`cli.s` 1965 `idt_desc_int.c` 1960 `idt_load.c` 1960 `idt_print.c` 1960 `int.h` 1955 `irq_remap.c` 1960 `isr.s` 1955 `isr_exception_name.c` 1963 `isr_exception_unrecoverable.c` 1963 `isr_irq.c` 1963 `isr_syscall.c` 1963 `sti.s` 1965

In questa fase dello sviluppo del sistema è opportuno predisporre la tabella IDT (*interrupt description table*), con le eccezioni del microprocessore e le interruzioni hardware (IRQ), anche se inizialmente nulla viene gestito effettivamente.

File di intestazione «int.h» e file delle routine di interruzione «isr.s»

Il file di intestazione '`int.h`' contiene la dichiarazione delle funzioni per la gestione delle interruzioni. Viene proposto subito nella sua versione completa, anche se non tutte le funzioni dichiarate vengono presentate immediatamente.

Listato u171.1. '`./05/include/kernel/int.h`'

```
#ifndef _INT_H
#define _INT_H  1

#include <inttypes.h>
#include <stdbool.h>
#include <stdarg.h>
#include <kernel/os.h>

void idt_desc_int    (int      desc,
                      uint32_t offset,
                      uint16_t selector,
                      bool     present,
                      char     type,
                      char     dpl);

void  idt_load       (void *idtr);
void  idt            (void);
void  irq_remap      (unsigned int offset_1, unsigned int offset_2);
char *exception_name (int exception);
void  idt_print      (void *idtr);

void isr_0  (void);
void isr_1  (void);
void isr_2  (void);
void isr_3  (void);
void isr_4  (void);
void isr_5  (void);
void isr_6  (void);
void isr_7  (void);
void isr_8  (void);
void isr_9  (void);
void isr_10 (void);
void isr_11 (void);
void isr_12 (void);
void isr_13 (void);
void isr_14 (void);
void isr_15 (void);
void isr_16 (void);
void isr_17 (void);
void isr_18 (void);
void isr_19 (void);
void isr_20 (void);
void isr_21 (void);
void isr_22 (void);
void isr_23 (void);
void isr_24 (void);
void isr_25 (void);
void isr_26 (void);
void isr_27 (void);
void isr_28 (void);
void isr_29 (void);
void isr_30 (void);
void isr_31 (void);
void isr_32 (void);
void isr_33 (void);
void isr_34 (void);
void isr_35 (void);
void isr_36 (void);
void isr_37 (void);
void isr_38 (void);
```

```
void isr_39 (void);
void isr_40 (void);
void isr_41 (void);
void isr_42 (void);
void isr_43 (void);
void isr_44 (void);
void isr_45 (void);
void isr_46 (void);
void isr_47 (void);
void isr_128 (void);

void sti (void);
void cli (void);

void isr_exception_unrecoverable (uint32_t eax, uint32_t ecx, uint32_t edx,
                                  uint32_t ebx, uint32_t ebp, uint32_t esi,
                                  uint32_t edi, uint32_t ds,  uint32_t es,
                                  uint32_t fs,  uint32_t gs,
                                  uint32_t interrupt, uint32_t error,
                                  uint32_t eip, uint32_t cs, uint32_t eflags);

void isr_irq (uint32_t eax, uint32_t ecx, uint32_t edx, uint32_t ebx,
              uint32_t ebp, uint32_t esi, uint32_t edi, uint32_t ds,
              uint32_t es,  uint32_t fs,  uint32_t gs,  uint32_t interrupt);

uint32_t isr_syscall (uint32_t start, ...);
uint32_t int_128     (void);

#endif
```

Si può osservare l'elenco delle funzioni '**`isr_n()`**', per la gestione delle varie interruzioni catalogate nella tabella IDT. In particolare, l'interruzione 128_{10}, ovvero 80_{16}, viene usata per le chiamate di sistema. Queste funzioni sono dichiarate formalmente nel file '`isr.s`' che viene mostrato integralmente nel listato successivo.

