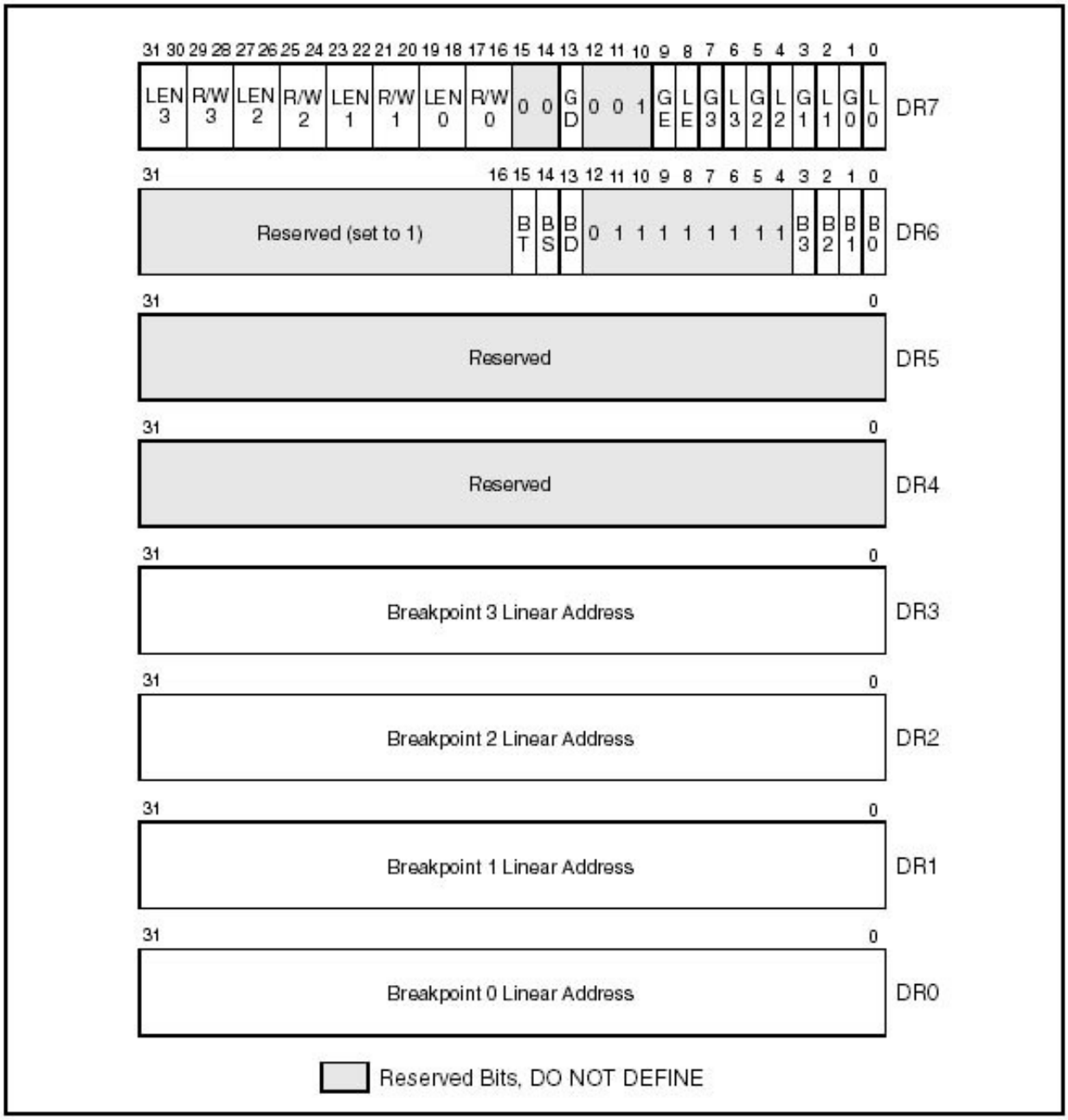

Figure 15-1. Debug Registers

Debug Registers are used for breakpoints, in the case of softice its the BPM command and they're usual refered to as hardware breakpoints since they use the CPUs internal DRx regisers.

There are eight debug registers and these are context specfic, you can set a maximum of 4 breakpoints the location of the address is stored in DR0->3

DR4 and DR5 are reserved, probably for really leet stuff which intel neglect to tell us about.

DR6 contains status information about set breakpoints, the first nibble has a bit for each breakpoint, its set when a breakpoint meets its condition and even when the breakpoint is not active.

The last three documented bits are BT BS BD,

* BT - Debug exception occured because of a task switch. (flag in TSS needed)
* BS - Debug exception occured because of a single step (INT 1)
* BD - Debug exception occured because next instr. is access DRX related, (flag in dr7 needed)

D7 contains breakpoint properties, the first byte is about the locality of the breakpoint, theres L and G flags for each breakpoint if L is set then the breakpoint is only for that task, but if G is set then the breakpoint is global.

Bits 9 and 8 are GE and LE, these are the local and global exact breakpoints, this means when a debug exception occurs the debugger knows the exact instruction that caused this, SoftICE sets these bits on all of its BPM which makes DR7 in the 7xx range, usually its 4xx, this is worth noting since this is a method of debugger detection.

Bit 13 is the GD bit, GD stands for General Detection and is very handy to reversers unfortunatley i havent seen it used much but it holds great power, when the GD bit is set it detects DRx access, when a drx interaction occurs an int 1 occurs and the BD bit is set in DR6, once the int 1 has occured the GD bit is removed. (See My GD in pratice article)

```
mov eax,DR7
or eax,2000h ; 10000000000000b
mov DR7,eax
```

Bits 16->29 is the condition for each breakpoint, each is R/W 2bits long

```
0 = Break on execution
1 = Break on data write
3 = Break on data read/write (1st bit 1, 2nd bit 1 for RW)
```

by clearing the DE flag in CR4 (Control Registers) 2 can be used for I/O detection

after a R/W for a register comes the length, it can be either 1,2 or 4 bytes, if the breakpoint is on execution the length must be 0.

yates.
07/DEC/02