Übung zu Betriebssystembau

Interruptbehandlung

25. November 2022

Peter Ulbrich & Alexander Lochmann
(Mit Material vom Lehrstuhl 4 der FAU)

Arbeitsgruppe Systemsoftware
Technische Universität Dortmund

technische universität
dortmund

arbeitsgruppe
systemsoftware

Interrupts und Traps

Dann schlug ein Blitz ein …

Dann schlug ein Blitz ein …

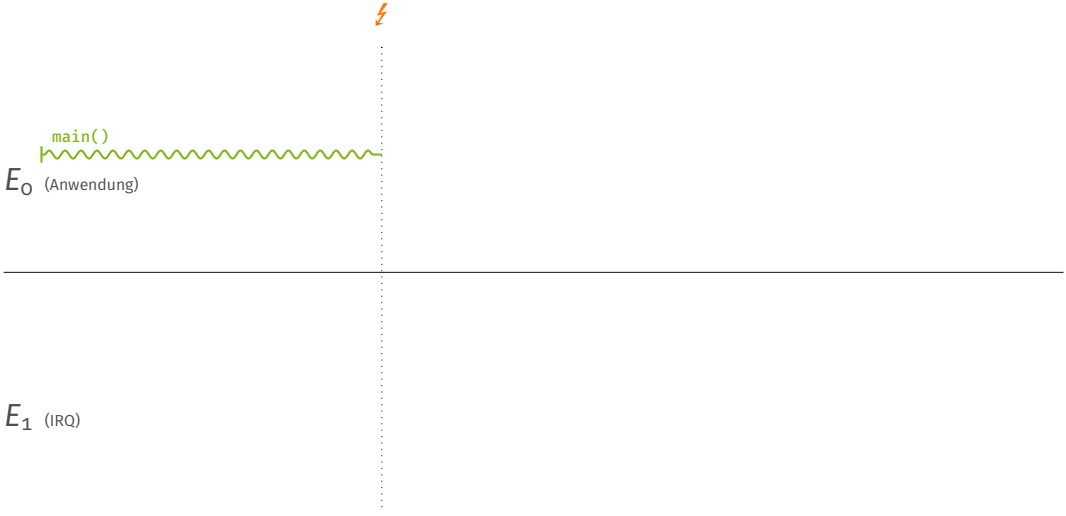
Dann schlug ein Blitz ein …

Unterbrechung aus Anwendungssicht

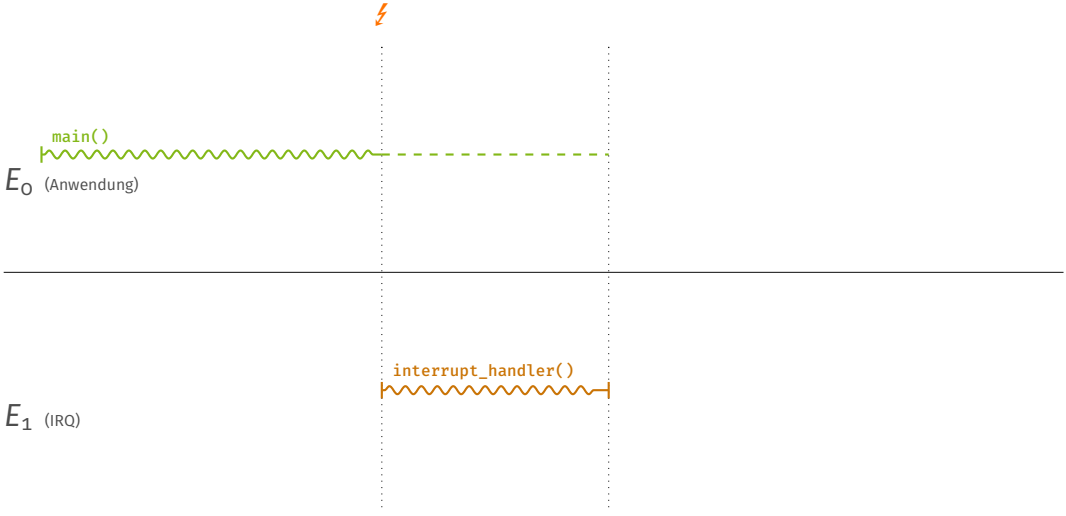
E_0 (Anwendung)

E_1 (IRQ)

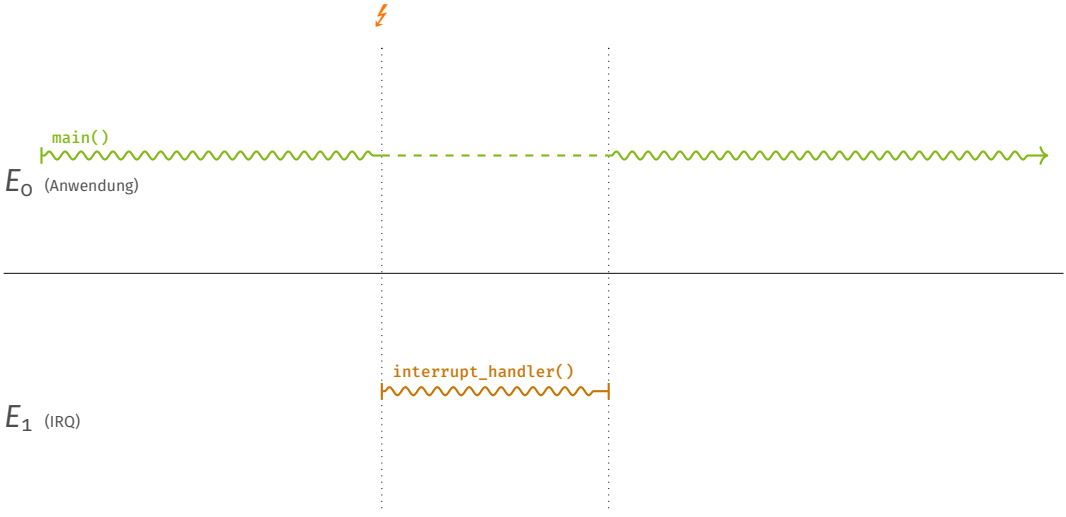
Unterbrechung aus Anwendungssicht



Unterbrechung aus Anwendungssicht



Unterbrechung aus Anwendungssicht



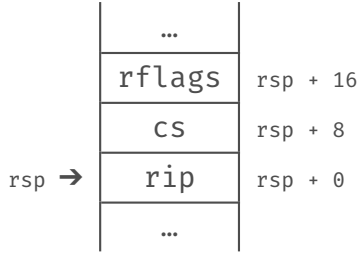
Zustandsicherung (1)

Was muss muss **mindestens** gesichert werden?

Zustandsicherung (1)

Was muss muss **mindestens** gesichert werden?

- CPU sichert automatisch
  - **rip** Instruktionszeiger/Rücksprungadresse
  - **rflags** Status/Condition Codes
  - **cs** Aktuelles Code Segment

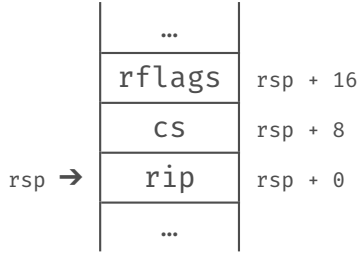


Zustandsicherung (1)

Was muss muss **mindestens** gesichert werden?

- CPU sichert automatisch

  rip Instruktionszeiger/Rücksprungadresse
  rflags Status/Condition Codes
  cs Aktuelles Code Segment



- Wiederherstellung des ursprünglichen Prozessorzustandes durch Befehl `iretq`

Unterbrechungsbehandlung

```
;; Assembler
interrupt_entry:
  ;; Behandle IRQ


  iretq
```

Unterbrechungsbehandlung

unter Verwendung einer Hochsprache

```
;; Assembler
interrupt_entry:
  ;; Behandle IRQ
  ;; in Hochsprache
  call interrupt_handler
  iretq
```

Unterbrechungsbehandlung

unter Verwendung einer Hochsprache

```
;; Assembler
interrupt_entry:
  ;; Behandle IRQ
  ;; in Hochsprache
  call interrupt_handler
  iretq
```

```
// C++

void interrupt_handler()
{
    // Magie.
}
```

Unterbrechungsbehandlung

unter Verwendung einer Hochsprache

```
;; Assembler
interrupt_entry:
  ;; Behandle IRQ
  ;; in Hochsprache
  call interrupt_handler
  iretq
```

```
// C++

void interrupt_handler()
{
    // Magie.
}
```

```
01 heinloth:~/oostubs$ make
02 LD          .build/system64
03 .build/interrupt/handler.asm.o: in function `interrupt_entry':
04 interrupt/handler.asm:(.text+0x16): undefined reference to `
       interrupt_handler'
```

Unterbrechungsbehandlung

unter Verwendung einer Hochsprache

```
;; Assembler
interrupt_entry:
  ;; Behandle IRQ
  ;; in Hochsprache
  call interrupt_handler
  iretq
```

```
// C++

void interrupt_handler()
{
    // Magie.
}
```

```
heinloth:~/oostubs$ objdump -d .build/interrupt/handler.o
Disassembly of section .text:

0000000000000000 <_Z17interrupt_handlerv>:
   0:  c3                      retq
```

Unterbrechungsbehandlung

unter Verwendung einer Hochsprache

```
;; Assembler
interrupt_entry:
  ;; Behandle IRQ
  ;; in Hochsprache
  call interrupt_handler
  iretq
```

```
// C++ (mit C Linkage)
extern "C"
void interrupt_handler()
{
    // Magie.
}
```

Unterbrechungsbehandlung

unter Verwendung einer Hochsprache

```
;; Assembler
interrupt_entry:
  ;; Behandle IRQ
  ;; in Hochsprache
  call interrupt_handler
  iretq
```

```
// C++ (mit C Linkage)
extern "C"
void interrupt_handler()
{
    // Magie.
}
```

```
01 heinloth:~/oostubs$ objdump -d .build/interrupt/handler.o
02 Disassembly of section .text:
03
04 0000000000000000 <interrupt_handler>:
05    0:  f3 c3                   repz ret
```

Zustandssicherung (2)

Was ist mit den restlichen Registern?

Zustandssicherung (2)

Was ist mit den restlichen Registern?

- Müssen durch den Interrupthandler selbst gesichert werden.
  - entweder im Assembler-Teil oder
  - der Compiler generiert bereits entsprechend Code

Zustandssicherung (2)

Was ist mit den restlichen Registern?

- Müssen durch den Interrupthandler selbst gesichert werden.
  - entweder im Assembler-Teil oder
  - der Compiler generiert bereits entsprechend Code
- Kontextsicherung beim Aufruf von Funktionen

Zustandssicherung (2)

Was ist mit den restlichen Registern?

- Müssen durch den Interrupthandler selbst gesichert werden.
  - entweder im Assembler-Teil oder
  - der Compiler generiert bereits entsprechend Code
- Kontextsicherung beim Aufruf von Funktionen
  1. Aufrufende Funktion sichert alle Register, die sie braucht

Zustandssicherung (2)

Was ist mit den restlichen Registern?

- Müssen durch den Interrupthandler selbst gesichert werden.
  - entweder im Assembler-Teil oder
  - der Compiler generiert bereits entsprechend Code
- Kontextsicherung beim Aufruf von Funktionen
  1. Aufrufende Funktion sichert alle Register, die sie braucht
  2. Aufgerufene Funktion sichert alle Register, die sie verändert

Zustandssicherung (2)

Was ist mit den restlichen Registern?

- Müssen durch den Interrupthandler selbst gesichert werden.
  - entweder im Assembler-Teil oder
  - der Compiler generiert bereits entsprechend Code
- Kontextsicherung beim Aufruf von Funktionen
  1. Aufrufende Funktion sichert alle Register, die sie braucht
  2. Aufgerufene Funktion sichert alle Register, die sie verändert
  3. Ein Teil der Register wird vom Aufrufer, ein anderer Teil vom Aufgerufenen gesichert

Zustandssicherung (2)

Was ist mit den restlichen Registern?

