Protected-Mode Address Translation

Logical Address

Segment Translation

Linear Address

Page Translation

Physical Address

CPU

Selector Offset

Logical Address GDT/LDT

Selector Offset

Linear Address Dir Table Offset

Physical Address PPN Offset

PPN Flags Page Table

CR3 Page Directory

Physical Page Number AVL DADTWUWP

Page table and page directory entries are identical except for the D bit.

P - Present
W - Writable
U - User
WT - 1=Write-through, 0=Write-back
CD - Cache Disabled
A - Accessed
D - Dirty (0 in page directory)
AVL - Available for system use
To select the various table entries, the linear address is divided into three sections:

- **Page-directory entry**—Bits 22 through 31 provide an offset to an entry in the page directory. The selected entry provides the base physical address of a page table.

- **Page-table entry**—Bits 12 through 21 of the linear address provide an offset to an entry in the selected page table. This entry provides the base physical address of a page in physical memory.

- **Page offset**—Bits 0 through 11 provides an offset to a physical address in the page.

Memory management software has the option of using one page directory for all programs and tasks, one page directory for each task, or some combination of the two.

**Figure 3-13** shows how a page directory can be used to map linear addresses to 4-MByte pages. The entries in the page directory point to 4-MByte pages in physical memory. This paging method can be used to map up to 1024 pages into a 4-GByte linear address space.
To return from an exception- or interrupt-handler procedure, the handler must use the IRET (or IRETD) instruction. The IRET instruction is similar to the RET instruction except that it restores the saved flags into the EFLAGS register. The IOPL field of the EFLAGS register is restored only if the CPL is 0. The IF flag is changed only if the CPL is less than or equal to the IOPL. See Chapter 3, "Instruction Set Reference, A-M," of the Intel® 64 and IA-32 Architectures Software Developer’s Manual, Volume 2A, for a description of the complete operation performed by the IRET instruction.

If a stack switch occurred when calling the handler procedure, the IRET instruction switches back to the interrupted procedure’s stack on the return.

The privilege-level protection for exception- and interrupt-handler procedures is similar to that used for ordinary procedure calls when called through a call gate (see Section 4.8.4, "Accessing a Code Segment Through a Call Gate"). The processor does not use the CS, EIP, and ESP registers when calling a handler procedure.

On an IRET instruction:

- The processor restores the saved flags into the EFLAGS register.
- The stack pointer is restored. If the stack switch occurred when calling the handler procedure, the IRET instruction switches back to the interrupted procedure’s stack on the return.
- The processor does not use the CS, EIP, and ESP registers when calling a handler procedure.