CS 333
Introduction to Operating Systems

Class 12 - Virtual Memory (2)

Jonathan Walpole
Computer Science
Portland State University
Inverted page tables

- Problem:
  - Page table overhead increases with address space size
  - Page tables get too big to fit in memory!

- Consider a computer with 64 bit addresses
  - Assume 4 Kbyte pages (12 bits for the offset)
  - Virtual address space = $2^{52}$ pages!
  - Page table needs $2^{52}$ entries!
  - This page table is much too large for memory!
Inverted page tables

How many mappings do we need (maximum) at any time?
Inverted page tables

How many mappings do we need (maximum) at any time?

We only need mappings for pages that are in memory!
  - A 256 Mbyte memory can only hold 64 4Kbyte pages
  - Only need 64 page table entries on this computer!
Inverted page tables

- An inverted page table
  - Has one entry for every frame of memory
  - Records which page is in that frame
  - Is indexed by frame number not page number!

- So how can we search an inverted page table on a TLB miss fault?
Inverted page tables

- If we have a page number (from a faulting address) and want to find its page table entry, do we
  - Do an exhaustive search of all entries?
Inverted page tables

- If we have a page number (from a faulting address) and want to find it page table entry, do we
  - Do an exhaustive search of all entries?
  - No, that’s too slow!
  - Why not maintain a hash table to allow fast access given a page number?
    - $O(1)$ lookup time with a good hash function
Inverted page table

Traditional page table with an entry for each of the $2^{52}$ pages

Indexed by virtual page

$2^{52} - 1$

256-MB physical memory has $2^{16}$ 4-KB page frames

Indexed by hash on virtual page

Hash table

Virtual page

Page frame
Which page table design is best?

- The best choice depends on CPU architecture.
- 64 bit systems need inverted page tables.
- Some systems use a combination of regular page tables together with segmentation (later).
Memory protection

- Protection though addressability
  - If address translation only allows a process to access its own pages, it is implementing memory protection

- But what if you want a process to be able to read and execute some pages but not write them?
  - text segment

- Or read and write them but not execute them?
  - stack

- Need some way of implementing protection based on access type
Memory protection

- **How is protection checking implemented?**
  - compare page protection bits with process capabilities and operation types on every load/store
  - sounds expensive!
  - Requires hardware support!

- **How can protection checking be done efficiently?**
  - Use the TLB as a “protection” look-aside buffer as well as a translation lookaside buffer
  - Use special segment registers
Protection lookaside buffer

- A TLB is often used for more than just “translation”
- Memory accesses need to be checked for validity
  - Does the address refer to an allocated segment of the address space?
    - If not: segmentation fault!
  - Is this process allowed to access this memory segment?
    - If not: segmentation/protection fault!
  - Is the type of access valid for this segment?
    - Read, write, execute ...?
    - If not: protection fault!
### Page-grain protection checking with a TLB

<table>
<thead>
<tr>
<th>Valid</th>
<th>Virtual page</th>
<th>Modified</th>
<th>Protection</th>
<th>Page frame</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>140</td>
<td>1</td>
<td>RW</td>
<td>31</td>
</tr>
<tr>
<td>1</td>
<td>20</td>
<td>0</td>
<td>R X</td>
<td>38</td>
</tr>
<tr>
<td>1</td>
<td>130</td>
<td>1</td>
<td>RW</td>
<td>29</td>
</tr>
<tr>
<td>1</td>
<td>129</td>
<td>1</td>
<td>RW</td>
<td>62</td>
</tr>
<tr>
<td>1</td>
<td>19</td>
<td>0</td>
<td>R X</td>
<td>50</td>
</tr>
<tr>
<td>1</td>
<td>21</td>
<td>0</td>
<td>R X</td>
<td>45</td>
</tr>
<tr>
<td>1</td>
<td>860</td>
<td>1</td>
<td>RW</td>
<td>14</td>
</tr>
<tr>
<td>1</td>
<td>861</td>
<td>1</td>
<td>RW</td>
<td>75</td>
</tr>
</tbody>
</table>
Page grain protection in a page table

A typical page table entry with support for page grain protection
Memory protection granularity

- At what granularity should protection be implemented?
  - page-level?
    - A lot of overhead for storing protection information for non-resident pages
  - segment level?
    - Coarser grain than pages
    - Makes sense if contiguous groups of pages share the same protection status
Segment-grain protection