Listato u171.2. '`./05/lib/int/isr.s`'

```
.extern isr_exception_unrecoverable
.extern isr_irq
.extern isr_syscall
#
.globl isr_0
.globl isr_1
.globl isr_2
.globl isr_3
.globl isr_4
.globl isr_5
.globl isr_6
.globl isr_7
.globl isr_8
.globl isr_9
.globl isr_10
.globl isr_11
.globl isr_12
.globl isr_13
.globl isr_14
.globl isr_15
.globl isr_16
.globl isr_17
.globl isr_18
.globl isr_19
.globl isr_20
.globl isr_21
.globl isr_22
.globl isr_23
.globl isr_24
.globl isr_25
.globl isr_26
.globl isr_27
.globl isr_28
.globl isr_29
.globl isr_30
.globl isr_31
.globl isr_32
.globl isr_33
.globl isr_34
.globl isr_35
.globl isr_36
.globl isr_37
.globl isr_38
.globl isr_39
.globl isr_40
.globl isr_41
.globl isr_42
.globl isr_43
.globl isr_44
.globl isr_45
.globl isr_46
.globl isr_47
.globl isr_128

    ###############################################################################
    # Nella pila è già stato inserito dal microprocessore:                        #
    #   [omissis]                                                                 #
    #   push %eflags                                                              #
    #   push %cs                                                                  #
    #   push %eip                                                                 #
    ###############################################################################

isr_0:          # «division by zero exception»
    cli
    push $0     # Codice di errore fittizio.
    push $0     # Numero dell'eccezione.
    jmp exception_unrecoverable
#
isr_1:          # «debug exception»
    cli
    push $0     # Codice di errore fittizio.
    push $1     # Numero dell'eccezione.
    jmp exception_unrecoverable
#
isr_2:          # «non maskable interrupt exception»
    cli
    push $0     # Codice di errore fittizio.
    push $2     # Numero dell'eccezione.
    jmp exception_unrecoverable
#
isr_3:          # «breakpoint exception»
    cli
    push $0     # Codice di errore fittizio.
    push $3     # Numero dell'eccezione.
    jmp exception_unrecoverable
#
isr_4:          # «into detected overflow exception»
    cli
    push $0     # Codice di errore fittizio.
    push $4     # Numero dell'eccezione.
    jmp exception_unrecoverable
#
isr_5:          # «out of bounds exception»
    cli
    push $0     # Codice di errore fittizio.
    push $5     # Numero dell'eccezione.
    jmp exception_unrecoverable
#
isr_6:          # «invalid opcode exception»
    cli
    push $0     # Codice di errore fittizio.
    push $6     # Numero dell'eccezione.
    jmp exception_unrecoverable
#
isr_7:          # «no coprocessor exception»
    cli
    push $0     # Codice di errore fittizio.
    push $7     # Numero dell'eccezione.
    jmp exception_unrecoverable
#
isr_8:          # «double fault exception»
    cli
    #
    push $8     # Numero dell'eccezione.
    jmp exception_unrecoverable
#
isr_9:          # «coprocessor segment overrun exception»
    cli
    push $0     # Codice di errore fittizio.
    push $9     # Numero dell'eccezione.
    jmp exception_unrecoverable
#
isr_10:         # «bad TSS exception»
    cli
    #
    push $10    # Numero dell'eccezione.
    jmp exception_unrecoverable
#
isr_11:         # «segment not present exception»
    cli
    #
    push $11    # Numero dell'eccezione.
    jmp exception_unrecoverable
#
isr_12:         # «stack fault exception»
    cli
    #
    push $12    # Numero dell'eccezione.
    jmp exception_unrecoverable
#
isr_13:         # «general protection fault exception»
    cli
    #
    push $13    # Numero dell'eccezione.
    jmp exception_unrecoverable
#
isr_14:         # «page fault exception»
    cli
    #
    push $14    # Numero dell'eccezione.
    jmp exception_unrecoverable
#
isr_15:         # «unknown interrupt exception»
    cli
    push $0     # Codice di errore fittizio.
    push $15    # Numero dell'eccezione.
    jmp exception_unrecoverable
#
isr_16:         # «coprocessor fault exception»
    cli
    push $0     # Codice di errore fittizio.
    push $16    # Numero dell'eccezione.
    jmp exception_unrecoverable
#
isr_17:         # «alignment check exception»
    cli
```

```
    push $0     # Codice di errore fittizio.
    push $17    # Numero dell'eccezione.
    jmp exception_unrecoverable
#
isr_18:         # «machine check exception»
    cli
    push $0     # Codice di errore fittizio.
    push $18    # Numero dell'eccezione.
    jmp exception_unrecoverable
#
isr_19:         # «reserved exception»
    cli
    push $0     # Codice di errore fittizio.
    push $19    # Numero dell'eccezione.
    jmp exception_unrecoverable
#
isr_20:         # «reserved exception»
    cli
    push $0     # Codice di errore fittizio.
    push $20    # Numero dell'eccezione.
    jmp exception_unrecoverable
#
isr_21:         # «reserved exception»
    cli
    push $0     # Codice di errore fittizio.
    push $21    # Numero dell'eccezione.
    jmp exception_unrecoverable
#
isr_22:         # «reserved exception»
    cli
    push $0     # Codice di errore fittizio.
    push $22    # Numero dell'eccezione.
    jmp exception_unrecoverable
#
isr_23:         # «reserved exception»
    cli
    push $0     # Codice di errore fittizio.
    push $23    # Numero dell'eccezione.
    jmp exception_unrecoverable
#
isr_24:         # «reserved exception»
    cli
    push $0     # Codice di errore fittizio.