- Müssen durch den Interrupthandler selbst gesichert werden.
  - entweder im Assembler-Teil oder
  - der Compiler generiert bereits entsprechend Code
- Kontextsicherung beim Aufruf von Funktionen
  1. Aufrufende Funktion sichert alle Register, die sie braucht
  2. Aufgerufene Funktion sichert alle Register, die sie verändert
  3. Ein Teil der Register wird vom Aufrufer, ein anderer Teil vom Aufgerufenen gesichert
- In der Praxis wird Variante 3 verwendet
  - Aufteilung ist grundsätzlich compilerspezifisch
  - Um Interoperabilität auf Binärcodeebene sicher zu stellen gibt es jedoch Konventionen (bei x64 zwei: *Microsoft* und *System V*)

  → Aufrufkonvention ist Teil der *Application Binary Interface* (ABI)

Aufteilung der Register in zwei Gruppen

- Flüchtige Register (*scratch registers*)
  - Compiler geht davon aus, dass Unterprogramm den Inhalt verändert
  - Aufrufer muss Inhalt gegebenenfalls sichern
  - Beim x64 (nach *System V* ABI) sind `rax`, `rcx`, `rdx`, `rsi`, `rdi` und `r8` – `r11` als flüchtig definiert

Aufteilung der Register in zwei Gruppen

- Flüchtige Register (*scratch registers*)
  - Compiler geht davon aus, dass Unterprogramm den Inhalt verändert
  - Aufrufer muss Inhalt gegebenenfalls sichern
  - Beim x64 (nach *System V* ABI) sind `rax`, `rcx`, `rdx`, `rsi`, `rdi` und `r8` – `r11` als flüchtig definiert
- Nicht-flüchtige Register (*non-scratch registers*)
  - Compiler geht davon aus, dass der Inhalt durch Unterprogramm nicht verändert wird
  - Aufgerufene Funktion muss Inhalt gegebenenfalls sichern
  - Beim x64 sind alle sonstigen Register als nicht-flüchtig definiert: `rbx`, `rbp`, `rsp` und `r12` – `r15`

Aufteilung der Register in zwei Gruppen

- Flüchtige Register (*scratch registers*)
  - Compiler geht davon aus, dass Unterprogramm den Inhalt verändert
  - Aufrufer muss Inhalt gegebenenfalls sichern
  - Beim x64 (nach *System V* ABI) sind `rax`, `rcx`, `rdx`, `rsi`, `rdi` und `r8` – `r11` als flüchtig definiert
- Nicht-flüchtige Register (*non-scratch registers*)
  - Compiler geht davon aus, dass der Inhalt durch Unterprogramm nicht verändert wird
  - Aufgerufene Funktion muss Inhalt gegebenenfalls sichern
  - Beim x64 sind alle sonstigen Register als nicht-flüchtig definiert: `rbx`, `rbp`, `rsp` und `r12` – `r15`

Unterbrechungsbehandlungen müssen auch flüchtige Register sichern!

Kontextsicherung in der Unterbrechungsbehandlung

```
;; Assembler
interrupt_entry:

  call interrupt_handler

  iretq
```

Kontextsicherung in der Unterbrechungsbehandlung

```
;; Assembler
interrupt_entry:
  ;; Kontext sichern
  push rax
  push rcx
  ;; ...
  push r11


  call interrupt_handler
  ;; wiederherstellen
  pop r11
  ;; ...
  pop rcx
  pop rax
  iretq
```

Kontextsicherung in der Unterbrechungsbehandlung

```
;; Assembler
interrupt_entry:
  ;; Kontext sichern
  push rax
  push rcx
  ;; ...
  push r11


  call interrupt_handler
  ;; wiederherstellen
  pop r11
  ;; ...
  pop rcx
  pop rax
  iretq
```

```
// C++


extern "C"
void interrupt_handler()
{
    // Magie.
}
```

Kontextsicherung in der Unterbrechungsbehandlung

```
;; Assembler
interrupt_entry:
  ;; Kontext sichern
  push rax
  push rcx
  ;; ...
  push r11


  call interrupt_handler
  ;; wiederherstellen
  pop r11
  ;; ...
  pop rcx
  pop rax
  iretq
```

```
// C++
struct Context {









} __attribute__((packed));

extern "C"
void interrupt_handler(Context* c)
{
    // Magie.
}
```

Kontextsicherung in der Unterbrechungsbehandlung

```
;; Assembler
interrupt_entry:
  ;; Kontext sichern
  push rax
  push rcx
  ;; ...
  push r11


  call interrupt_handler
  ;; wiederherstellen
  pop r11
  ;; ...
  pop rcx
  pop rax
  iretq
```

```
// C++
struct Context {
    uint64_t r11;
    // ...
    uint64_t rcx;
    uint64_t rax;



} __attribute__((packed));

extern "C"
void interrupt_handler(Context* c)
{
    // Magie.
}
```

Parameterübergabe

- auf Stack
  - bei x86 war dies gemäß der *C declaration* der Standard

Parameterübergabe

- auf Stack
  - bei x86 war dies gemäß der *C declaration* der Standard
- in Register
  - Vorteil: schneller
  - Problem: Anzahl der Register begrenzt
- kombiniert
  - die ersten Parameter via Register, danach bei Bedarf Stack

Parameterübergabe

- auf Stack
  - bei x86 war dies gemäß der *C declaration* der Standard
- in Register
  - Vorteil: schneller
  - Problem: Anzahl der Register begrenzt
- kombiniert
  - die ersten Parameter via Register, danach bei Bedarf Stack
  - auch nach x64 *System V* ABI:
    - Parameter zuerst in Register `rdi`, `rsi`, `rdx` `rcx`, `r8` und `r9`
    - im Userspace danach auch in die Register `xmm0` – `xmm7`
    - Rest auf Stack (letzter Parameter wird als erstes gepushed)

Kontextsicherung in der Unterbrechungsbehandlung

```
;; Assembler
interrupt_entry:
  ;; Kontext sichern
  push rax
  push rcx
  ;; ...
  push r11


  call interrupt_handler
  ;; wiederherstellen
  pop r11
  ;; ...
  pop rcx
  pop rax
  iretq
```

```
// C++
struct Context {
    uint64_t r11;
    // ...
    uint64_t rcx;
    uint64_t rax;



} __attribute__((packed));

extern "C"
void interrupt_handler(Context* c)
{
    // Magie.
}
```

Kontextsicherung in der Unterbrechungsbehandlung

```
;; Assembler
interrupt_entry:
  ;; Kontext sichern
  push rax
  push rcx
  ;; ...
  push r11
  ;; Pointer auf Stack
  mov rdi, rsp
  call interrupt_handler
  ;; wiederherstellen
  pop r11
  ;; ...
  pop rcx
  pop rax
  iretq
```

```
// C++
struct Context {
    uint64_t r11;
    // ...
    uint64_t rcx;
    uint64_t rax;




} __attribute__((packed));

extern "C"
void interrupt_handler(Context* c)
{
    // Magie.
}
```

Kontextsicherung in der Unterbrechungsbehandlung

```
;; Assembler
interrupt_entry:
  ;; Kontext sichern
  push rax
  push rcx
  ;; ...
  push r11
  ;; Pointer auf Stack
  mov rdi, rsp
  call interrupt_handler
  ;; wiederherstellen
  pop r11
  ;; ...
  pop rcx
  pop rax
  iretq
```

```
// C++
struct Context {
    uint64_t r11;
    // ...
    uint64_t rcx;
    uint64_t rax;
    uint64_t rip;
    uint64_t cs;
    uint64_t rflags;
} __attribute__((packed));

extern "C"
void interrupt_handler(Context* c)
{
    // Magie.
}
```

Dann schlug ein Blitz ein …

Dann schlug ein Blitz ein …

Interruptvektoren (x86/x64)

Interruptvektoren (x86/x64)

Interruptvektoren (x86/x64)

0	Division-by-Zero
1	Debug Exception
2	Non-Maskable Interrupt(NMI)
3	Breakpoint (INT 3)
4	Overflow Exception
5	Bound Exception
6	Invalid Opcode
7	FPU not Available
8	Double Fault
10	Invalid TSS
11	Segment not Present
12	Stack Exception
13	General Protection Fault
14	Page Fault
16	Floating-Point Error
17	Alignment Check
18	Machine Check

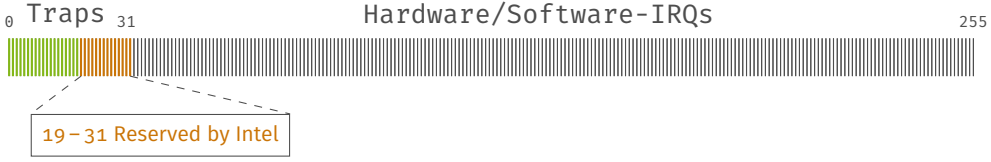
Interruptvektoren (x86/x64)

0	**Division-by-Zero**
1	Debug Exception
2	Non-Maskable Interrupt(NMI)
3	**Breakpoint (INT 3)**
4	Overflow Exception
5	Bound Exception
6	**Invalid Opcode**
7	FPU not Available
8	Double Fault
10	Invalid TSS
11	Segment not Present
12	Stack Exception
13	**General Protection Fault**
14	Page Fault
16	Floating-Point Error
17	Alignment Check
18	Machine Check

Interruptvektoren (x86/x64)

0	Division-by-Zero
1	Debug Exception
2	Non-Maskable Interrupt(NMI)
3	Breakpoint (INT 3)
4	Overflow Exception
5	Bound Exception
6	Invalid Opcode
7	FPU not Available
8	Double Fault
10	Invalid TSS
11	Segment not Present
12	Stack Exception
13	General Protection Fault
14	**Page Fault**
16	Floating-Point Error
17	Alignment Check
18	Machine Check

Interruptvektoren (x86/x64)



Interruptvektoren (x86/x64)

32 – 255 Einträge für IRQs

- Softwareauslösung mit `int <vec#>`
- Hardwareauslösung durch externe Geräte

Interruptvektoren (x86/x64)

Kann durch Prozessorbefehle maskiert werden

- `cli` (**cl**ear **i**nterrupt flag) Interruptleitung sperren
- `sti` (**s**e**t** **i**nterrupt flag) Interruptleitung freigeben

Unterbrechungsbehandlung

```
;; Assembler
interrupt_entry:
  ;; Kontext sichern
  push rax
  push rcx
  ;; ...
  push r11
  ;; Pointer auf Stack
  mov rdi, rsp


  call interrupt_handler
  ;; wiederherstellen
  pop r11
  ;; ...
  pop rcx
  pop rax
  iretq
```

```
// C++
extern "C"
void interrupt_handler(
    Context* c

  )
{
    // Magie:









}
```

Unterbrechungsbehandlung

```
;; Assembler
interrupt_entry:
  ;; Kontext sichern
  push rax
  push rcx
  ;; ...
  push r11
  ;; Pointer auf Stack
  mov rdi, rsp


  call interrupt_handler
  ;; wiederherstellen
  pop r11
  ;; ...
  pop rcx
  pop rax
  iretq
```

```
// C++
extern "C"
void interrupt_handler(
    Context* c,
    uint32_t vector
  )
{
    // Magie:
    switch (vector){
        case KBD:
            kbd.magic();
            break;
        case TMR:
            tmr.magic();
            break;
    }
}
```

Unterbrechungsbehandlung für Vektor 6

```
;; Assembler
interrupt_entry_6:
  ;; Kontext sichern
  push rax
  push rcx
  ;; ...
  push r11
  ;; Pointer auf Stack
  mov rdi, rsp
  ;; Vektornummer
  mov rsi, 6
  call interrupt_handler
  ;; wiederherstellen
  pop r11
  ;; ...
  pop rcx
  pop rax
  iretq
```

```
// C++
extern "C"
void interrupt_handler(
    Context* c,
    uint32_t vector
  )
{
    // Magie:
    switch (vector){
        case KBD:
            kbd.magic();
            break;
        case TMR:
            tmr.magic();
            break;
    }
}
```

