Operating Systems

Christopher Kruegel
Department of Computer Science
UC Santa Barbara
http://www.cs.ucsb.edu/~chris/

Segmentation

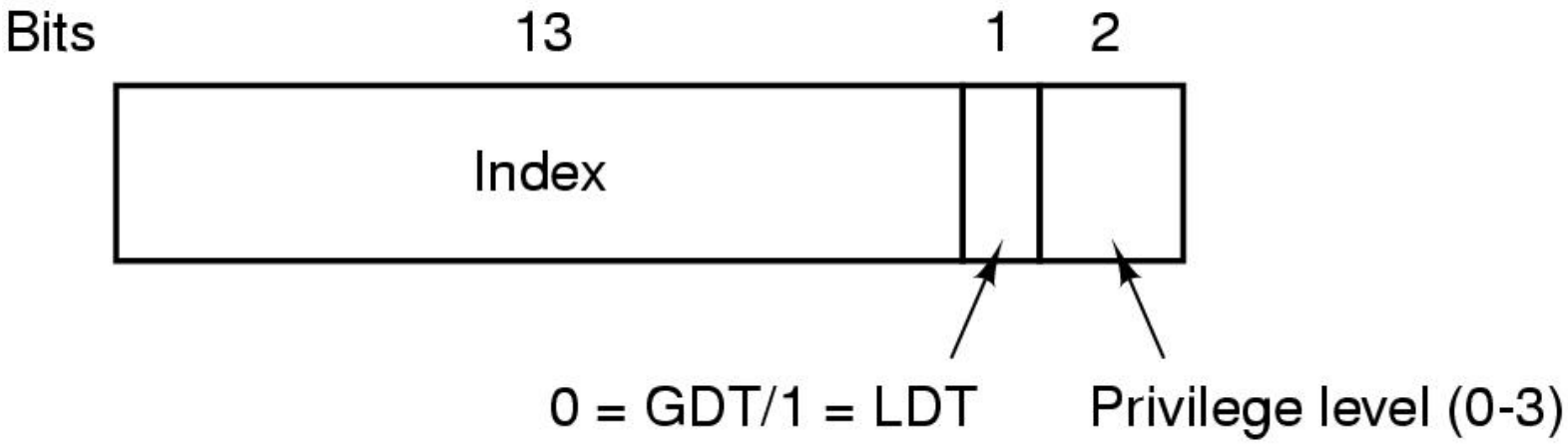
- One-dimensional address space is cumbersome to deal with if different portions of the program have to grow/shrink
- Provide the virtual machine with several independent address spaces, called *segments*
- Addressing is done by specifying
  - Segment
  - Address within the segment
- Advantages
  - Easy to share code and data segments (shared libraries)
  - Different segments can have different types of protection
- Segmentation is usually composed with paging

Segmentation with Paging: Pentium

- Virtual memory with 16K segments
- Local Descriptor Table (LDT) for each program
- Global Descriptor Table (LDT) for the whole system
- To access a segment a selector for the segment is loaded into one of the segment registers (six in total)
  - CS holds code segment
  - DS holds data segment