    push $24    # Numero dell'eccezione.
    jmp exception_unrecoverable
#
isr_25:         # «reserved exception»
    cli
    push $0     # Codice di errore fittizio.
    push $25    # Numero dell'eccezione.
    jmp exception_unrecoverable
#
isr_26:         # «reserved exception»
    cli
    push $0     # Codice di errore fittizio.
    push $26    # Numero dell'eccezione.
    jmp exception_unrecoverable
#
isr_27:         # «reserved exception»
    cli
    push $0     # Codice di errore fittizio.
    push $27    # Numero dell'eccezione.
    jmp exception_unrecoverable
#
isr_28:         # «reserved exception»
    cli
    push $0     # Codice di errore fittizio.
    push $28    # Numero dell'eccezione.
    jmp exception_unrecoverable
#
isr_29:         # «reserved exception»
    cli
    push $0     # Codice di errore fittizio.
    push $29    # Numero dell'eccezione.
    jmp exception_unrecoverable
#
isr_30:         # «reserved exception»
    cli
    push $0     # Codice di errore fittizio.
    push $30    # Numero dell'eccezione.
    jmp exception_unrecoverable
#
isr_31:         # «reserved exception»
    cli
    push $0     # Codice di errore fittizio.
    push $31    # Numero dell'eccezione.
    jmp exception_unrecoverable
#
isr_32:         # IRQ 0: «timer»
    cli
    push $0     # Codice di errore fittizio.
    push $32    # Numero IRQ + 32.
    jmp irq
#
isr_33:         # IRQ 1: tastiera
    cli
    push $0     # Codice di errore fittizio.
    push $33    # Numero IRQ + 32.
    jmp irq
#
isr_34:         # IRQ 2: viene attivato per gli IRQ da 8 a 15.
    cli
    push $0     # Codice di errore fittizio.
```



```
    push $34    # Numero IRQ + 32.
    jmp irq
#
isr_35:         # IRQ 3
    cli
    push $0     # Codice di errore fittizio.
    push $35    # Numero IRQ + 32.
    jmp irq
#
isr_36:         # IRQ 4
    cli
    push $0     # Codice di errore fittizio.
    push $36    # Numero IRQ + 32.
    jmp irq
#
isr_37:         # IRQ 5
    cli
    push $0     # Codice di errore fittizio.
    push $37    # Numero IRQ + 32.
    jmp irq
#
isr_38:         # IRQ 6: unità a dischetti
    cli
    push $0     # Codice di errore fittizio.
    push $38    # Numero IRQ + 32.
    jmp irq
#
isr_39:         # IRQ 7: LPT 1
    cli
    push $0     # Codice di errore fittizio.
    push $39    # Numero IRQ + 32.
    jmp irq
#
isr_40:         # IRQ 8: «real time clock (RTC)»
    cli
    push $0     # Codice di errore fittizio.
    push $40    # Numero IRQ + 32.
    jmp irq
#
isr_41:         # IRQ 9
    cli
    push $0     # Codice di errore fittizio.
    push $41    # Numero IRQ + 32.
    jmp irq
#
isr_42:         # IRQ 10
    cli
    push $0     # Codice di errore fittizio.
    push $42    # Numero IRQ + 32.
    jmp irq
#
isr_43:         # IRQ 11
    cli
    push $0     # Codice di errore fittizio.
    push $43    # Numero IRQ + 32.
    jmp irq
#
isr_44:         # IRQ 12: mouse PS/2
    cli
    push $0     # Codice di errore fittizio.
    push $44    # Numero IRQ + 32.
    jmp irq
#
isr_45:         # IRQ 13: coprocessore matematico
    cli
    push $0     # Codice di errore fittizio.
    push $45    # Numero IRQ + 32.
    jmp irq
#
isr_46:         # IRQ 14: canale IDE primario
    cli
    push $0     # Codice di errore fittizio.
    push $46    # Numero IRQ + 32.
    jmp irq
#
isr_47:         # IRQ 15: canale IDE secondario
    cli
    push $0     # Codice di errore fittizio.
    push $47    # Numero IRQ + 32.
    jmp irq
#
isr_128:        # Chiamate di sistema.
    cli
    call isr_syscall
    iret
#
# Eccezioni che per il momento non sono gestibili.
#
exception_unrecoverable:

    ###########################################################################
    # A questo punto, nella pila sono stati aggiunti:                         #
    #   push $<n_errore>                                                      #
    #   push $<n_voce_idt>                                                    #
    ###########################################################################

    pushl %gs
    pushl %fs
    pushl %es
    pushl %ds
    pushl %edi
    pushl %esi
    pushl %ebp
```

```
    pushl %ebx
    pushl %edx
    pushl %ecx
    pushl %eax
    #
    call isr_exception_unrecoverable
    #
    popl %eax
    popl %ecx
    popl %edx
    popl %ebx
    popl %ebp
    popl %esi
    popl %edi
    popl %ds
    popl %es
    popl %fs
    popl %gs
    add $4, %esp        # espelle il numero dell'eccezione
    add $4, %esp        # espelle il codice di errore
    #
    iret
#
# IRQ hardware.
#
irq:

    ###############################################################
    # A questo punto, nella pila sono stati aggiunti:             #
    #   push $0                                                   #
    #   push $<n_voce_idt>                                        #
    ###############################################################

    pushl %gs
    pushl %fs
    pushl %es
    pushl %ds
    pushl %edi
    pushl %esi
    pushl %ebp
    pushl %ebx
    pushl %edx
    pushl %ecx
    pushl %eax
    #
    call isr_irq
    #
    popl %eax
    popl %ecx
    popl %edx
    popl %ebx
    popl %ebp
    popl %esi
    popl %edi
    popl %ds
    popl %es
    popl %fs
    popl %gs
    add $4, %esp        # espelle il numero dell'interruzione
    add $4, %esp        # espelle il codice di errore fittizio.
    #
    iret
#
```