Unterbrechungsbehandlung beim Binden

```
;; Assembler
interrupt_entry_6:
  ;; Kontext sichern
  push rax
  push rcx
  ;; ...
  push r11
  ;; Pointer auf Stack
  mov rdi, rsp
  ;; Vektornummer
  mov rsi, 6
  call 0x10070f0 <interrupt_handler>
  ;; wiederherstellen
  pop r11
  ;; ...
  pop rcx
  pop rax
  iretq
```

```
01 heinloth:~/oostubs$ make
02 ASM  interrupt/handler.asm
03 CXX  interrupt/handler.cc
04 LD   .build/system64
```

Speicheradressen beim **Binden**:

```
100 70f0 <interrupt_handler>
```

Unterbrechungsbehandlung beim Binden

```
;; Assembler
interrupt_entry_6:
  ;; Kontext sichern
  push rax
  push rcx
  ;; ...
  push r11
  ;; Pointer auf Stack
  mov rdi, rsp
  ;; Vektornummer
  mov rsi, 6
  call interrupt_handler
  ;; wiederherstellen
  pop r11
  ;; ...
  pop rcx
  pop rax
  iretq
```

```
01 heinloth:~/oostubs$ make
02 ASM  interrupt/handler.asm
03 CXX  interrupt/handler.cc
04 LD   .build/system64
```

Speicheradressen beim **Binden**:

```
100 70f0 <interrupt_handler>

100 0230 <interrupt_entry_6>
```

Unterbrechungsbehandlung beim Binden

```
;; Assembler
interrupt_entry_6:
  ;; Kontext sichern
  push rax
  push rcx
  ;; ...
  push r11
  ;; Pointer auf Stack
  mov rdi, rsp
  ;; Vektornummer
  mov rsi, 6
  call interrupt_handler
  ;; wiederherstellen
  pop r11
  ;; ...
  pop rcx
  pop rax
  iretq
```

```
heinloth:~/oostubs$ make
ASM   interrupt/handler.asm
CXX   interrupt/handler.cc
LD    .build/system64
```

Speicheradressen beim **Binden**:

```
100 70f0 <interrupt_handler>
         ...
100 0230 <interrupt_entry_6>
100 0200 <interrupt_entry_5>
100 01d0 <interrupt_entry_4>
100 01a0 <interrupt_entry_3>
100 0170 <interrupt_entry_2>
100 0140 <interrupt_entry_1>
100 0110 <interrupt_entry_0>
```

Generische Unterbrechungsbehandlungen

```
%macro IRQ 1
align 8
interrupt_entry_%1:
  ;; Kontext sichern
  push rax
  push rcx
  ;; ...
  push r11
  ;; Pointer auf Stack
  mov rdi, rsp
  ;; Vektornummer
  mov rsi, %1
  call interrupt_handler
  ;; wiederherstellen
  pop r11
  ;; ...
  pop rcx
  pop rax
  iretq
%endmacro
```

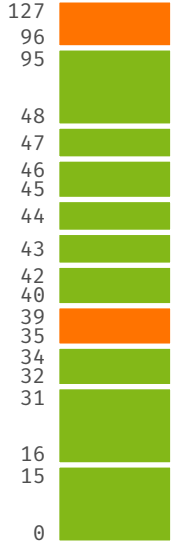
```
heinloth:~/oostubs$ make
ASM   interrupt/handler.asm
CXX   interrupt/handler.cc
LD    .build/system64
```

Speicheradressen beim **Binden**:

```
100 70f0 <interrupt_handler>
         ...
100 0230 <interrupt_entry_6>
100 0200 <interrupt_entry_5>
100 01d0 <interrupt_entry_4>
100 01a0 <interrupt_entry_3>
100 0170 <interrupt_entry_2>
100 0140 <interrupt_entry_1>
100 0110 <interrupt_entry_0>
```

Woher weiß die CPU wo die entsprechende Unterbrechungsbehandlung liegt?

Interrupt Deskriptor



Unused – muss `0` sein

Offset (high): *oberer* Teil der Einsprungsadresse für die Interruptbehandlung (z.B. `interrupt_entry_6`)

Present: Eintrag aktiv (`1`) oder inaktiv (`0`)

Descriptor Privilege Level

Storage Segment: `0` für Interrupt und Traps

Mode: 16-bit (`0`) oder 32/64-bit (`1`)

Type: Task (`5`), Interrupt (`6`) oder Trap (`7`)?

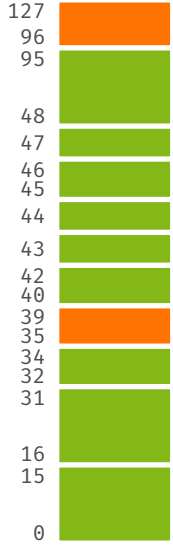
Unused – muss `0` sein

Interrupt Stack Table

Selector: Codesegment, in das beim Interrupt gewechselt wird (i.d.R. Kernel-Codesegment)

Offset (low): *unterer* Teil der Einsprungsadresse für die Interruptbehandlung

Interrupt Deskriptor – Beispiel für Unterbrechung Nr. 6



Unused – muss `0` sein

Offset (high): *oberer* Teil der Einsprungsadresse für die Interruptbehandlung (z.B. `interrupt_entry_6`)

Present: Eintrag aktiv (`1`) oder inaktiv (`0`)

Descriptor Privilege Level

Storage Segment: `0` für Interrupt und Traps

Mode: 16-bit (`0`) oder 32/64-bit (`1`)

Type: Task (`5`), Interrupt (`6`) oder Trap (`7`)?

Unused – muss `0` sein

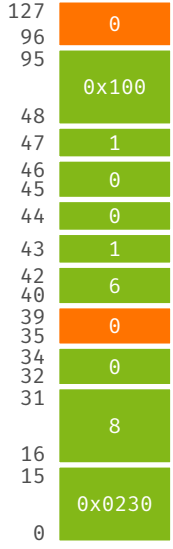
Interrupt Stack Table

Selector: Codesegment, in das beim Interrupt gewechselt wird (i.d.R. Kernel-Codesegment)

Offset (low): *unterer* Teil der Einsprungsadresse für die Interruptbehandlung

für `100 0230 <interrupt_entry_6>`

Interrupt Deskriptor – Beispiel für Unterbrechung Nr. 6



Unused – muss `0` sein

Offset (high): *oberer* Teil der Einsprungsadresse für die Interruptbehandlung (z.B. `interrupt_entry_6`)

Present: Eintrag aktiv (`1`) oder inaktiv (`0`)

Descriptor Privilege Level

Storage Segment: `0` für Interrupt und Traps

Mode: 16-bit (`0`) oder 32/64-bit (`1`)

Type: Task (`5`), Interrupt (`6`) oder Trap (`7`)?

Unused – muss `0` sein

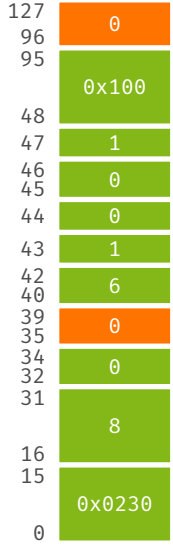
Interrupt Stack Table

Selector: Codesegment, in das beim Interrupt gewechselt wird (i.d.R. Kernel-Codesegment)

Offset (low): *unterer* Teil der Einsprungsadresse für die Interruptbehandlung

für `100 0230 <interrupt_entry_6>`

Interrupt Deskriptor – Beispiel für Unterbrechung Nr. 6



Unused – muss `0` sein

Offset (high): *oberer* Teil der Einsprungsadresse für die Interruptbehandlung (z.B. `interrupt_entry_6`)

Present: Eintrag aktiv (`1`) oder inaktiv (`0`)

Descriptor Privilege Level

Storage Segment: `0` für Interrupt und Traps

Mode: 16-bit (`0`) oder 32/64-bit (`1`)

Type: Task (`5`), Interrupt (`6`) oder Trap (`7`)?

Unused – muss `0` sein

Interrupt Stack Table

Selector: Codesegment, in das beim Interrupt gewechselt wird (i.d.R. Kernel-Codesegment)

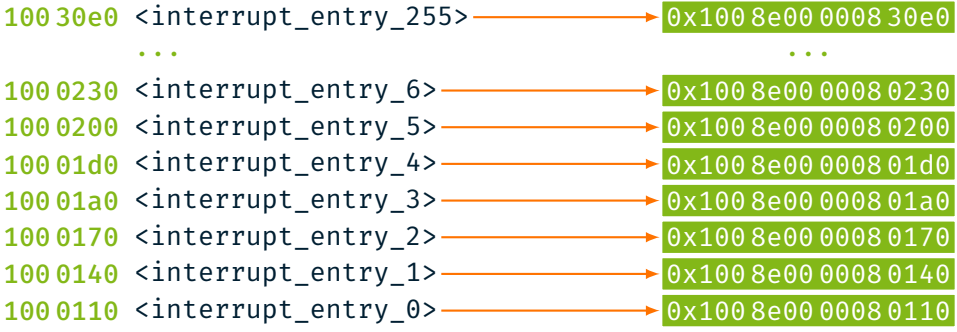
Offset (low): *unterer* Teil der Einsprungsadresse für die Interruptbehandlung

für `100 0230 <interrupt_entry_6>` → `0x100 8e00 0008 0230`

Interrupt Deskriptor Tabelle (IDT)

```
100 30e0 <interrupt_entry_255>
         ...
100 0230 <interrupt_entry_6>
100 0200 <interrupt_entry_5>
100 01d0 <interrupt_entry_4>
100 01a0 <interrupt_entry_3>
100 0170 <interrupt_entry_2>
100 0140 <interrupt_entry_1>
100 0110 <interrupt_entry_0>
```

Interrupt Deskriptor Tabelle (IDT)



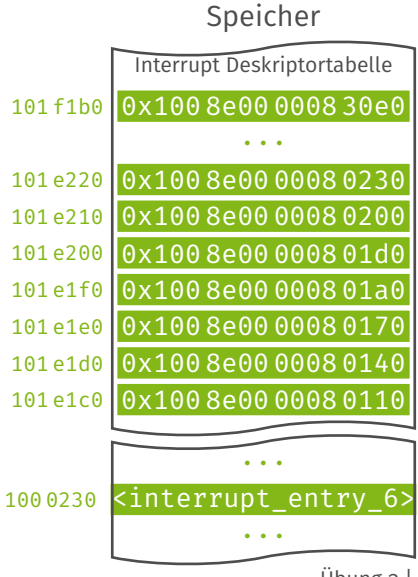
Interrupt Deskriptor Tabelle (IDT)

```
100 30e0 <interrupt_entry_255>
         ...
100 0230 <interrupt_entry_6>
100 0200 <interrupt_entry_5>
100 01d0 <interrupt_entry_4>
100 01a0 <interrupt_entry_3>
100 0170 <interrupt_entry_2>
100 0140 <interrupt_entry_1>
100 0110 <interrupt_entry_0>
```

Interrupt Deskriptor Tabelle (IDT)

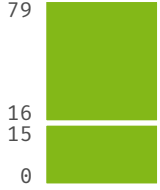
```
100 30e0 <interrupt_entry_255>
         ...
100 0230 <interrupt_entry_6>
100 0200 <interrupt_entry_5>
100 01d0 <interrupt_entry_4>
100 01a0 <interrupt_entry_3>
100 0170 <interrupt_entry_2>
100 0140 <interrupt_entry_1>
100 0110 <interrupt_entry_0>
```

Interrupt Deskriptor Tabelle (IDT)



Interrupt Deskriptor Tabelle (IDT)

IDT-Register `idtr`



Basis: Startadresse der IDT

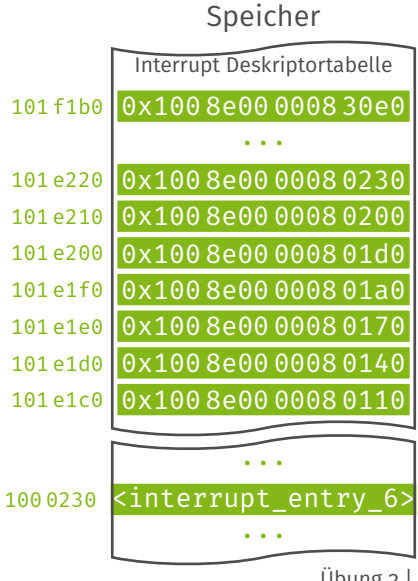
Limit: Bytes *Einträge * 16 - 1*

Speicher

Interrupt Deskriptortabelle

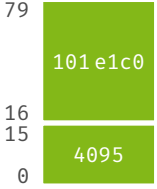
101 f1b0	0x100 8e00 0008 30e0
	...
101 e220	0x100 8e00 0008 0230
101 e210	0x100 8e00 0008 0200
101 e200	0x100 8e00 0008 01d0
101 e1f0	0x100 8e00 0008 01a0
101 e1e0	0x100 8e00 0008 0170
101 e1d0	0x100 8e00 0008 0140
101 e1c0	0x100 8e00 0008 0110
	...
100 0230	<interrupt_entry_6>
	...

