Report : Project 4 - XINU Memory Virtualisation

Aspects of Implementation:

Initialisation:(in xinu/system/meminit.c - `initialize_page_table`())

- Page Directory allocated to system processes(pd.allocated and pd.valid bits are set) and rest all pages have their PDE initialized to 0.
- All 17k pages(8096+4096+1024+4096) are mapped to the system processes which fit in 17 entries of the PAGE TABLE.
- CR3 is set to the PDBR of system processes and paging is enabled in CR0[31], initial_pdbr and sys_proc have been added to the proctab as well to help with preserving pd during context switches during a “kernel-mode” operation.

Page Fault Handler:(in xinu/system/page_fault_handler.c)

- pagefault_handler_disp.S: Page fault handler dispatcher called when interrupt 14(Interrupt vector for Page Faults) is triggered. Also modifies the ESP so that the error message popped onto the stack is skipped after the subroutine is finished executing and error message is available as a function parameter for the page_fault_handler function.
- pagefault_handler.c :
    - Before the page fault is handled, the PDBR is always changed to system processes’ PDBR making the whole address space available to the handler.
    - bit0 of error code==0 - Page not present
    - bit0 of error code==1 - Page-level protection violation
    - Allocated a new page by iterating through the page list and finding pages not allocated. If no unallocated page, find victim and move to swap space.
    - Segmentation Fault in case of access to an invalid page table or directory.

Usage of the PDE bits allocated for programmer use:

- *page allocated bit*
- *valid bit*
- *is in swap space bit*

Swapping is done by checking the swap bit for a valid record. If the swap bit is 1 then the value is copied in from the swap space to the new physical memory location. If the swap bit is 0 then junk value is left in the memory location and present bit is set to 1.
When a memory location is moved to the swap space because the ffs space is full then the location of the swap space is saved in the pd_base while setting the swap bit to 1.

vcreate:

- Creates processes similar to create.c, allocates PDBR and stores in the proctab. Also, it maps the XINU PAGES in the page directory for that process.

generic_getmem:

- Separate free list head maintained for FFS and Swap Space. generic_getmem is called with the head of the space to get the block from as the argument along with the size required. It picks a block and modifies the linked list accordingly.

generic_freemem:

- Similar to the freemem function except that the memlist is passed as a parameter to the function allowing the memlist to be be generic.

vmalloc:

- Checks for contiguous blocks of requested size from the ffsmemlist and returns the block if available. find_contiguous_vheap is used to find free virtual memory using the page tables for the process. The virtual address is then marked as valid.

vfree:

- Calls the generic freemem function for all the frames which need to be freed and marks the valid bit to 0.