Microprocessors with Security
Final Exam, Fall 2014

Name: _____

Note: No Explanations, No Credits!

1. Interrupts **(25 points)**

   a. Cortex-A9 (ARM) **physically** accepts 2 kinds of interrupt inputs. What are those? How are these 2 interrupts different and why? (5 points)

   b. Explain **what** is done by H/W (Cortex-A9) upon an entry to the interrupt handling? (8 points)

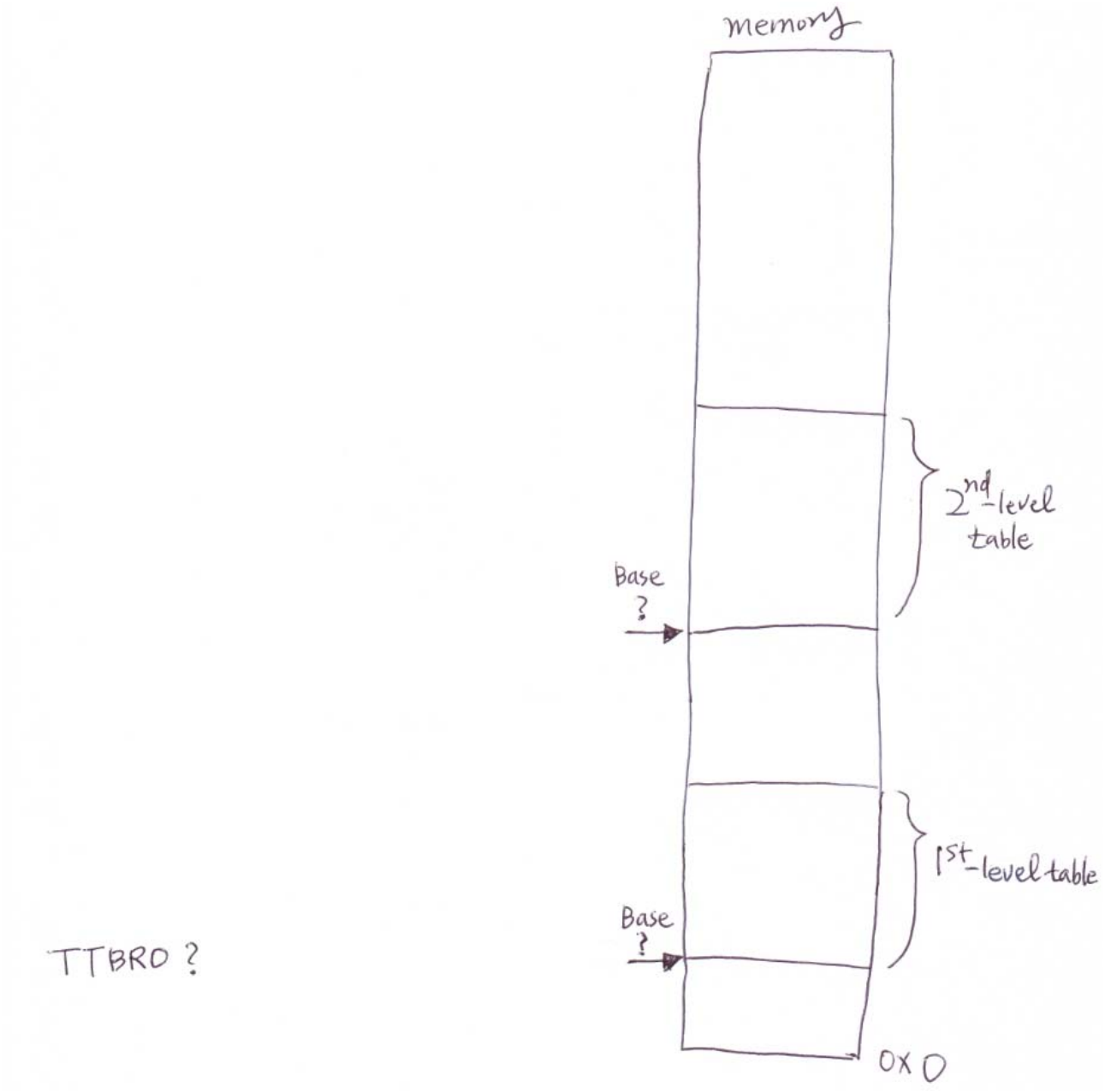
   c. **What instruction** would you use to return from the interrupt and **why**? (5 points)

   d. What is the difference between the following 2 instructions? When would you use the instructions? (7 points)