Interrupt Deskriptor Tabelle (IDT)



Interrupt Deskriptor Tabelle (IDT)

IDT-Register `idtr`



Basis: Startadresse der IDT

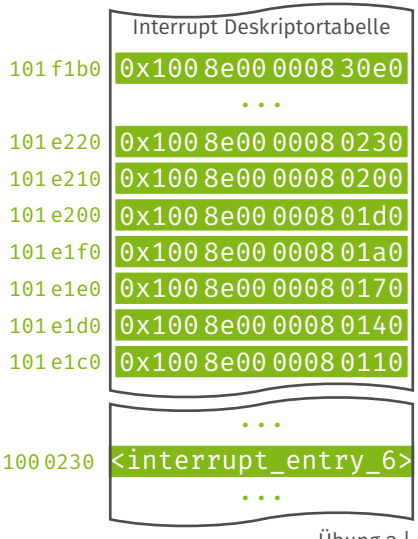
Limit: Bytes *Einträge * 16 - 1*

Instruktionen:

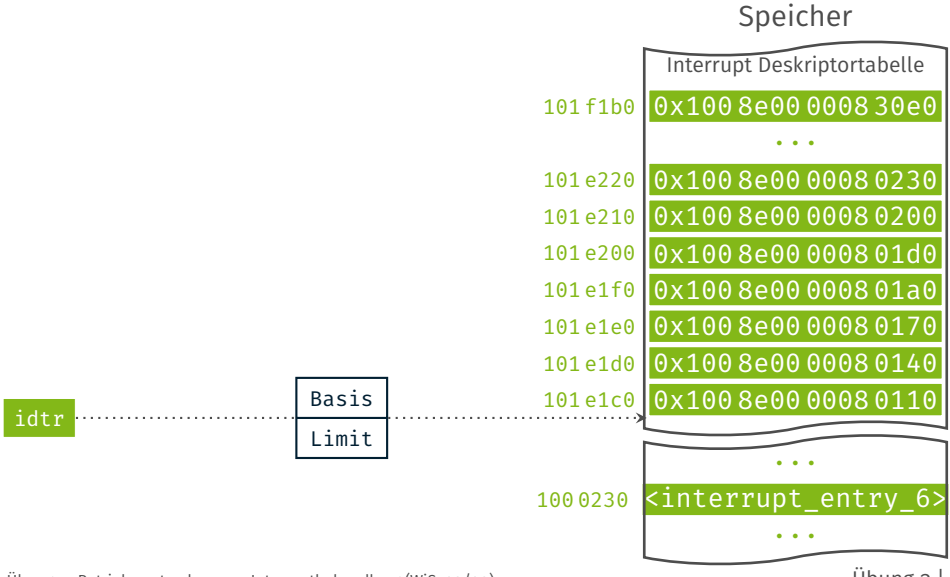
`lidt` in Register laden

`sidt` aus Register lesen

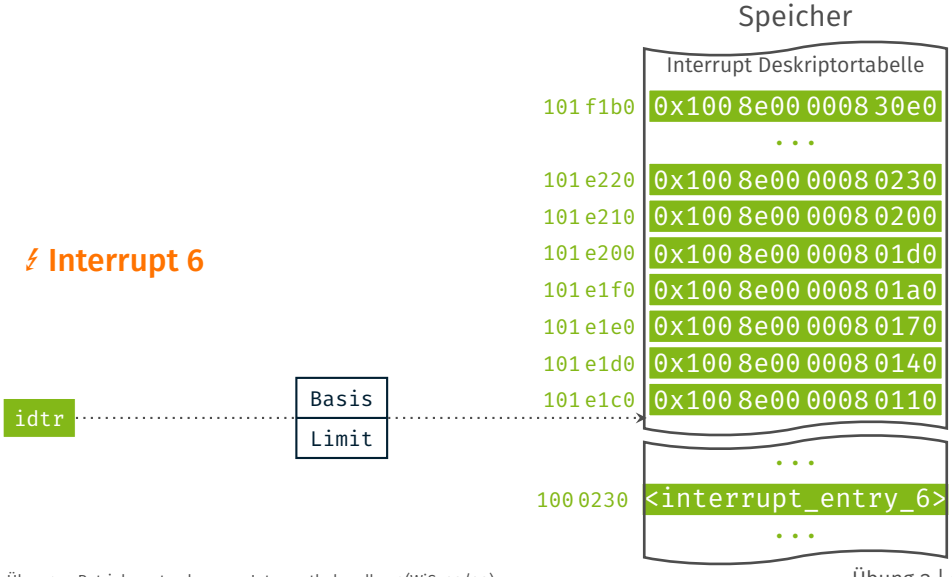
Speicher



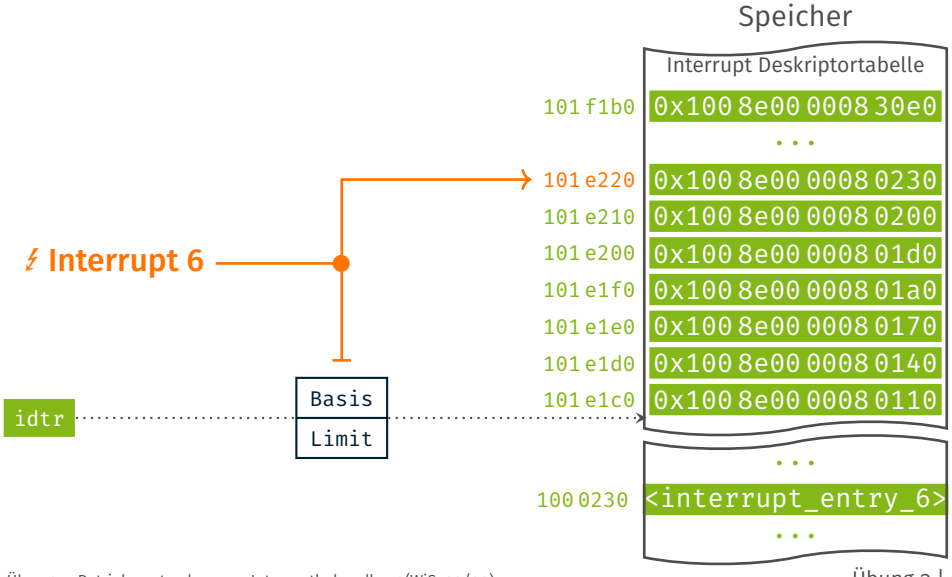
Interrupt Deskriptor Tabelle (IDT)



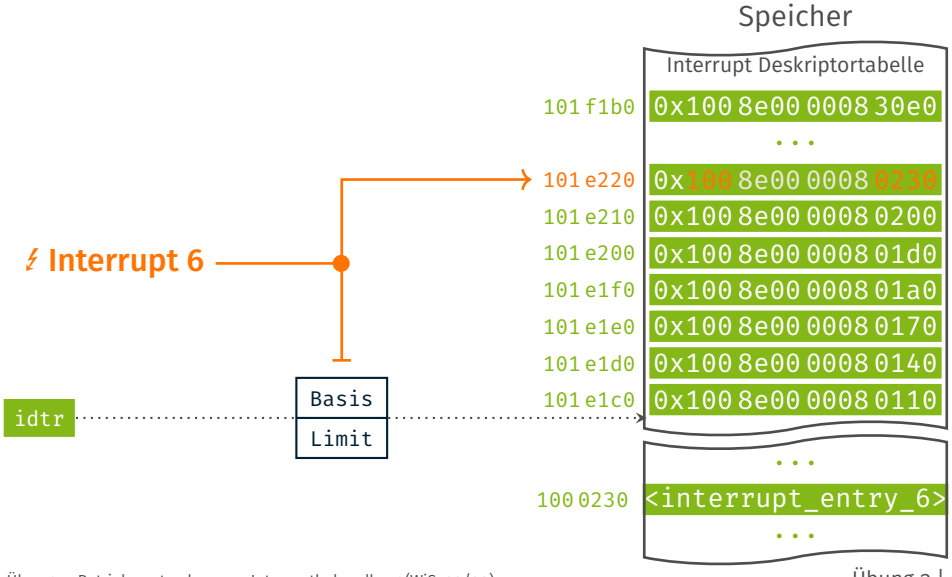
Interrupt Deskriptor Tabelle (IDT)



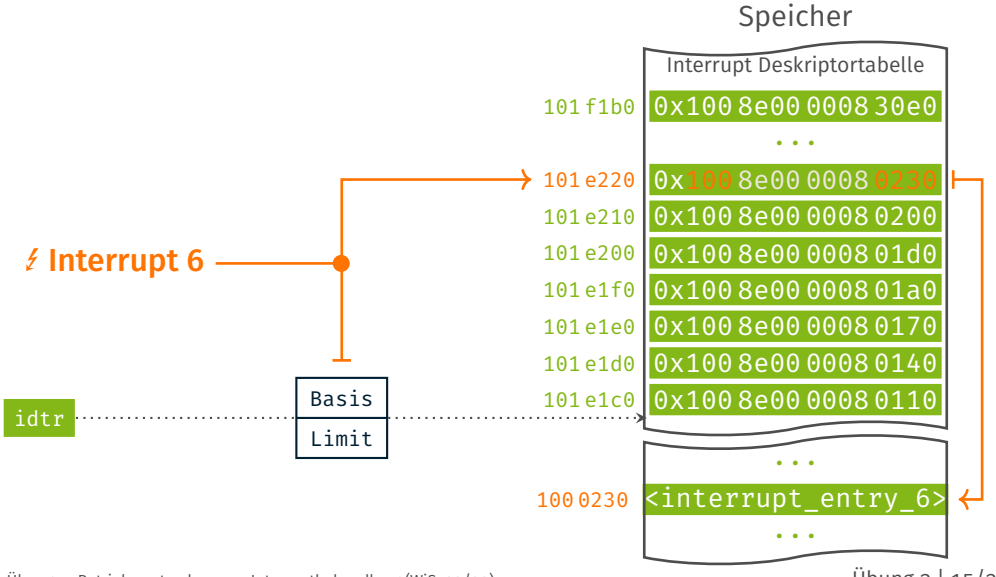
Interrupt Deskriptor Tabelle (IDT)



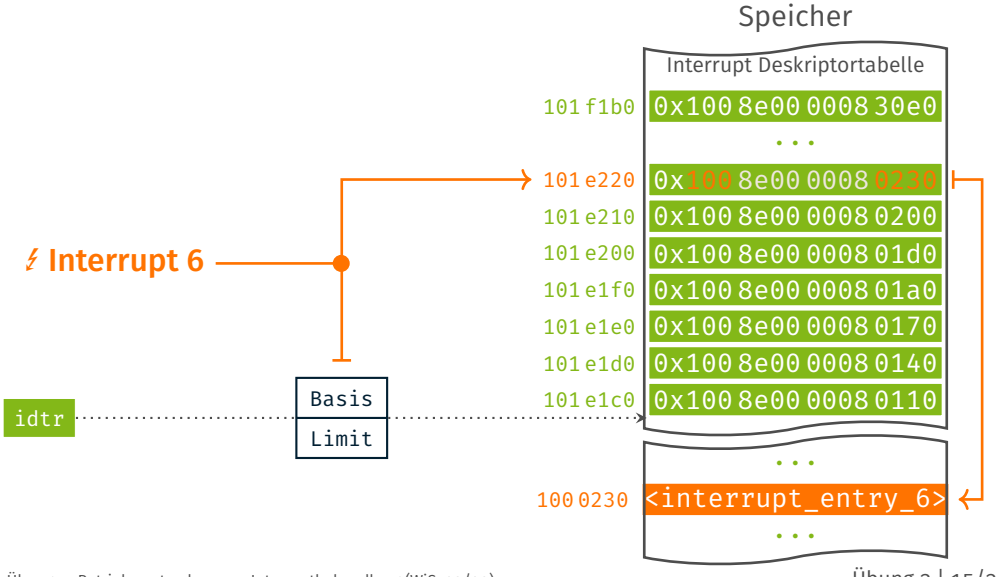
Interrupt Deskriptor Tabelle (IDT)