- All pages within a segment usually share the same protection status
  - So we should be able to batch the protection information
- Then why not just use segment-size pages?
Segment-grain protection

- All pages within a segment usually share the same protection status
  - So we should be able to batch the protection information

- Then why not just use segment-size pages?
  - Segments vary in size from process to process
  - Segments change size dynamically (stack, heap etc)

- Need to manage addressability and access-based protection separately from memory allocation
Segmented address spaces

- **Traditional Virtual Address Space**
  - “flat” address space (1 dimensional)

- **Segmented Address Space**
  - Program made of several pieces or “segments”
  - Each segment is its own mini-address space
  - Addresses within a segment start at zero
  - The program must always say which segment it means
    - either embed a segment id in an address
    - or load a value into a segment register and refer to the register
  - Addresses:
    - Segment + Offset
  - Each segment can grow independently of others
Segmentation in a single address space

Example: A compiler

Virtual address space

- Call stack
- Parse tree
- Constant table
- Source text
- Symbol table

Address space allocated to the parse tree

Free

Space currently being used by the parse tree

Symbol table has bumped into the source text table
Segmented memory

- Each space grows, shrinks independently!
Separate instruction and data spaces

* One address space
* Separate I and D spaces
## Comparison of paging vs. segmentation

<table>
<thead>
<tr>
<th>Consideration</th>
<th>Paging</th>
<th>Segmentation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Need the programmer be aware that this technique is being used?</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>How many linear address spaces are there?</td>
<td>1</td>
<td>Many</td>
</tr>
<tr>
<td>Can the total address space exceed the size of physical memory?</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Can procedures and data be distinguished and separately protected?</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Can tables whose size fluctuates be accommodated easily?</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Is sharing of procedures between users facilitated?</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Why was this technique invented?</td>
<td>To get a large linear address space without having to buy more physical memory</td>
<td>To allow programs and data to be broken up into logically independent address spaces and to aid sharing and protection</td>
</tr>
</tbody>
</table>
Segmentation vs. Paging

- Do we need to choose one or the other?
- Why not use both together
  - Paged segments
Segmentation with paging (MULTICS)

- Each segment is divided up into pages.
- Each segment descriptor points to a page table.
Segmentation with paging (MULTICS)

- Each entry in segment table...

<table>
<thead>
<tr>
<th>18</th>
<th>9</th>
<th>111</th>
<th>3</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Main memory address of the page table</td>
<td>Segment length (in pages)</td>
<td>Page size: 0 = 1024 words 1 = 64 words</td>
<td>0 = segment is paged 1 = segment is not paged</td>
<td>Miscellaneous bits</td>
</tr>
</tbody>
</table>
Segmentation with paging: MULTICS

MULTICS virtual address

Segment number

Page number

Offset

Conversion of a 2-part MULTICS address into a main memory address
## Segmentation with Paging: TLB operation

- Simplified version of the MULTICS TLB
- Existence of 2 page sizes makes actual TLB more complicated

<table>
<thead>
<tr>
<th>Comparison field</th>
<th>Segment number</th>
<th>Virtual page</th>
<th>Page frame</th>
<th>Protection</th>
<th>Age</th>
<th>Is this entry used?</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>4</td>
<td>1</td>
<td>7</td>
<td>Read/write</td>
<td>13</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>6</td>
<td>0</td>
<td>2</td>
<td>Read only</td>
<td>10</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>12</td>
<td>3</td>
<td>1</td>
<td>Read/write</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0</td>
<td></td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>1</td>
<td>0</td>
<td>Execute only</td>
<td>7</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>2</td>
<td>12</td>
<td>Execute only</td>
<td>9</td>
<td>1</td>
</tr>
</tbody>
</table>
Conversion of a (selector, offset) pair to a linear address
Segmentation & paging in the Pentium

- Pentium segment descriptor

![Diagram of Pentium segment descriptor]

- 0: 16-Bit segment
- 1: 32-Bit segment
- 0: Li is in bytes
- 1: Li is in pages

- 0: Segment is absent from memory
- 1: Segment is present in memory

- Privilege level (0-3)
- 0: System
- 1: Application

- Segment type and protection

- Base 24-31
- GD 0
- Limit 16-19
- P DPL S Type
- Base 16-23

- Base 0-15
- Limit 0-15

- 32 Bits

- Relative address