Funzioni per definire la tabella IDT

Per facilitare la compilazione della tabella IDT viene usata la funzione ***idt_desc_int()***, con la quale si deve specificare il numero del descrittore della tabella e i dati da inserirvi. La tabella IDT è definita nella variabile strutturata ***os.idt***, dichiarata nel file 'os.h'.

Listato u171.3. './05/lib/int/idt_desc_int.c'

```
#include <kernel/int.h>
void
idt_desc_int (int      desc,
              uint32_t offset,
              uint16_t selector,
              bool     present,
              char     type,
              char     dpl)
{
    //
    // Azzera i bit riservati e quello di sistema.
    //
    os.idt[desc].filler = 0;
    os.idt[desc].system = 0;
    //
    // Indirizzo relativo.
    //
    os.idt[desc].offset_a = (offset & 0x0000FFFF);
    os.idt[desc].offset_b = (offset / 0x10000);
    //
    // Selettore.
    //
    os.idt[desc].selector = selector;
    //
    // Voce valida o meno.
    //
    os.idt[desc].present = present;
    //
    // Tipo (gate type).
    //
    os.idt[desc].type = (type & 0x0F);
    //
    // DPL.
    //
    os.idt[desc].dpl = (dpl & 0x03);
}
```

Per verificare il contenuto della tabella IDT viene predisposta la funzione ***idt_print()*** che richiede come parametro il puntatore all'area di memoria che descrive il registro ***IDTR***. Così come viene proposta, la funzione mostra il contenuto completo della tabella IDT, ma questo supera generalmente le righe visualizzabili sullo schermo; pertanto, in caso di necessità, la funzione va modificata in modo da mostrare solo la porzione di proprio interesse.