Interrupt Deskriptor Tabelle (IDT)



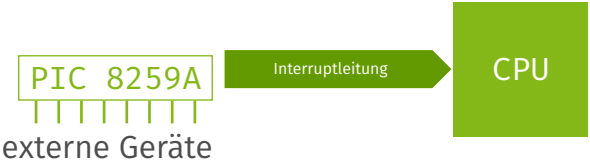
Interrupt Deskriptor Tabelle (IDT)



Externe Interrupts

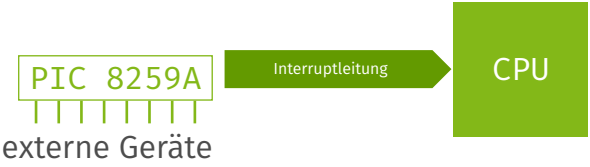
Unterbrechungen durch externe Geräte bei x86-CPUs

Unterbrechungen durch externe Geräte bei x86-CPUs



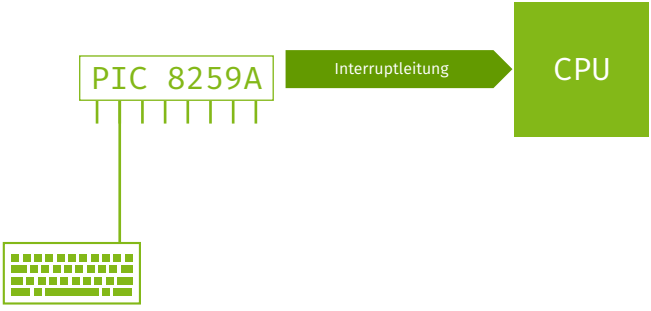
- Anschluss von mehreren Geräten durch Programmable Interrupt Controller

Unterbrechungen durch externe Geräte bei x86-CPUs



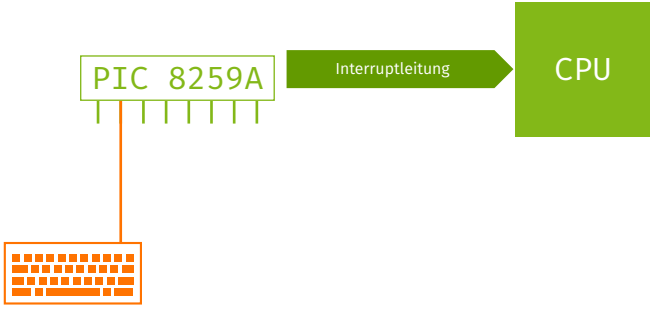
- Anschluss von mehreren Geräten durch Programmable Interrupt Controller
  - feste Prioritätenreihenfolge
  - Interruptvektornummer bedingt änderbar (Vielfaches von 8)
  - Konfiguration über I/O-Ports

Unterbrechungen durch externe Geräte bei x86-CPUs



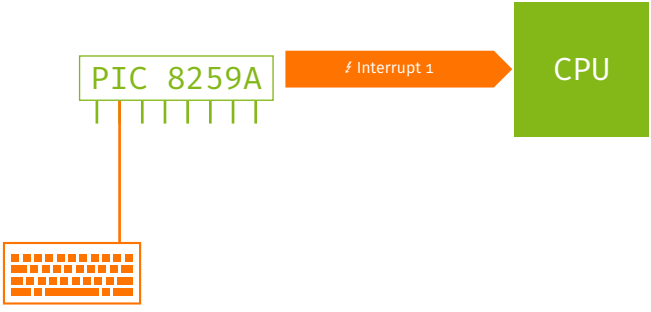
- Anschluss von mehreren Geräten durch Programmable Interrupt Controller
  - feste Prioritätenreihenfolge
  - Interruptvektornummer bedingt änderbar (Vielfaches von 8)
  - Konfiguration über I/O-Ports

Unterbrechungen durch externe Geräte bei x86-CPUs



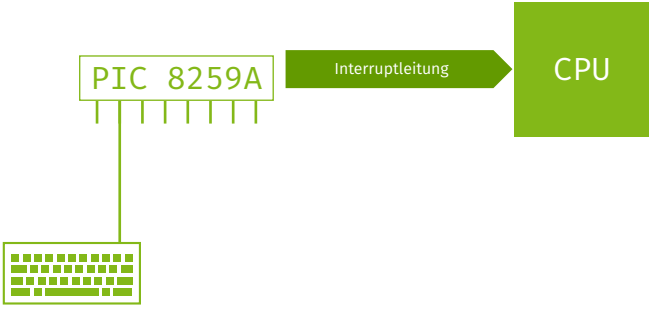
- Anschluss von mehreren Geräten durch Programmable Interrupt Controller
  - feste Prioritätenreihenfolge
  - Interruptvektornummer bedingt änderbar (Vielfaches von 8)
  - Konfiguration über I/O-Ports

Unterbrechungen durch externe Geräte bei x86-CPUs



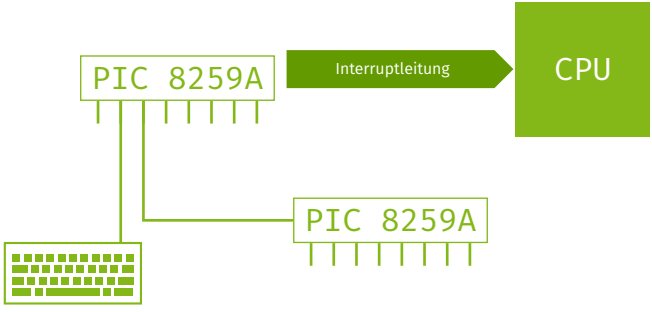
- Anschluss von mehreren Geräten durch Programmable Interrupt Controller
  - feste Prioritätenreihenfolge
  - Interruptvektornummer bedingt änderbar (Vielfaches von 8)
  - Konfiguration über I/O-Ports

Unterbrechungen durch externe Geräte bei x86-CPUs



- Anschluss von mehreren Geräten durch Programmable Interrupt Controller
  - feste Prioritätenreihenfolge
  - Interruptvektornummer bedingt änderbar (Vielfaches von 8)
  - Konfiguration über I/O-Ports

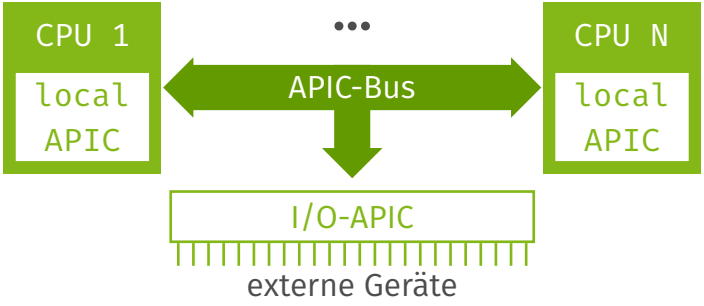
Unterbrechungen durch externe Geräte bei x86-CPUs



- Anschluss von mehreren Geräten durch Programmable Interrupt Controller
  - feste Prioritätenreihenfolge
  - Interruptvektornummer bedingt änderbar (Vielfaches von 8)
  - Konfiguration über I/O-Ports
- Erweiterung von 8 auf 15 Geräte durch Kaskadierung

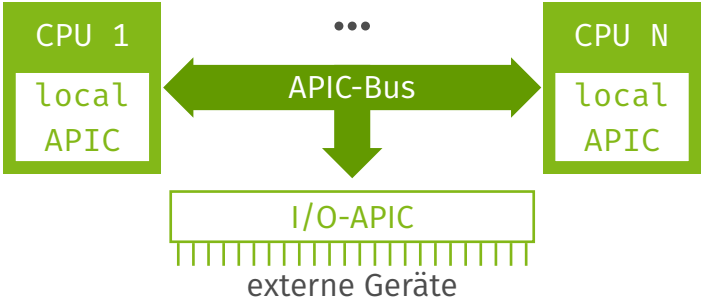
Externe Interrupts mit dem APIC

Aufbau der APIC-Architektur



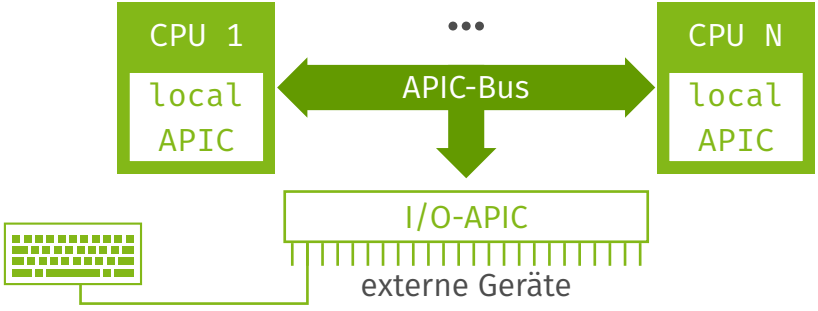
Aufteilung in lokalen APIC und I/O APIC

Aufbau der APIC-Architektur



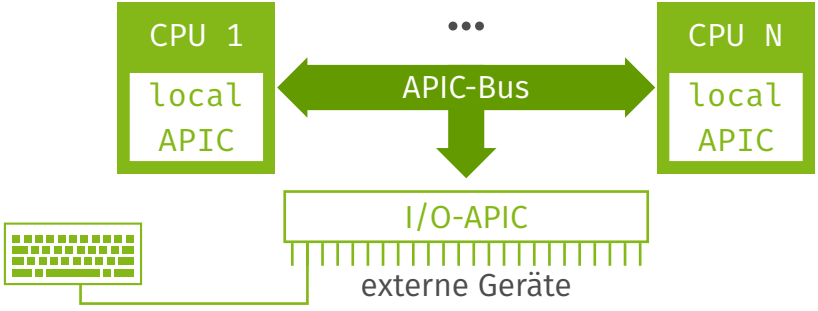
I/O-APIC dient zum Anschluss der Geräte

Aufbau der APIC-Architektur



I/O-APIC dient zum Anschluss der Geräte

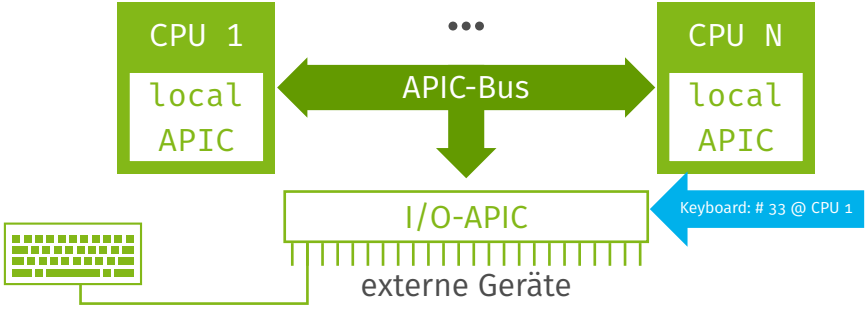
Aufbau der APIC-Architektur



I/O-APIC dient zum Anschluss der Geräte

- Zuweisung von beliebigen Vektornummern
- Aktivieren und Deaktivieren von einzelnen Interruptquellen
- Zuweisung von Zielprozessoren für einzelnen Interrupts in MP-Systemen