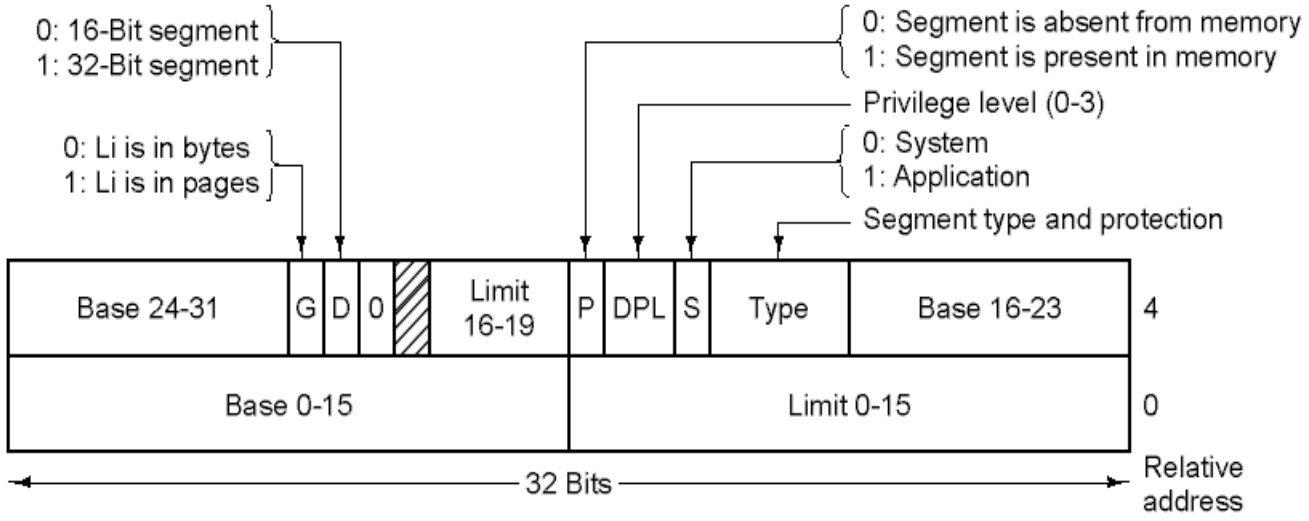
Segment Selector

- A Pentium selector contains a bit to specify if the selector is part of the GDT or the LDT (8K segments each)
- A set of bits determines the privilege level
- Segment selector determines which segment descriptor to use



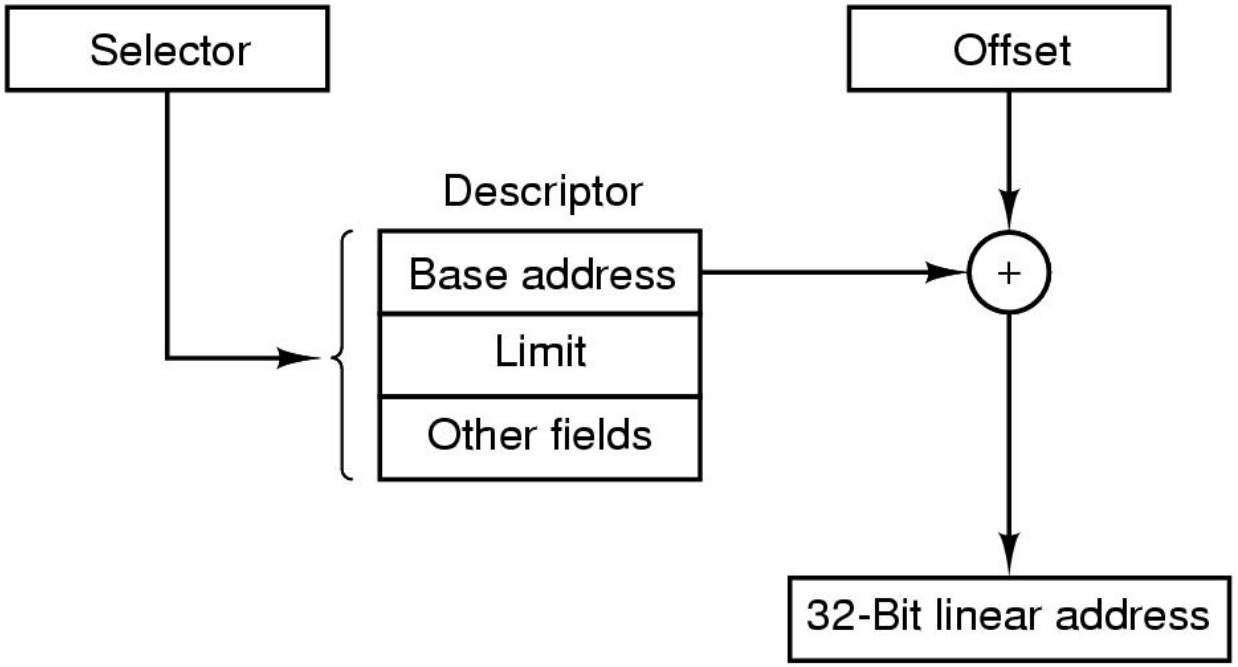
Segment Descriptor

- The segment descriptor is 64 bit long
- The “limit” is expressed with 20 bits: if Granularity bit is 0, then max limit is 1MB; if the G-bit is 1, then limit is in pages of 4K (the missing 12 bits!)