Listato u171.4. './05/lib/int/idt_print.c'

```
#include <kernel/int.h>
#include <stdio.h>
//
// Mostra il contenuto di una tabella IDT, a partire dal puntatore al
// registro IDTR in memoria. Pertanto non si avvale, volutamente, della
// struttura già predisposta con il linguaggio C, mentre «local_idtr_t»
// viene creata qui solo provvisoriamente, per uso interno. Ciò serve ad
// assicurare che questa funzione compia il proprio lavoro in modo
// indipendente, garantendo la visualizzazione di dati reali.
//
typedef struct {
    uint16_t  limit;
    uint32_t  base;
} __attribute__ ((packed)) local_idtr_t;
//
void
idt_print (void *idtr)
{
    local_idtr_t *g = idtr;
        uint32_t *p = (uint32_t *) g->base;

    int max = (g->limit + 1) / (sizeof (uint32_t));
    int i;

    for (i = 0; i < max; i+=2)
      {
        printf ("[%s] %02" PRIx32 " %08X %08X\n",
                __func__, i/2, p[i], p[i+1]);
      }
}
```

La funzione ***irq_remap()*** è necessaria per rimappare le interruzioni hardware nella tabella IDT, in modo che non intralcino quelle associate alle eccezioni. La funzione richiede l'indicazione del numero iniziale di interruzione per i due gruppi di IRQ (da IRQ 0 a IRQ 7 e da IRQ 8 a IRQ 15). Successivamente, nella funzione ***idt()***, viene usata ***irq_remap()*** in modo da rimappare le interruzioni hardware a partire da 32, per finire a 47.

Listato u171.5. './05/lib/int/irq_remap.c'

```
#include <kernel/int.h>
#include <stdio.h>
void
irq_remap (unsigned int offset_1, unsigned int offset_2)
{
    //
    // PIC_P è il PIC primario o «master»;
    // PIC_S è il PIC secondario o «slave».
    //
    // Quando si manifesta un IRQ che riguarda il PIC secondario,
    // il PIC primario riceve IRQ 2.
    //
    // ICW = initialization command word.
    // OCW = operation command word.
    //
    printf ("[%s] PIC (programmable interrupt controller) remap: ", __func__);

    outb (0x20, 0x10 + 0x01);   // Inizializzazione: 0x10 significa che
    outb (0xA0, 0x10 + 0x01);   // si tratta di ICW1; 0x01 significa che
    printf ("ICW1");            // si deve arrivare fino a ICW4.

    outb (0x21, offset_1);      // ICW2: PIC_P a partire da «offset_1».
    outb (0xA1, offset_2);      //       PIC_S a partire da «offset_2».
```

```
    printf (", ICW2");
    outb (0x21, 0x04);          // ICW3 PIC_P: IRQ2 pilotato da PIC_S.
    outb (0xA1, 0x02);          // ICW3 PIC_S: pilota IRQ2 di PIC_P.
    printf (", ICW3");
    outb (0x21, 0x01);          // ICW4: si precisa solo la modalità
    outb (0xA1, 0x01);          // del microprocessore; 0x01 = 8086.
    printf (", ICW4");

    outb (0x21, 0x00);          // OCW1: azzera la maschera in modo da
    outb (0xA1, 0x00);          // abilitare tutti i numeri IRQ.
    printf (", OCW1.\n");
}
```

Per caricare la tabella IDT dichiarata in memoria, occorre predisporre la copia del registro ***IDTR*** con i riferimenti necessari a raggiungerla, quindi va usata l'istruzione '**`LIDT`**', con il linguaggio assemblatore. La funzione ***idt_load()*** viene usata per pilotare l'istruzione '**`LIDT`**'.

Listato u171.6. '`./05/lib/int/idt_load.s`'

```
.globl  idt_load
#
idt_load:
    enter $0, $0
    .equ idtr_pointer,  8          # Primo argomento.
    mov  idtr_pointer(%ebp), %eax  # Copia il puntatore
                                   # in EAX.
    leave
    #
    lidt (%eax)   # Utilizza la tabella IDT a cui punta EAX.
    #
    ret
```

La funzione ***idt()*** utilizza le altre descritte in questa sezione, per mettere in funzione la gestione delle interruzioni.

