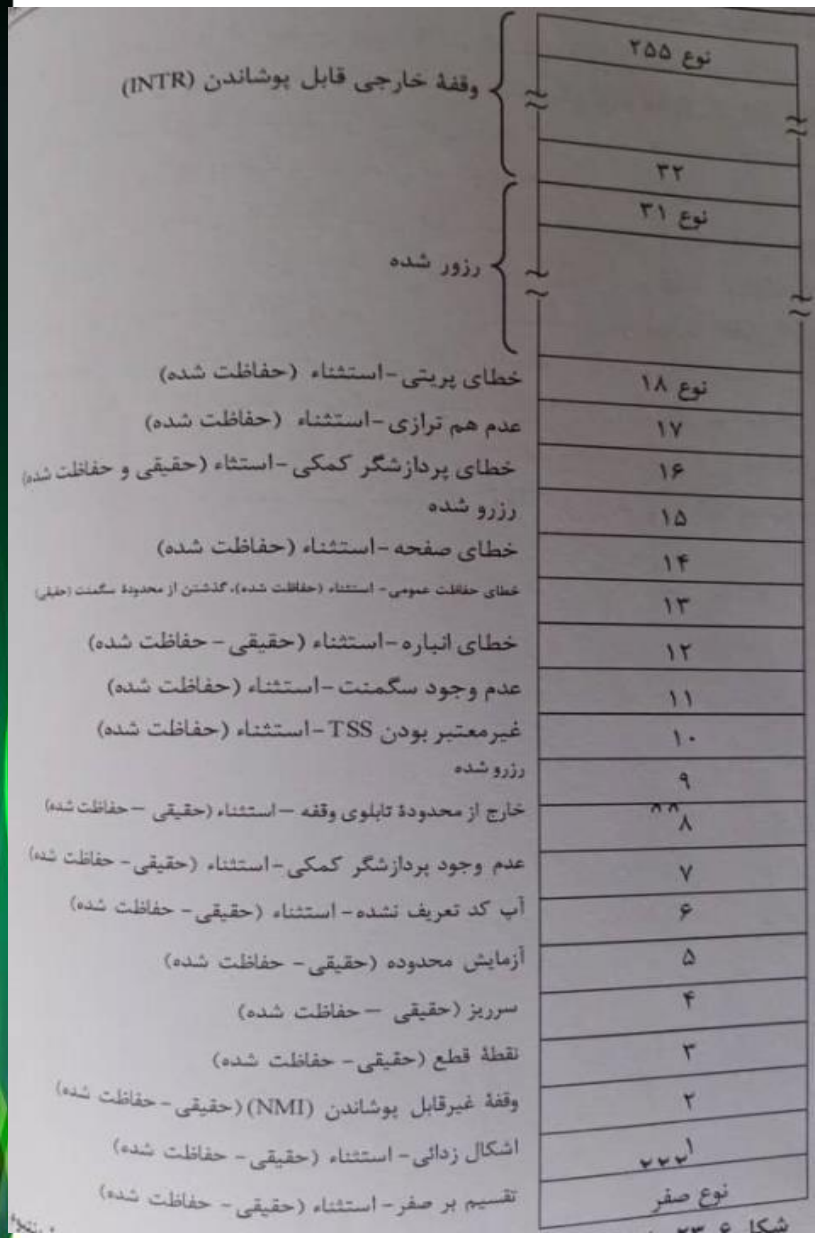
- در بین وقفه ها آنهایی که مربوط به وقوع خطا می شوند استثنا نامیده می‌شوند
- وقفه های استثنا کمک بسیار موثری در پیدا کردن خطا و رفع آنها می باشند.
- ریز پردازنده پنتیوم دارای دو نوع کد خطا مطابق شکل زیر می باشد :

- کد خطای IDT در اکثر استثناءها مورد استفاده قرار می‌گیرد ولی کد خطای صفحه در صورت خطا در آدرس دهی صفحه استفاده می شود.



شکل ۶-۲۲-الف) کد خطای IDT ب) کد خطای صفحه

انواع وقفه در ریز پردازنده ی پنتیوم



- شکل انواع وقفه در حال حقیقی و حفاظت شده در پردازنده پنتیوم را نشان می‌دهد :

- همانطور که میبینید تا وقفه نوع ۱۸ برای وقفه های مورد استفاده سیستم به کار رفته که بیشتر آنها از نوع وقفه استثنا هستند
- از وقفه نوع ۱۹ تا ۳۱ رزرو شده می باشند و برای توسعه بعدی ریزپردازنده در نظر گرفته شده است.
- از وقتفه نوع ۳۲ تا ۲۵۵ نیز برای وقفه خارجی قابل پوشاندن در نظر گرفته شده است که توسط وقتفه نرم افزاری نیز قابل استفاده است

