

Трансляция context\_switch в qemu. Context\_switch переключает mm и register state. Context\_switch вызывается в schedule() (kernel/sched.c).

cpu_arm926_switch_mm			
native		target	
mov	2	mov	14
mcr	4	b	5
mrc	1	str	6
		bl	5
		movt	5
		ldr	5
		and	1
		mvn	1
		movw	10
summary	7		52

switch_to			
native		target	
mov	3	tsteq	24
ldm	1	ldreq	37
str	1	b	6
mcr	1	cmp	24
stmia	1	beq	24
add	2	lsr	24
ldr	3	movt	1
mvn	1	add	49
		mvn	3
		movw	7
		and	26
		mov	77
		str	23
		streq	11
		bl	25
		addmi	2
		ldr	46
	13		409

## Трансляция системных вызовов (do\_fork())

do_fork()			
native		target	
sub	12	tsteq	255
rsbs	3	sub	12
b	33	b	90
cmp	57	ldreq	423
adds	24	lsl	3
lsls	3	cmp	255
pop	3	beq	255
cmn	3	lsr	258
add	39	add	492
movt	9	movw	219
push	3	mvn	9
mvn	12	tsteq	255
movw	15	mov	1062
mov	90	str	546
movs	45	streq	87
str	60	bl	369
subs	3	addmi	33
ldr	141	ldr	693
	<b>555</b>		<b>5316</b>