Listato u171.7. '`./05/lib/int/idt.c`'

```
#include <kernel/int.h>
void
idt (void)
{
    //
    // Imposta i dati necessari al registro IDTR.
    //
    os.idtr.limit = (sizeof (os.idt) - 1);
    os.idtr.base  = (uint32_t) &os.idt[0];
    //
    // Azzera le voci previste dell'array «os.idt[]».
    //
    int i;
    for (i = 0; i < ((sizeof (os.idt)) / 8); i++)
      {
        idt_desc_int (i, 0, 0, 0, 0, 0);
      }
    //
    // Associa le interruzioni hardware da IRQ 0 a IRQ 7
    // a partire dal descrittore 32 e quelle da IRQ 8 a
    // IRQ 15, a partire dal descrittore 40.
    //
    irq_remap (32, 40);
    //
    // Associa le routine ISR ai descrittori della tabella
    // IDT.
    //
    idt_desc_int ( 0, (uint32_t) isr_0,  0x0008, 1, 0xE, 0);
    idt_desc_int ( 1, (uint32_t) isr_1,  0x0008, 1, 0xE, 0);
    idt_desc_int ( 2, (uint32_t) isr_2,  0x0008, 1, 0xE, 0);
    idt_desc_int ( 3, (uint32_t) isr_3,  0x0008, 1, 0xE, 0);
    idt_desc_int ( 4, (uint32_t) isr_4,  0x0008, 1, 0xE, 0);
    idt_desc_int ( 5, (uint32_t) isr_5,  0x0008, 1, 0xE, 0);
    idt_desc_int ( 6, (uint32_t) isr_6,  0x0008, 1, 0xE, 0);
    idt_desc_int ( 7, (uint32_t) isr_7,  0x0008, 1, 0xE, 0);
    idt_desc_int ( 8, (uint32_t) isr_8,  0x0008, 1, 0xE, 0);
    idt_desc_int ( 9, (uint32_t) isr_9,  0x0008, 1, 0xE, 0);
    idt_desc_int (10, (uint32_t) isr_10, 0x0008, 1, 0xE, 0);
    idt_desc_int (11, (uint32_t) isr_11, 0x0008, 1, 0xE, 0);
    idt_desc_int (12, (uint32_t) isr_12, 0x0008, 1, 0xE, 0);
    idt_desc_int (13, (uint32_t) isr_13, 0x0008, 1, 0xE, 0);
    idt_desc_int (14, (uint32_t) isr_14, 0x0008, 1, 0xE, 0);
    idt_desc_int (15, (uint32_t) isr_15, 0x0008, 1, 0xE, 0);
    idt_desc_int (16, (uint32_t) isr_16, 0x0008, 1, 0xE, 0);
    idt_desc_int (17, (uint32_t) isr_17, 0x0008, 1, 0xE, 0);
```



```
    idt_desc_int (18, (uint32_t) isr_18, 0x0008, 1, 0xE, 0);
    idt_desc_int (19, (uint32_t) isr_19, 0x0008, 1, 0xE, 0);
    idt_desc_int (20, (uint32_t) isr_20, 0x0008, 1, 0xE, 0);
    idt_desc_int (21, (uint32_t) isr_21, 0x0008, 1, 0xE, 0);
    idt_desc_int (22, (uint32_t) isr_22, 0x0008, 1, 0xE, 0);
    idt_desc_int (23, (uint32_t) isr_23, 0x0008, 1, 0xE, 0);
    idt_desc_int (24, (uint32_t) isr_24, 0x0008, 1, 0xE, 0);
    idt_desc_int (25, (uint32_t) isr_25, 0x0008, 1, 0xE, 0);
    idt_desc_int (26, (uint32_t) isr_26, 0x0008, 1, 0xE, 0);
    idt_desc_int (27, (uint32_t) isr_27, 0x0008, 1, 0xE, 0);
    idt_desc_int (28, (uint32_t) isr_28, 0x0008, 1, 0xE, 0);
    idt_desc_int (29, (uint32_t) isr_29, 0x0008, 1, 0xE, 0);
    idt_desc_int (30, (uint32_t) isr_10, 0x0008, 1, 0xE, 0);
    idt_desc_int (31, (uint32_t) isr_31, 0x0008, 1, 0xE, 0);
    idt_desc_int (32, (uint32_t) isr_32, 0x0008, 1, 0xE, 0);
    idt_desc_int (33, (uint32_t) isr_33, 0x0008, 1, 0xE, 0);
    idt_desc_int (34, (uint32_t) isr_34, 0x0008, 1, 0xE, 0);
    idt_desc_int (35, (uint32_t) isr_35, 0x0008, 1, 0xE, 0);
    idt_desc_int (36, (uint32_t) isr_36, 0x0008, 1, 0xE, 0);
    idt_desc_int (37, (uint32_t) isr_37, 0x0008, 1, 0xE, 0);
    idt_desc_int (38, (uint32_t) isr_38, 0x0008, 1, 0xE, 0);
    idt_desc_int (39, (uint32_t) isr_39, 0x0008, 1, 0xE, 0);
    idt_desc_int (40, (uint32_t) isr_40, 0x0008, 1, 0xE, 0);
    idt_desc_int (41, (uint32_t) isr_41, 0x0008, 1, 0xE, 0);
    idt_desc_int (42, (uint32_t) isr_42, 0x0008, 1, 0xE, 0);
    idt_desc_int (43, (uint32_t) isr_43, 0x0008, 1, 0xE, 0);
    idt_desc_int (44, (uint32_t) isr_44, 0x0008, 1, 0xE, 0);
    idt_desc_int (45, (uint32_t) isr_45, 0x0008, 1, 0xE, 0);
    idt_desc_int (46, (uint32_t) isr_46, 0x0008, 1, 0xE, 0);
    idt_desc_int (47, (uint32_t) isr_47, 0x0008, 1, 0xE, 0);
    //
    // Questo è per le chiamate di sistema.
    //
    idt_desc_int (128, (uint32_t) isr_128, 0x0008, 1, 0xE,
                  0);
    //
    // Rende operativa la tabella con le eccezioni e gli
    // IRQ.
    //
    idt_load (&os.idtr);
    //
    // Abilita le interruzioni hardware (IRQ).
    //
    sti ();
}
```