	Detailed operations	Usage case
`mov pc, lr;`		
`movs pc, lr;`		

2. The SVC (Supervisor Call, previously SWI) instruction is typically used to implement system calls in OS. The diverse system calls in OS are differentiated by the 24-bit immediate field in the SVC instruction. Write an ARM assembly code that extracts the immediate field after jumping to the ISR of SVC. **(10 points)**

3. You want to map a 64KB virtual page from 0x0010_0000 to a physical page from 0x0030_0000. Draw page tables in memory below as detailed as possible. Focus only on memory addresses when you create page tables (ignore the other bit fields). Specify the base locations of page tables in the figure as well. Elaborate why you chose the base locations. What value would you program to the TTBR register? (Refer to the page table entry information in the next page) **(25 points)**



Short-descriptor translation table first-level descriptor formats

Each entry in the first-level table describes the mapping of the associated 1MB MVA range.

Figure B3-4 shows the possible first-level descriptor formats.

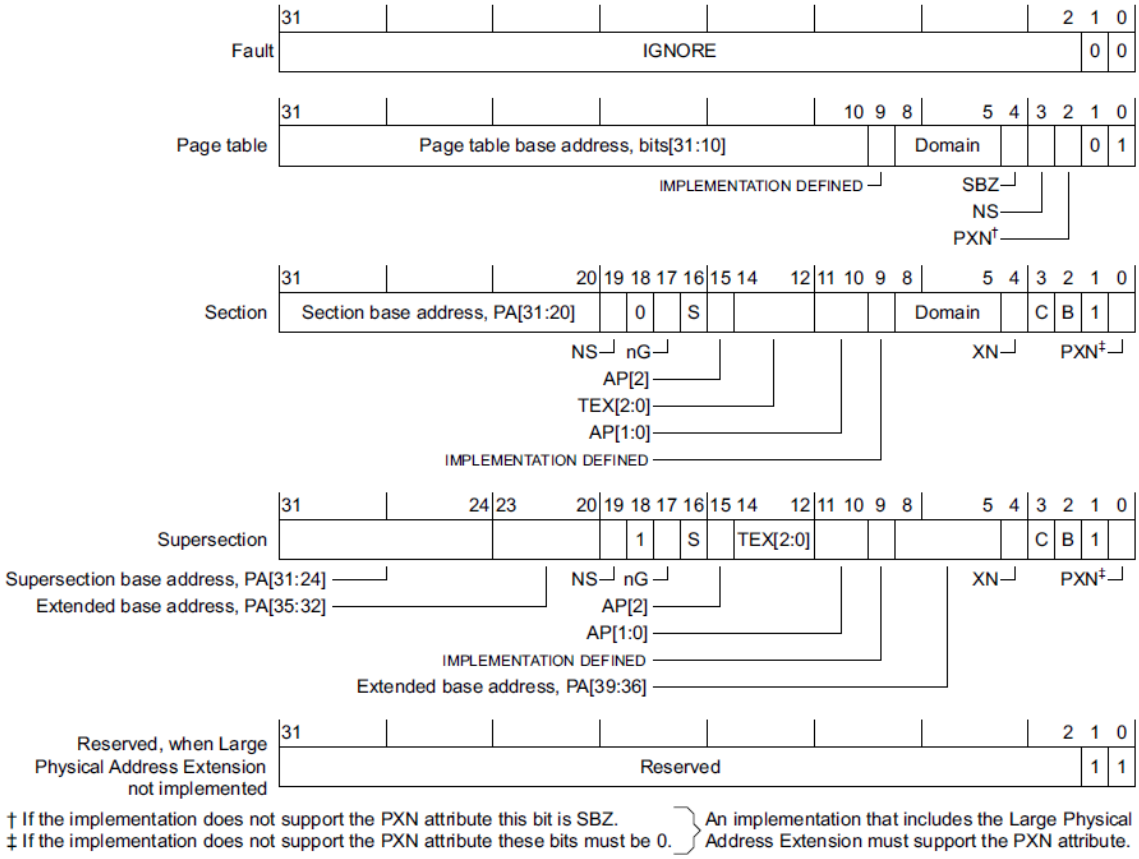


Figure B3-4 Short-descriptor first-level descriptor formats

Short-descriptor translation table second-level descriptor formats

