Operating System Calls

Certain operations require specialized knowledge and protection:

- **specific knowledge of I/O device registers and the sequence of operations needed to use them**
- **I/O resources shared among multiple users/programs; a mistake could affect lots of other users!**

Not every programmer knows (or wants to know) this level of detail

Provide *service routines* or *system calls* (part of operating system) to safely and conveniently perform low-level, privileged operations

System Call

1. User program invokes system call.

2. Operating system code performs operation.

3. Returns control to user program.

In LC-3, this is done through the *TRAP mechanism*

OTHER MOTIVATIONS FOR TRAPS

LC-3 TRAP Mechanism

1. A set of service routines.

- **part of operating system -- routines start at arbitrary addresses**
  (convention is that system code is below x3000)
- **up to 256 routines**

2. Table of starting addresses.

- **stored at x0000 through x00FF in memory**
- **called System Control Block in some architectures**

3. TRAP instruction.

- **used by program to transfer control to operating system**
- **8-bit trap vector names one of the 256 service routines**

4. A linkage back to the user program.

- **want execution to resume immediately after the TRAP instruction**

TRAP Instruction

	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
TRAP	1	1	1	1	0	0	0	0	trapvect8							

Trap vector

- **identifies which system call to invoke**
- **8-bit index into table of service routine addresses**
  - ➢ **in LC-3, this table is stored in memory at 0x0000 – 0x00FF**
  - ➢ **8-bit trap vector is zero-extended into 16-bit memory address**

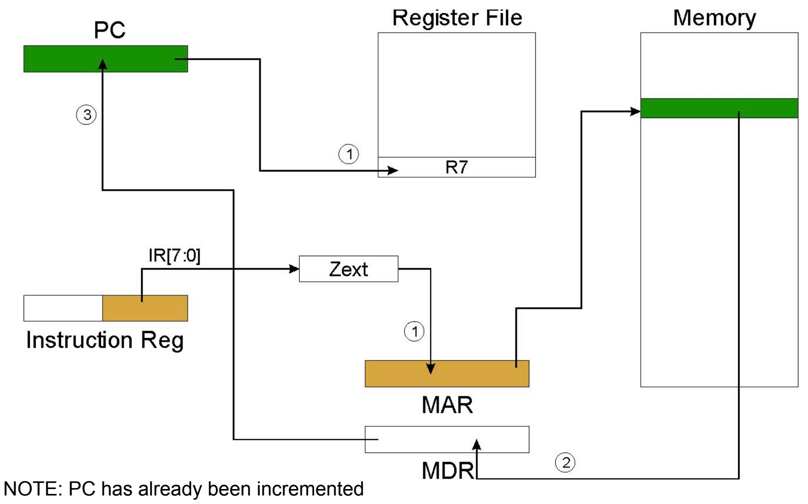
Where to go

- **lookup starting address from table; place in PC**

How to get back

- **save address of next instruction (current PC) in R7**

TRAP



NOTE: PC has already been incremented during instruction fetch stage.

RET (JMP R7)

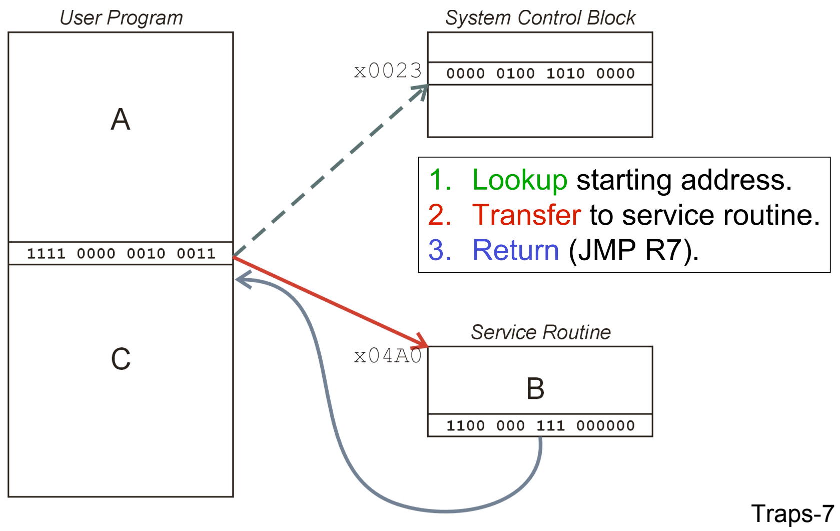
How do we transfer control back to instruction following the TRAP?

We saved old PC in R7.

- **JMP R7 gets us back to the user program at the right spot.**
- **LC-3 assembly language lets us use RET (return) in place of "JMP R7".**

Must make sure that service routine does not change R7, or we won't know where to return.

TRAP Mechanism Operation



1. Lookup starting address.
2. Transfer to service routine.
3. Return (JMP R7).

Example: Using the TRAP Instruction

```
          .ORIG x3000
          LD    R2, TERM    ; Load negative ASCII '7'
          LD    R3, ASCII   ; Load ASCII difference
AGAIN           TRAP  x23         ; input character
          ADD   R1, R2, R0        ; Test for terminate
          BRz   EXIT        ; Exit if done
          ADD   R0, R0, R3        ; Change to lowercase
          TRAP  x21         ; Output to monitor...
          BRnzp  AGAIN      ; ... again and again...
TERM      .FILL       xFFC9       ; -'7'
ASCII           .FILL       x0020       ; lowercase bit
EXIT      TRAP  x25         ; halt
          .END
```