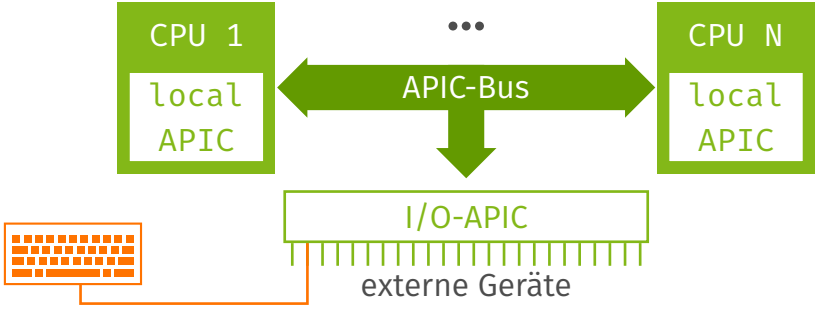
Aufbau der APIC-Architektur



I/O-APIC dient zum Anschluss der Geräte

- Zuweisung von beliebigen Vektornummern
- Aktivieren und Deaktivieren von einzelnen Interruptquellen
- Zuweisung von Zielprozessoren für einzelnen Interrupts in MP-Systemen

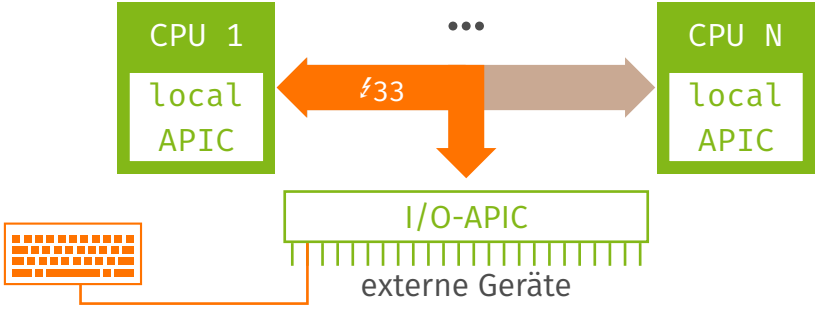
Aufbau der APIC-Architektur



I/O-APIC dient zum Anschluss der Geräte

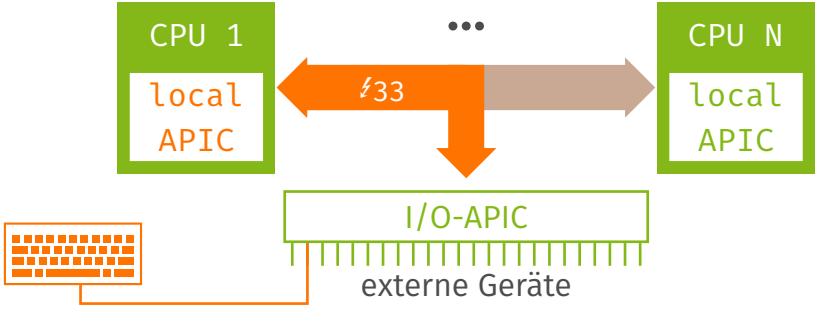
- Zuweisung von beliebigen Vektornummern
- Aktivieren und Deaktivieren von einzelnen Interruptquellen
- Zuweisung von Zielprozessoren für einzelnen Interrupts in MP-Systemen

Aufbau der APIC-Architektur



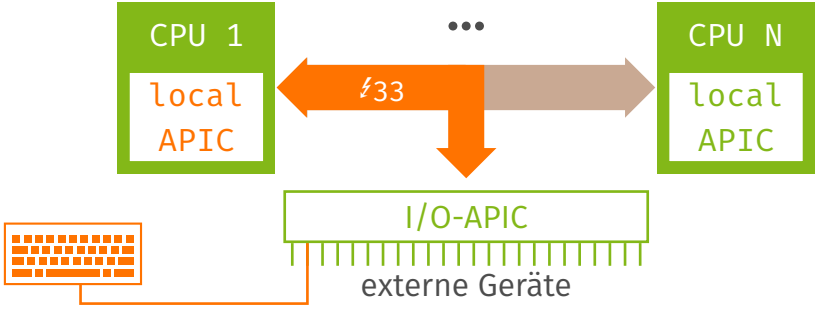
Interrupts werden zu Nachrichten auf dem APIC-Bus

Aufbau der APIC-Architektur



Empfang durch Local APIC

Aufbau der APIC-Architektur



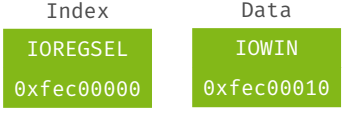
Empfang durch Local APIC

- Verbindet eine CPU mit dem APIC-Bus
- Liest Nachrichten vom APIC-Bus und unterbricht die CPU
- Muss Interrupts explizit quittieren (ACK)

Programmierung des Intel I/O-APIC

Zugriff auf die internen Register über memory-mapped I/O

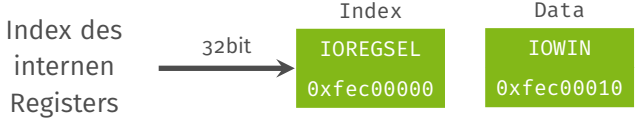
- Jedoch keine direkte Abbildung von internen Registern auf Speicheradressen
- *Umweg* über ein Index- und Datenregister



Programmierung des Intel I/O-APIC

Zugriff auf die internen Register über memory-mapped I/O

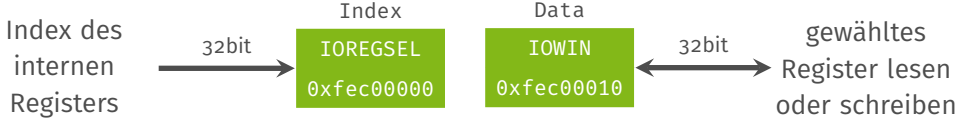
- Jedoch keine direkte Abbildung von internen Registern auf Speicheradressen
- *Umweg* über ein Index- und Datenregister



Programmierung des Intel I/O-APIC

Zugriff auf die internen Register über memory-mapped I/O

- Jedoch keine direkte Abbildung von internen Registern auf Speicheradressen
- *Umweg* über ein Index- und Datenregister

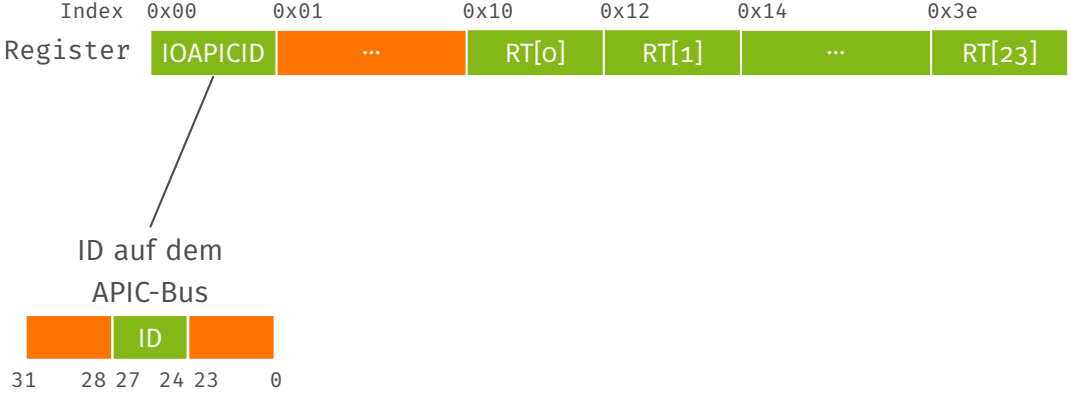


Programmierung des Intel I/O-APIC (2)

Interne Register des I/O-APICs

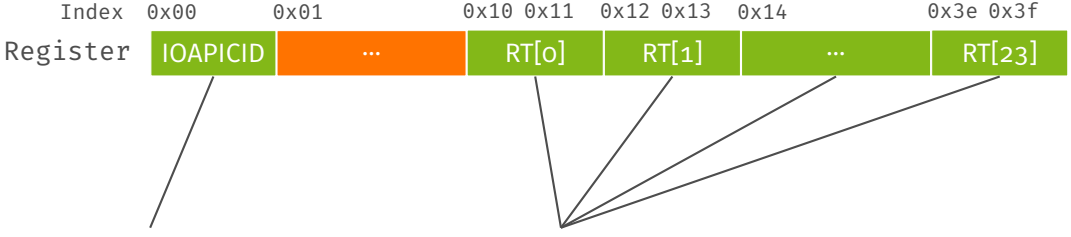
Programmierung des Intel I/O-APIC (2)

Interne Register des I/O-APICs



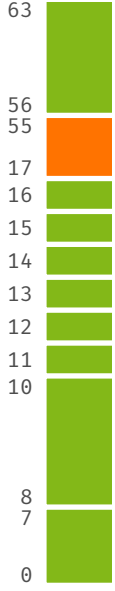
Programmierung des Intel I/O-APIC (2)

Interne Register des I/O-APICs



- Ein Eintrag für jede Interruptquelle
- Konfiguration dadurch pro Interruptquelle
- Zwei interne Register pro Eintrag (64bit)

Aufbau eines Redirection Table Eintrags



Destination Field: Zieladresse des IRQs

bei `Dest. Mode == Physical` APIC ID der Ziel-CPU

bei `Dest. Mode == Logical` Gruppe von Ziel-CPUs

reserviert

Interrupt-Mask: Interrupt aktiv (`0`) oder inaktiv (`1`)

Trigger Mode: Flanken-(`0`) oder Pegelsteuerung (`1`)

Remote IRR: Art der erhaltenen Bestätigung

Interrupt Polarity: Active High (`0`) bzw. Active Low (`1`)

Delivery Status: Interrupt Nachricht noch unterwegs?

Destination Mode: Physical (`0`) oder Logical (`1`) Mode

Delivery Mode: Modus der Nachrichtenzustellung, z.B.

`0` **Fixed** – Signal allen Zielprozessoren zustellen

`1` **Lowest Priority** – CPU mit niedrigster Priorität

Interrupt Vektor: Nummer in der Vektortabelle (32 – 255)

Umsetzung in StuBS

Programmierung des APIC Systems

Programmierung des APIC Systems

Wo ist welches Gerät angeschlossen?

Programmierung des APIC Systems

Wo ist welches Gerät angeschlossen?

- Das kann evtl. unterschiedlich sein von Rechner zu Rechner!

Programmierung des APIC Systems

Wo ist welches Gerät angeschlossen?

- Das kann evtl. unterschiedlich sein von Rechner zu Rechner!
- Steht in der Systemkonfiguration, heutzutage i.d.R. **ACPI** (Advanced Configuration and Power Interface)

Programmierung des APIC Systems

Wo ist welches Gerät angeschlossen?

- Das kann evtl. unterschiedlich sein von Rechner zu Rechner!
- Steht in der Systemkonfiguration, heutzutage i.d.R. **ACPI** (Advanced Configuration and Power Interface)
- Bei uns stellt `APIC` die relevanten Teile dieser Informationen bereit

Programmierung des APIC Systems

Wo ist welches Gerät angeschlossen?

- Das kann evtl. unterschiedlich sein von Rechner zu Rechner!
- Steht in der Systemkonfiguration, heutzutage i.d.R. **ACPI** (Advanced Configuration and Power Interface)
- Bei uns stellt `APIC` die relevanten Teile dieser Informationen bereit

  `APIC::getIOAPICSlot` liefert für jedes Gerät den Index in die Redirection Table (siehe `enum Device` in `machine/apic.h`)

Programmierung des APIC Systems

Wo ist welches Gerät angeschlossen?