Gestione delle interruzioni

Le funzioni '**`isr_n()`**' si limitano a chiamare altre funzioni scritte in linguaggio C, per la gestione delle eccezioni, delle interruzioni hardware e per le chiamate di sistema. In questa fase vengono mostrate le funzioni per la gestione delle eccezioni, anche se in forma estremamente limitata, e si propongono temporaneamente delle funzioni fittizie per la gestione degli altri casi.

Listato u171.8. '`./05/lib/int/isr_exception_unrecoverable.c`'

```
#include <kernel/int.h>
#include <stdio.h>
void
isr_exception_unrecoverable (uint32_t eax, uint32_t ecx,
                             uint32_t edx, uint32_t ebx,
                             uint32_t ebp, uint32_t esi,
                             uint32_t edi, uint32_t ds,
                             uint32_t es, uint32_t fs,
                             uint32_t gs,
                             uint32_t interrupt,
                             uint32_t error, uint32_t eip,
                             uint32_t cs,
                             uint32_t eflags)
{
    printf ("[%s] ERROR: exception %i: \"%s\"\n",
            __func__, interrupt,
            exception_name (interrupt));
    //
    _Exit (0);
}
```

La funzione ***isr_exception_unrecoverable()***, appena mostrata, vie-

ne chiamata dal file ‘isr.s’, per le interruzioni che riguardano le eccezioni. La funzione si limita a visualizzare un messaggio di errore e a fermare il sistema. Per visualizzare il tipo di eccezione che si è verificato si avvale della funzione ***exception_name()*** che appare nel listato successivo.

Listato u171.9. ‘./05/lib/int/exception_name.c’

```
#include <kernel/int.h>
char
*exception_name (int exception)
{
    char *description[19] = {"division by zero",
                             "debug",
                             "non maskable interrupt",
                             "breakpoint",
                             "into detected overflow",
                             "out of bounds",
                             "invalid opcode",
                             "no coprocessor",
                             "double fault",
                             "coprocessor segmento overrun",
                             "bad TSS",
                             "segment not present",
                             "stack fault",
                             "general protection fault",
                             "page fault",
                             "unknown interrupt",
                             "coprocessor fault",
                             "alignment check",
                             "machine check"};
    //
    if (exception >= 0 && exception <= 18)
      {
        return description[exception];
      }
    else
      {
        return "unknown";
      }
}
```

A proposito della funzione ***exception_name()*** va osservata la particolarità del comportamento del compilatore GNU C, il quale utilizza, senza che ciò sia stato richiesto espressamente, la funzione standard ***memcpy()***. Pertanto, tale funzione deve essere disponibile, altrimenti, in fase di collegamento (*link*) la compilazione fallisce.

