WIKIPEDIA

Trap flag

A **trap flag** permits operation of a processor in single-step mode. If such a flag is available, debuggers can use it to step through the execution of a computer program.

Single-step interrupt

When a system is instructed to single-step, it will execute one instruction and then stop. The contents of registers and memory locations can be examined; if they are correct, the system can be told to go on and execute the next instruction. The Intel 8086 trap flag and type-1 interrupt response make it quite easy to implement a single-step feature in an 8086-based system. If the trap flag is set, the 8086 will automatically do a type-1 interrupt after each instruction executes. When the 8086 does a type-1 interrupt, it pushes the flag register on the stack.

Setting

The 8086 has no instruction to directly set or reset the trap flag. These operations are done by pushing the flag register on the stack, changing the trap flag bit to what the programmer wants it to be, and then popping the flag register back off the stack. The instructions to set the trap flag are:

```
PUSHF                   ; Push flags on stack
MOV BP,SP               ; Copy SP to BP for use as index
OR WORD PTR[BP+0],0100H ; Set TF flag
POPF                    ; Restore flag Register
```

Actually you do not use the Trap flag in this way, because you are normally monitoring a program from an ISR. You continue execution of the program by an IRET.

```
Int3ServiceRoutine:       ; Stack: Ret, Flags
  PUSHA                   ; Stack: Ret, Flags, AX, CX, DX, BX, SP, BP, SI, DI
  PUSH DS
  PUSH ES                 ; Stack: Ret, Flags, AX, CX, DX, BX, SP, BP, SI, DI, DS, ES

   ... the ISR code using only integer (otherwise you must also store floating point registers)

  MOV BP,SP               ; Stack: Ret, Flags, AX, CX, DX, BX, SP, BP, SI, DI, DS, ES
  MOV BP,[BP+10]          ; Stored SP
  OR WORD PTR[BP+0],0100H ; Set TF flag in the stored Flag register
  POP ES
  POP DS
  POPA
  IRET                    ; continue execution for ONE instruction, then calling ISR again.
```

Resetting

To reset the trap flag, simply replace the OR instruction in the preceding sequence with the instruction:

```
AND WORD PTR[BP+0],0FEFFH
```

The trap flag is reset when the 8086 does a type-1 interrupt, so the single-step mode will be disabled during the interrupt-service procedure.

Status register

15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0	(bit position)
-	-	-	-	O	D	I	T	S	Z	-	A	-	P	-	C	Flags