- Das kann evtl. unterschiedlich sein von Rechner zu Rechner!
- Steht in der Systemkonfiguration, heutzutage i.d.R. **ACPI** (Advanced Configuration and Power Interface)
- Bei uns stellt `APIC` die relevanten Teile dieser Informationen bereit

  `APIC::getIOAPICSlot` liefert für jedes Gerät den Index in die Redirection Table (siehe `enum Device` in `machine/apic.h`)

  `APIC::getIOAPICID` liefert die ID des I/O-APICs

Programmierung des APIC Systems

Adressierung der APIC Nachrichten in StuBS

- Zusammenspiel mehrerer Faktoren
  - `Destination Mode`, `Destination Field` und `Delivery Mode` im I/O-APIC
  - Prozessor Priorität in den Local APICs der einzelnen CPUs

Programmierung des APIC Systems

Adressierung der APIC Nachrichten in StuBS

- Zusammenspiel mehrerer Faktoren
  - `Destination Mode`, `Destination Field` und `Delivery Mode` im I/O-APIC
  - Prozessor Priorität in den Local APICs der einzelnen CPUs
- **Ziel:** Gleichverteilung der Interrupts auf alle CPUs

Programmierung des APIC Systems

Adressierung der APIC Nachrichten in StuBS

- Zusammenspiel mehrerer Faktoren
  - `Destination Mode`, `Destination Field` und `Delivery Mode` im I/O-APIC
  - Prozessor Priorität in den Local APICs der einzelnen CPUs
- **Ziel:** Gleichverteilung der Interrupts auf alle CPUs
  - Priorität der Prozessoren im Local APIC fest auf `0` einstellen

Programmierung des APIC Systems

Adressierung der APIC Nachrichten in StuBS

- Zusammenspiel mehrerer Faktoren
  - `Destination Mode`, `Destination Field` und `Delivery Mode` im I/O-APIC
  - Prozessor Priorität in den Local APICs der einzelnen CPUs
- **Ziel:** Gleichverteilung der Interrupts auf alle CPUs
  - Priorität der Prozessoren im Local APIC fest auf `0` einstellen
  - Im I/O-APIC `Lowest Priority` als Delivery Mode verwenden

Programmierung des APIC Systems

Adressierung der APIC Nachrichten in StuBS

- Zusammenspiel mehrerer Faktoren
  - `Destination Mode`, `Destination Field` und `Delivery Mode` im I/O-APIC
  - Prozessor Priorität in den Local APICs der einzelnen CPUs
- **Ziel:** Gleichverteilung der Interrupts auf alle CPUs
  - Priorität der Prozessoren im Local APIC fest auf `0` einstellen
  - Im I/O-APIC `Lowest Priority` als Delivery Mode verwenden
  - Verwendung des `Logical Destination Mode`; bis zu 8 CPUs adressierbar

Programmierung des APIC Systems

Adressierung der APIC Nachrichten in StuBS

- Zusammenspiel mehrerer Faktoren
  - `Destination Mode`, `Destination Field` und `Delivery Mode` im I/O-APIC
  - Prozessor Priorität in den Local APICs der einzelnen CPUs
- **Ziel:** Gleichverteilung der Interrupts auf alle CPUs
  - Priorität der Prozessoren im Local APIC fest auf `0` einstellen
  - Im I/O-APIC `Lowest Priority` als Delivery Mode verwenden
  - Verwendung des `Logical Destination Mode`; bis zu 8 CPUs adressierbar
  - `Destination Field`: Bitmaske mit gesetztem Bit pro aktivierter CPU

Redirection Table Einträge in StuBS

Destination Field: Zieladresse des IRQs

bei `Dest. Mode == Physical` APIC ID der Ziel-CPU

bei `Dest. Mode == Logical` Gruppe von Ziel-CPUs

reserviert

Interrupt-Mask: Interrupt aktiv (`0`) oder inaktiv (`1`)

Trigger Mode: Flanken-(`0`) oder Pegelsteuerung (`1`)

Remote IRR: Art der erhaltenen Bestätigung

Interrupt Polarity: Active High (`0`) bzw. Active Low (`1`)

Delivery Status: Interrupt Nachricht noch unterwegs?

Destination Mode: Physical (`0`) oder Logical (`1`) Mode

Delivery Mode: Modus der Nachrichtenzustellung, z.B.

`0` **Fixed** – Signal allen Zielprozessoren zustellen

`1` **Lowest Priority** – CPU mit niedrigster Priorität

Interrupt Vektor: Nummer in der Vektortabelle (32 – 255)

Zusammenfassendes Beispiel: Keyboard Interrupt in StuBS

Vorbereitung

Vorbereitung

- **I/O APIC** initialisieren

Vorbereitung

- **I/O APIC** initialisieren
  - **I/O APIC ID** setzen

Vorbereitung

- **I/O APIC** initialisieren
  - **I/O APIC ID** setzen
  - Einträge in **Redirection Table** initialisieren (deaktivieren)

Vorbereitung

- **I/O APIC** initialisieren
  - **I/O APIC ID** setzen
  - Einträge in **Redirection Table** initialisieren (deaktivieren)
- **Keyboard** konfigurieren

Vorbereitung

- **I/O APIC** initialisieren
  - **I/O APIC ID** setzen
  - Einträge in **Redirection Table** initialisieren (deaktivieren)
- **Keyboard** konfigurieren
  - Anmelden bei der **Plugbox**

Vorbereitung

- **I/O APIC** initialisieren
  - **I/O APIC ID** setzen
  - Einträge in **Redirection Table** initialisieren (deaktivieren)
- **Keyboard** konfigurieren
  - Anmelden bei der **Plugbox**
  - Tastaturslot herausfinden und den entsprechenden Eintrag in der **Redirection Table** konfigurieren und aktivieren
  - Tastaturbuffer leeren

Vorbereitung

- **I/O APIC** initialisieren
  - **I/O APIC ID** setzen
  - Einträge in **Redirection Table** initialisieren (deaktivieren)
- **Keyboard** konfigurieren
  - Anmelden bei der **Plugbox**
  - Tastaturslot herausfinden und den entsprechenden Eintrag in der **Redirection Table** konfigurieren und aktivieren
  - Tastaturbuffer leeren
- **Interruptbehandlung** erstellen
  - Einsprungsroutinen `interrupt_entry` mit Aufruf zu `interrupt_handler` schreiben [wird in der Vorgabe bereits erledigt]

Vorbereitung

- **I/O APIC** initialisieren
  - **I/O APIC ID** setzen
  - Einträge in **Redirection Table** initialisieren (deaktivieren)
- **Keyboard** konfigurieren
  - Anmelden bei der **Plugbox**
  - Tastaturslot herausfinden und den entsprechenden Eintrag in der **Redirection Table** konfigurieren und aktivieren
  - Tastaturbuffer leeren
- **Interruptbehandlung** erstellen
  - Einsprungsroutinen `interrupt_entry` mit Aufruf zu `interrupt_handler` schreiben [wird in der Vorgabe bereits erledigt]
  - Eintragen in die **Interrupt Deskriptor Tabelle** (**IDT**) und diese in das Register `idtr` laden [ebenfalls erledigt]

Vorbereitung

- **I/O APIC** initialisieren
  - **I/O APIC ID** setzen
  - Einträge in **Redirection Table** initialisieren (deaktivieren)
- **Keyboard** konfigurieren
  - Anmelden bei der **Plugbox**
  - Tastaturslot herausfinden und den entsprechenden Eintrag in der **Redirection Table** konfigurieren und aktivieren
  - Tastaturbuffer leeren
- **Interruptbehandlung** erstellen
  - Einsprungsroutinen `interrupt_entry` mit Aufruf zu `interrupt_handler` schreiben [wird in der Vorgabe bereits erledigt]
  - Eintragen in die **Interrupt Deskriptor Tabelle** (**IDT**) und diese in das Register `idtr` laden [ebenfalls erledigt]
  - Ereignisbehandlung in `interrupt_handler` mittels **Plugbox**

Vorbereitung

- **I/O APIC** initialisieren
  - **I/O APIC ID** setzen
  - Einträge in **Redirection Table** initialisieren (deaktivieren)
- **Keyboard** konfigurieren
  - Anmelden bei der **Plugbox**
  - Tastaturslot herausfinden und den entsprechenden Eintrag in der **Redirection Table** konfigurieren und aktivieren
  - Tastaturbuffer leeren
- **Interruptbehandlung** erstellen
  - Einsprungsroutinen `interrupt_entry` mit Aufruf zu `interrupt_handler` schreiben [wird in der Vorgabe bereits erledigt]
  - Eintragen in die **Interrupt Deskriptor Tabelle** (**IDT**) und diese in das Register `idtr` laden [ebenfalls erledigt]
  - Ereignisbehandlung in `interrupt_handler` mittels **Plugbox**
- Interrupts mit `Core::Interrupt::enable()` aktivieren

Ablauf

Ablauf

1. **Tastendruck** – Tastaturprozessor (in der Tastatur) meldet dies seriell an den **PS/2-Controller**

Ablauf

1. **Tastendruck** – Tastaturprozessor (in der Tastatur) meldet dies seriell an den **PS/2-Controller**
2. **PS/2-Controller** aktiviert Interruptleitung zu **I/O APIC**

Ablauf

1. **Tastendruck** – Tastaturprozessor (in der Tastatur) meldet dies seriell an den **PS/2-Controller**
2. **PS/2-Controller** aktiviert Interruptleitung zu **I/O APIC**
   2.1 Anhand der **Redirection Table** wird Aktion gewählt

Ablauf

1. **Tastendruck** – Tastaturprozessor (in der Tastatur) meldet dies seriell an den **PS/2-Controller**
2. **PS/2-Controller** aktiviert Interruptleitung zu **I/O APIC**
   2.1 Anhand der **Redirection Table** wird Aktion gewählt
   2.2 Nachricht auf **APIC-Bus** mit Interruptnr. 33 und Ziel-CPU

Ablauf

1. **Tastendruck** – Tastaturprozessor (in der Tastatur) meldet dies seriell an den **PS/2-Controller**
2. **PS/2-Controller** aktiviert Interruptleitung zu **I/O APIC**
   2.1 Anhand der **Redirection Table** wird Aktion gewählt
   2.2 Nachricht auf **APIC-Bus** mit Interruptnr. 33 und Ziel-CPU
3. entsprechender **LAPIC** empfängt Nachricht vom **APIC-Bus**

Ablauf

1. **Tastendruck** – Tastaturprozessor (in der Tastatur) meldet dies seriell an den **PS/2-Controller**
2. **PS/2-Controller** aktiviert Interruptleitung zu **I/O APIC**
   2.1 Anhand der **Redirection Table** wird Aktion gewählt
   2.2 Nachricht auf **APIC-Bus** mit Interruptnr. 33 und Ziel-CPU
3. entsprechender **LAPIC** empfängt Nachricht vom **APIC-Bus**
4. **CPU** führt Unterbrechungsbehandlung aus

Ablauf

1. **Tastendruck** – Tastaturprozessor (in der Tastatur) meldet dies seriell an den **PS/2-Controller**
2. **PS/2-Controller** aktiviert Interruptleitung zu **I/O APIC**
   2.1 Anhand der **Redirection Table** wird Aktion gewählt
   2.2 Nachricht auf **APIC-Bus** mit Interruptnr. 33 und Ziel-CPU
3. entsprechender **LAPIC** empfängt Nachricht vom **APIC-Bus**
4. **CPU** führt Unterbrechungsbehandlung aus
   4.1 Mittels Register `idtr` wird der entsprechende Eintrag in der **Interrupt Deskriptor Tabelle** ausgewählt und in die Einsprungsroutine gesprungen

Ablauf

1. **Tastendruck** – Tastaturprozessor (in der Tastatur) meldet dies seriell an den **PS/2-Controller**
2. **PS/2-Controller** aktiviert Interruptleitung zu **I/O APIC**
   2.1 Anhand der **Redirection Table** wird Aktion gewählt
   2.2 Nachricht auf **APIC-Bus** mit Interruptnr. `33` und Ziel-CPU
3. entsprechender **LAPIC** empfängt Nachricht vom **APIC-Bus**
4. **CPU** führt Unterbrechungsbehandlung aus
   4.1 Mittels Register `idtr` wird der entsprechende Eintrag in der **Interrupt Deskriptor Tabelle** ausgewählt und in die Einsprungsroutine gesprungen
   4.2 Einsprungsroutine `interrupt_entry_33` sichert Register und ruft `interrupt_handler` mit Parameter `vector = 33` auf

