

Princeton University  
COS 217: Introduction to Programming Systems  
Trace of an ARMv8 Assembly Language Function Call

Registers

SP	4000
X30	???
PC	996

CPU is executing f0

CPU reaches  
`bl g`

Memory

4000	???
-	-
-	-
-	-

Stack

996	bl g
1000	-
-	-
-	-
-	-
2000	g: sub sp,sp,16
2004	str x30,[sp]
2008	-
-	-
2992	ldr x30,[sp]
-	add sp,sp,16
-	ret

Text

Princeton University  
COS 217: Introduction to Programming Systems  
Trace of an ARMv8 Assembly Language Function Call

Registers

SP	4000
X30	1000
PC	2000

Memory

4000	???
-	-
-	-
-	-
-	-

After CPU executes  
**bl g**

Stack

Text

```
f:      -  
       -  
       -  
       -  
996    bl g  
1000    -  
       -  
       -  
       -  
       -  
       -  
       -  
2000  g: sub sp,sp,16  
2004    str x30,[sp]  
2008    -  
       -  
2992    ldr x30,[sp]  
2996    add sp,sp,16  
3000    ret
```

Princeton University  
COS 217: Introduction to Programming Systems  
Trace of an ARMv8 Assembly Language Function Call

Registers

SP	3984
X30	1000
PC	2004

After CPU executes  
`sub sp, sp, 16`

Memory

3984	???
3992	???
4000	???
-	-
-	-
-	-

Stack

Text

```
f:      -  
       -  
       -  
       -  
996    bl g  
1000    -  
       -  
       -  
       -  
       -  
       -  
       -  
       -  
       -  
       -  
       -  
       -  
2000   g: sub sp,sp,16  
2004   str x30,[sp]  
2008   -  
       -  
       -  
       -  
2992   ldr x30,[sp]  
2996   add sp,sp,16  
3000   ret
```

Princeton University  
COS 217: Introduction to Programming Systems  
Trace of an ARMv8 Assembly Language Function Call

Registers

SP	3984
X30	1000
PC	2008

After CPU executes  
`str x30, [sp]`

Memory

3984	1000
3992	???
4000	???

Stack

996	bl g
1000	-
2000	g: sub sp, sp, 16
2004	str x30, [sp]
2008	-
2992	ldr x30, [sp]
2996	add sp, sp, 16
3000	ret

Text

Princeton University  
COS 217: Introduction to Programming Systems  
Trace of an ARMv8 Assembly Language Function Call

Registers

SP	3984
X30	???
PC	2992

After CPU executes  
instructions in the  
body of g()

Memory

3984	1000
3992	???
4000	???

Stack

Text

```
f:      -  
       -  
       -  
       -  
996    bl  g  
1000    -  
       -  
       -  
       -  
2000   g:  sub sp,sp,16  
2004   str x30,[sp]  
2008    -  
       -  
2992   ldr x30,[sp]  
2996   add sp,sp,16  
3000   ret
```

Princeton University  
COS 217: Introduction to Programming Systems  
Trace of an ARMv8 Assembly Language Function Call

Registers

SP	3984
X30	1000
PC	2996

After CPU executes  
`ldr sp, [x30]`

Memory

3984	???
3992	???
4000	???
-	-
-	-

Stack

996	f:	bl g
1000		-
2000	g:	sub sp, sp, 16
2004		str x30, [sp]
2008		-
2992		-
2996		ldr x30, [sp]
3000		add sp, sp, 16
3004		ret

Text

Princeton University  
COS 217: Introduction to Programming Systems  
Trace of an ARMv8 Assembly Language Function Call

Registers

SP	4000
X30	1000
PC	3000

After CPU executes  
`add sp,sp,16`

Memory

4000	???
	-
	-
	-

Stack

Text

```
f:      -  
       -  
       -  
       -  
996    bl g  
1000    -  
       -  
       -  
       -  
       -  
       -  
       -  
2000   g: sub sp,sp,16  
2004   str x30,[sp]  
2008   -  
       -  
2992   ldr x30,[sp]  
2996   add sp,sp,16  
3000   ret
```

Princeton University  
COS 217: Introduction to Programming Systems  
Trace of an ARMv8 Assembly Language Function Call

Registers

SP	4000
X30	1000
PC	1000

Memory

4000	???
-	-
-	-
-	-
4000	???
-	-
-	-
-	-

Stack

f:	-
-	-
-	-
-	-
996	bl g
1000	-
-	-
ret	
2000	g: sub sp,sp,16
2004	str x30,[sp]
2008	-
-	-
2992	ldr x30,[sp]
2996	add sp,sp,16
3000	ret

Text

After CPU executes  
**ret**