Per la gestione delle interruzioni hardware è competente la funzione ***isr_irq()***, ma per il momento viene proposta una versione provvisoria, priva di alcuna gestione, dove ci si limita a inviare il messaggio «EOI» ai PIC (*programmable interrupt controller*) coinvolti.

Listato u171.10. Una prima versione del file ‘./05/lib/int/isr_irq.c’

```
#include <kernel/int.h>
#include <kernel/io.h>
void
isr_irq (uint32_t eax, uint32_t ecx, uint32_t edx,
         uint32_t ebx, uint32_t ebp, uint32_t esi,
         uint32_t edi, uint32_t ds, uint32_t es,
         uint32_t fs,  uint32_t gs,  uint32_t interrupt)
{
    int irq = interrupt - 32;
    //
    // Finito il compito della funzione che deve reagire
    // all'interruzione IRQ, occorre informare i PIC
    // (programmable interrupt controller).
    //
    // Se il numero IRQ è tra 8 e 15, manda un messaggio
    // «EOI»
    // (End of IRQ) al PIC 2.
    //
    if (irq >= 8)
      {
        outb (0xA0, 0x20);
      }
    //
    // Poi manda un messaggio «EOI» al PIC 1.
    //
    outb (0x20, 0x20);
}
```


Anche la funzione ***isr_syscall()*** che dovrebbe prendersi cura delle chiamate di sistema, viene proposta inizialmente priva di alcun effetto.

Listato u171.11. Una prima versione del file ‘./05/lib/int/isr_syscall.c’

```
#include <kernel/int.h>
uint32_t
isr_syscall (uint32_t start, ...)
{
    return 0;
}
```

Piccole funzioni di contorno

Per facilitare l'accesso alle istruzioni ‘**STI**’ e ‘**CLI**’ del linguaggio assemblatore, vengono predisposte due funzioni con lo stesso nome.

Listato u171.12. ‘./05/lib/int/cli.s’

```
.globl cli
#
cli:
    cli
    ret
```

Listato u171.13. ‘./05/lib/int/sti.s’

```
.globl sti
#
sti:
    sti
    ret
```

Verifica del funzionamento

Per verificare il lavoro svolto fino a questo punto, è necessario sviluppare ulteriormente i file ‘kernel_main.c’, dove in particolare si va a produrre un errore che causa un eccezione dovuta a una divisione per zero.

Figura u171.14. Modifiche da apportare al file ‘./05/kernel/kernel_main.c’

```
#include <kernel/kernel.h>
#include <kernel/build.h>
#include <stdio.h>
#include <kernel/gdt.h>
#include <kernel/mm.h>
#include <stdlib.h>
#include <kernel/int.h>
…
        kernel_memory (info);
        //
        // Predispone la tabella GDT.
        //
        gdt ();
        //
        // Predispone la memoria libera per l'utilizzo.
        //
        mm_init ();
        //
        // Omissis.
        //
        //
        // Predispone la tabella IDT.
        //
        idt();
        //
        // Crea un errore volontario.
        //
        int x = 3;
        x = 7 / (x - 3);        // x = 7 / 0
…
```

Dopo avere ricompilato, riavviando la simulazione si deve ottenere una schermata simile a quella seguente, dove alla fine si vede la segnalazione di errore dovuta alla divisione per zero:

```
05 20070821144531
[mboot_show] flags: 00000000000000000000011111100111 mlow: 027F mhigh: 00007BC0
[mboot_show] bootdev: 00FFFFFF cmdline: "(fd0)/kernel"
[kernel_memory_show] kernel 00100000..0010D8BC  avail. 0010D8BC..01EF0000
[kernel_memory_show] text   00100000..001049DC  rodata 001049E0..00104F34
[kernel_memory_show] data   00104F34..00104F34  bss    00104F40..0010D8BC
[kernel_memory_show] limit  00001EF0
[gdt_print] base: 0x0010CF88 limit: 0x0017
[gdt_print] 0 00000000000000000000000000000000 00000000010000000001000000000000
[gdt_print] 1 00000000000000000001111011110000 00000000110000001001101000000000
[gdt_print] 2 00000000000000000001111011110000 00000000110000001001001000000000
[mm_init] available memory: 31336256 byte
[irq_remap] PIC (programmable interrupt controller) remap: ICW1, ICW2, ICW3,
ICW4, OCW1.
[isr_exception_unrecoverable] ERROR: exception 0: "division by zero"
```