انواع وقفه در ریز پردازنده ی پنتیوم

- **وقفه نوع صفر:** نام این وقفه تقسیم بر صفر است و با تقسیم یک عدد بر صفر این وقفه اتفاق می‌افتد و به آن وقفه خطای تقسیم نیز گفته می‌شود .
- **وقفه نوع ۱:** وقفه اشکال زدایی برای پیدا کردن برخی از کارهای سخت افزاری و نرم افزاری در سیستم به کار می‌رود .
- **وقفه نوع ۲:** وقفه غیرقابل پوشاندن یک وقفه خارجی است که از طریق پایه NMI به پردازنده اعمال می‌شود و غیرقابل پوشاندن است.
- **وقفه نوع ۳ :** وقفه نقطه قطع از نوع نرم افزاری و دستورالعمل یک بایتی است و با اجرای آن برنامه متوقف شده و این وقفه اتفاق می‌افتد.
- **وقفه نوع ٤ :** چنانچه در حین عملیات ریاضی سرریز اتفاق بیفتد این وقتی داخلی به کمک دستورالعمل INTO ارسال می شود.
- **وقفه نوع ٥ :** اگر عملوند دستورالعمل در حال اجرا در محدوده ای که در دستورالعمل BOUND تعریف شده است قرار گیرد وقفه آزمایش محدود اتفاق می‌افتد.
- **وقفه نوع ٦ :** چنانچه آپ کد دستور در حال اجرا برای ریزپردازنده مفهوم نباشد این وقفه ی داخلی اجرا می شود

حفاظت از تراشه های جانبی

- عملکرد سیستم باید به نحوی باشد که در هر کار ورودی و خروجی ها تنها بتوانند به برنامه‌های خاص دسترسی پیدا کنند و برعکس برنامه ها نیز تنها بتوانند از ورودی خروجی های خاص استفاده نمایند.
- به این منظور از پردازنده ی پنتیوم به دو روش حفاظت از اطلاعات ورودی و خروجی مربوط به تراشه های جانبی را انجام می‌دهد.
- حفاظت اول توسط بیت های IOPL صورت می‌گیرد. به این ترتیب که شرایط هر کار در ثبات وضعیت آن ذخیره می شود و دوبیت ثبات وضعیت به IOPL اختصاص یافته است توسط دو بیت IOPL سطح امتیاز مجاز را مشخص می کنیم
- در این صورت تنها دستورالعمل ها یا برنامه‌هایی که دارای سطح امتیاز مساوی یا بزرگتر از IOPL هستند می توانند با ورودی و خروجی کار کنند
- روش دیگری که پردازنده پنتیوم به منظور حفاظت از ورودی و خروجی به کار می‌برد استفاده از روش اجازه دسترسی به I/O است
- به این ترتیب که دو بایت آخر از ۱۰۴ بایت TSS به عنوان آفست یا آدرس موقعیت دو بایت فوق جمع شده و مکانی دیگر از TSS را آدرس می‌نماید.

حالت مجازی ۸۰۸۶ (VM86)

- حالت مجازی ۸۰۸۶ این امکان را به سیستم می دهد در عین حال که مانند حالت حقیقی دستورالعملهای ۸۰۸۶ را اجرا می‌کند بتواند مانند حالت حفاظت شده برنامه و داده را حفاظت نموده و دارای چند کار باشد.
- به عنوان یک کاربرد این حالت سوئیچ کردن سیستم از محیط یونیکس (UNIX) به داس (DOS) را می‌توان نام برد.
- به این ترتیب که پردازنده پنتیوم در هنگام اجرای برنامه سیستم عامل یونیکس که در حالت حفاظت‌شده کار می کند می تواند با انتخاب حالت مجازی ۸۰۸۶ به محیط برنامه ی سیستم عامل داس که در حال تحقیق کار می کند و برعکس برود.

حالت مدیریت سیستم (SMM)

- حالت مدیریت سیستم همانطور که از نامش مشخص است به منظور مدیریت مجموعه سیستم به کار می رود.
- از جمله مهمترین عوامل مدیریت سیستم، مدیریت بار می باشد.
- با توسعه سیستم‌های ریزپردازنده ای مصرف انرژی در آن‌ها در حد قابل توجهی افزایش یافته است امکانات سخت افزاری و نرم افزاری SMM که در پردازنده پنتیوم این اجازه را به مجموعه سیستم می‌دهد که بتواند انرژی سیستم و عوامل مشابه به سادگی مدیریت نماید.
- حالت مدیریت سیستم اهمیت سه حالت اصلی ریزپردازنده را ندارد اما در هر صورت باعث افزایش توانایی سیستم می شود.

پایان