Figure B3-5 shows the possible formats of a second-level descriptor.

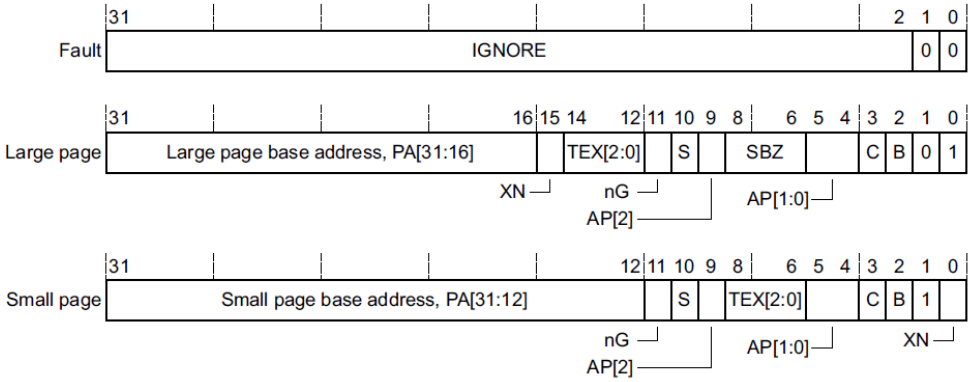
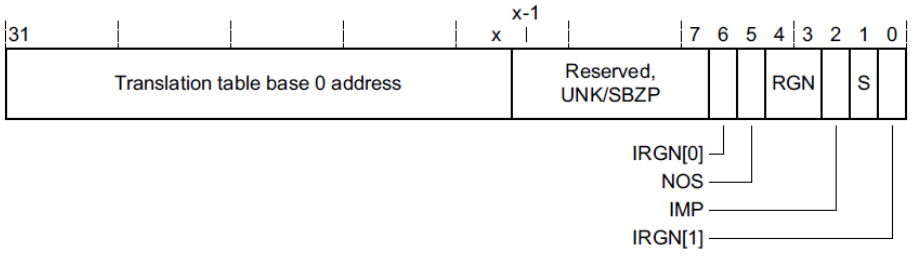


Figure B3-5 Short-descriptor second-level descriptor formats

In an implementation that includes the Multiprocessing Extensions, the 32-bit TTBR0 bit assignments are:



4. TrustZone **(20 points)**

   a. There are 2 ways to enter into the Monitor mode in TrustZone. Explain as detailed as possible. **(5 points)**

   b. Write an assembly code that sets the base addresses of 3 interrupt vector tables to VBARs and MVBAR for secure world, normal world, and monitor mode. Note that the program should include the world-switching code. You are allowed to use pseudo code, in case you don't remember the exact syntax of MCR and MRC instructions **(15 points).**

Secure World Code	Monitor Mode Code	Normal World Code

5. In the worst case, what would happen in L1 caches and L1 TLBs of Cortex-A9 when executing the following 4 instructions? Assume that the cache line size is 8 words (=32 bytes), and the page size is 4KB **(20 points)**

Address: Instructions	**Worst case scenario**	
	L1 Caches (I$ and D$)	**TLB**
0x0FFC: sub r0, r1, r2		
0x1000: mov r10, #0xA004		
0x1004: ldr r2, [r10, #0]		
0x1008: ldm sp!, {r0-r12}		