Ablauf

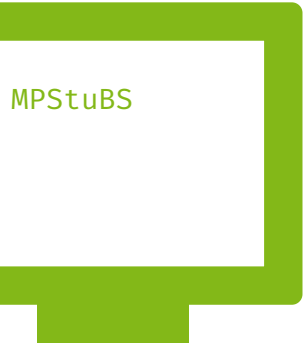
1. **Tastendruck** – Tastaturprozessor (in der Tastatur) meldet dies seriell an den **PS/2-Controller**
2. **PS/2-Controller** aktiviert Interruptleitung zu **I/O APIC**
   - 2.1 Anhand der **Redirection Table** wird Aktion gewählt
   - 2.2 Nachricht auf **APIC-Bus** mit Interruptnr. `33` und Ziel-CPU
3. entsprechender **LAPIC** empfängt Nachricht vom **APIC-Bus**
4. **CPU** führt Unterbrechungsbehandlung aus
   - 4.1 Mittels Register `idtr` wird der entsprechende Eintrag in der **Interrupt Deskriptor Tabelle** ausgewählt und in die Einsprungsroutine gesprungen
   - 4.2 Einsprungsroutine `interrupt_entry_33` sichert Register und ruft `interrupt_handler` mit Parameter `vector = 33` auf
   - 4.3 `interrupt_handler` behandelt mittels **Plugbox** den Interrupt

Ablauf

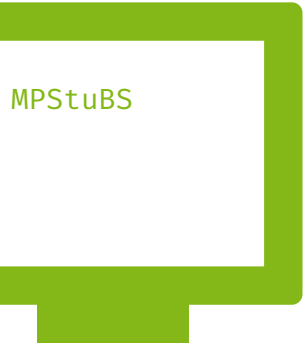
1. **Tastendruck** – Tastaturprozessor (in der Tastatur) meldet dies seriell an den **PS/2-Controller**
2. **PS/2-Controller** aktiviert Interruptleitung zu **I/O APIC**
   2.1 Anhand der **Redirection Table** wird Aktion gewählt
   2.2 Nachricht auf **APIC-Bus** mit Interruptnr. `33` und Ziel-CPU
3. entsprechender **LAPIC** empfängt Nachricht vom **APIC-Bus**
4. **CPU** führt Unterbrechungsbehandlung aus
   4.1 Mittels Register `idtr` wird der entsprechende Eintrag in der **Interrupt Deskriptor Tabelle** ausgewählt und in die Einsprungsroutine gesprungen
   4.2 Einsprungsroutine `interrupt_entry_33` sichert Register und ruft `interrupt_handler` mit Parameter `vector = 33` auf
   4.3 `interrupt_handler` behandelt mittels **Plugbox** den Interrupt
5. **LAPIC** quittiert die Behandlung

Remotedebugging mit GDB

Remote GDB



Remote GDB



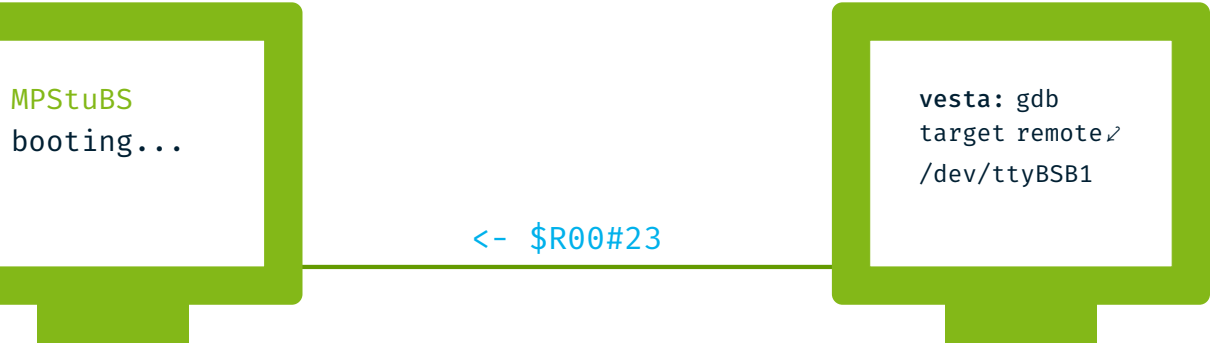
Remote GDB

Remote GDB

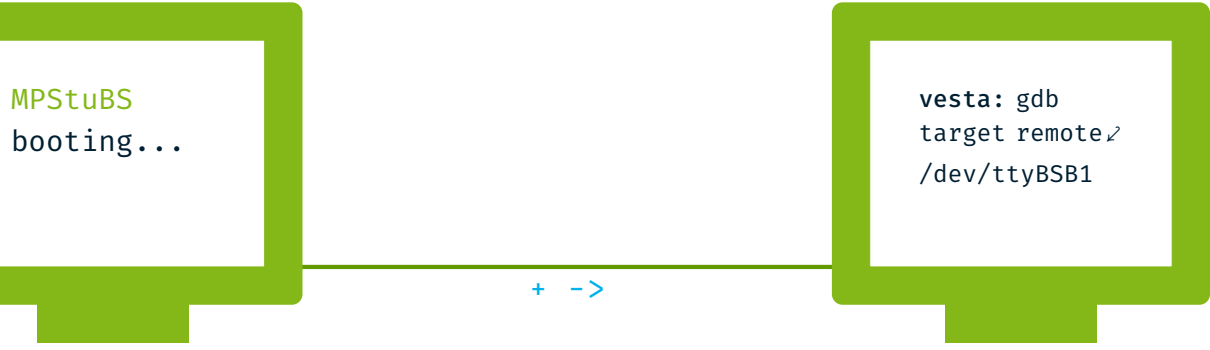
Remote GDB

Remote GDB

Remote GDB



Remote GDB



Remote GDB

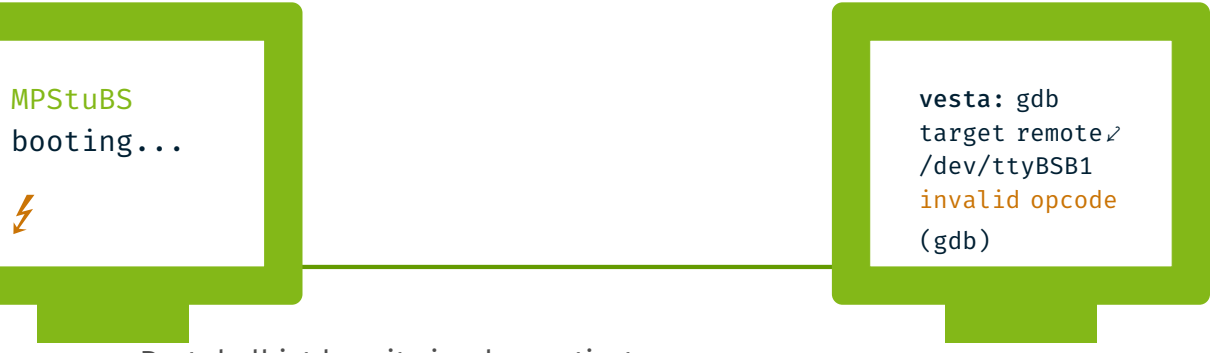
Remote GDB

Remote GDB

Remote GDB


MPStuBS
booting...
vesta: gdb
target remote
/dev/ttyBSB1
invalid opcode
(gdb)

Remote GDB

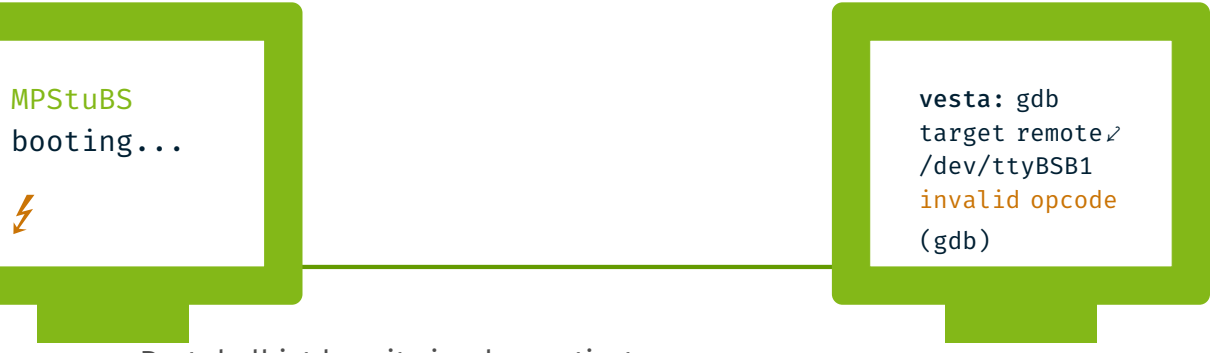


- Protokoll ist bereits implementiert
- verwendet eigene Unterbrechungsbehandlung für Traps

→ modifiziert die IDT

- nur die serielle Schnittstelle (von Aufgabe 1) wird benötigt

Remote GDB



- Protokoll ist bereits implementiert
- verwendet eigene Unterbrechungsbehandlung für Traps

→ modifiziert die IDT

- nur die serielle Schnittstelle (von Aufgabe 1) wird benötigt
- aber ist freiwillig

Aufgabe 2

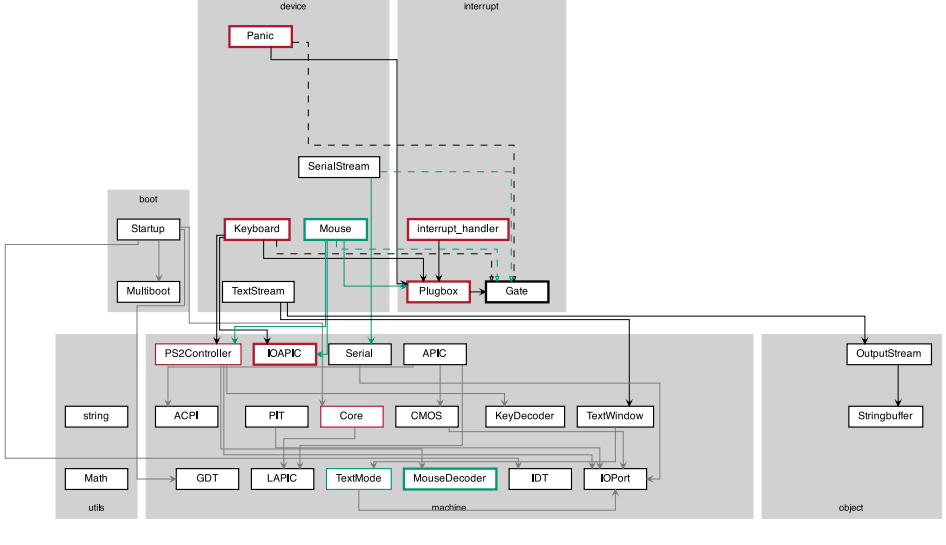
Aufgabe 2

Lernziele

- Behandlung asynchroner Ereignisse
- Problematik und Schutz kritischer Abschnitte

Aufgaben

- Konfiguration externer Geräte über I/O APIC
- Treiber für **Tastatur** und (*optional*) **Maus**
- **MPStuBS**: Wechselseitiger Ausschluss (**Ticket-**/**Spinlock**)
- *Optional:* **GDB Stub**


device
interrupt
Panic
SerialStream
boot
Startup
Keyboard
Mouse
interrupt_handler
Multiboot
TextStream
Plugbox
Gate
PS2Controller
IOAPIC
Serial
APIC
OutputStream
string
ACPI
PIT
Core
CMOS
KeyDecoder
TextWindow
Stringbuffer
Math
GDT
LAPIC
TextMode
MouseDecoder
IDT
IOPort
utils
machine
object

Vergnügen mit KVM

- **Problem:** Tastatur-Interrupts in KVM nur auf Core 1

Vergnügen mit KVM

KVM nutzt ggf. Vector Hashing

- **Problem:** Tastatur-Interrupts in KVM nur auf Core `1`
- **Lösung:** Datei `/etc/modprobe.d/kvm_options.conf` editieren, Eintrag **`options kvm vector_hashing=N`** hinzufügen und System neu starten.

(weitere Details siehe FAQ auf der Webseite)

Fragen?

Abgabe der 2. Aufgabe bis Mittwoch, 09. November
Übernächste Woche ist wieder ein Seminar (08. November)