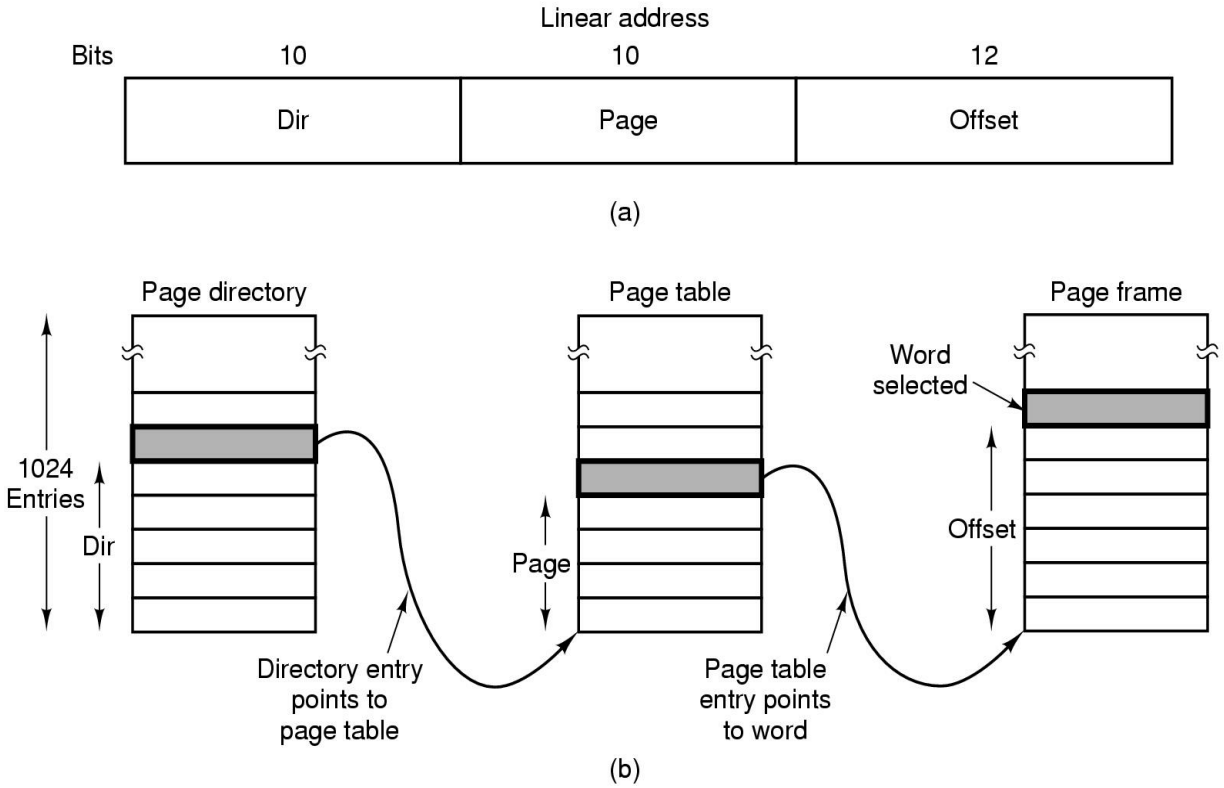
Mapping An Address

- Conversion of (selector, offset) pair to a linear address



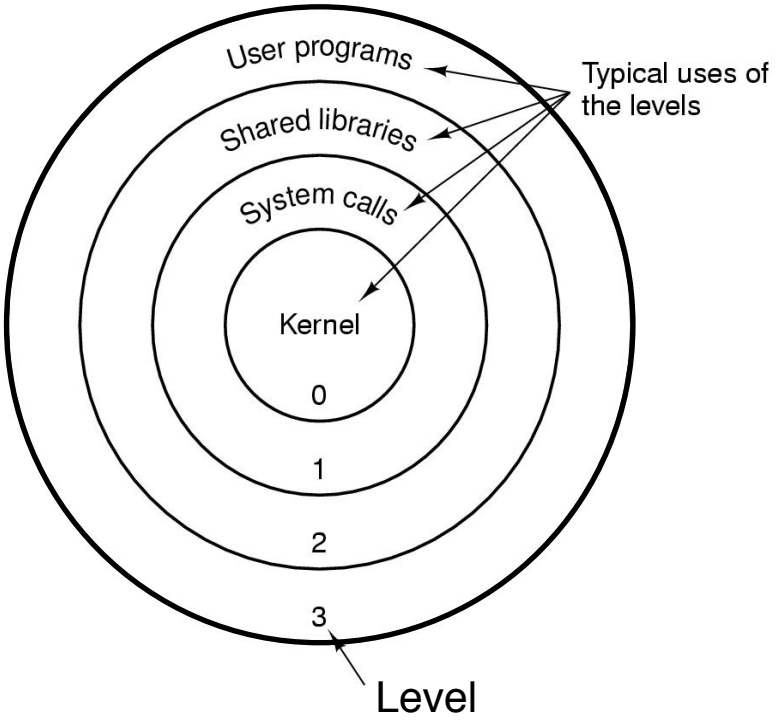
Paging the Segment

- Mapping of linear address in a segment onto a physical address



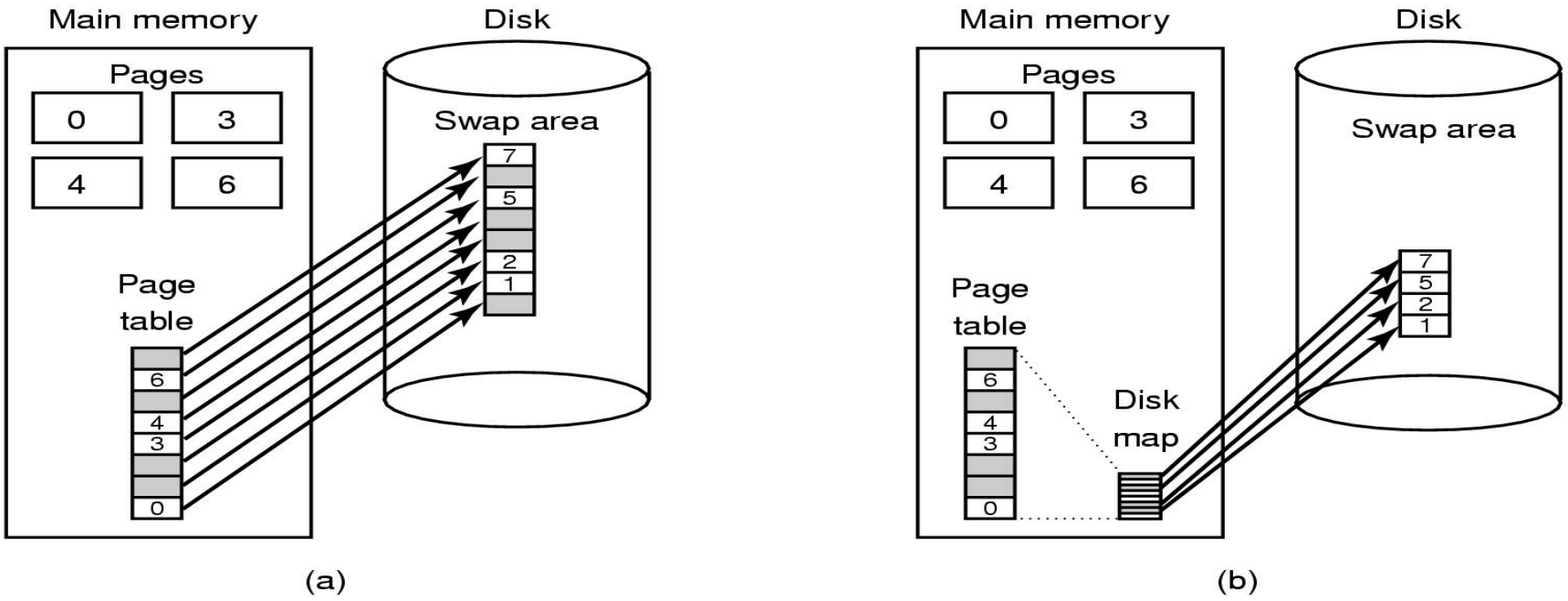
Protection on the Pentium

- Calls to procedures between protection levels must be performed by specifying a selector
- The selector is used to locate a *call gate* that gives the address of the required procedure
- This way, it is not possible to jump to arbitrary locations



Backing Store

- (a) Paging to static swap area
- (b) Backing up pages dynamically



Separate Instruction and Data Spaces

- One address space
- Separate I and D spaces