16.317: Microprocessor Systems Design I

Summer 2013

Lecture 7: Solutions to Key Questions
July 30, 2013

Assume an x86 processor is running in protected mode with the state given below (all values in hex); note that each memory location shown contains a descriptor about a particular segment:

GDTR = 00200000001F
LDTR = 000B

DS = 0017
SS = 0018
ESI = 00001000
EBX = 0001120

Memory	Address
Base = 030010F0 Limit = 020F	00200000
Base = 00200020 Limit = 0017	00200008
Base = 00200038 Limit = 0010	00200010
Base = 1200C000 Limit = FFFF	00200018
Base = 12340000 Limit = 00FF	00200020

Memory	Address
Base = 01000010 Limit = 1127	00200028
Base = 03170200 Limit = 03F7	00200030
Base = 1A000000 Limit = 01FF	00200038
Base = 06B01000 Limit = 0F07	00200040
Base = 05000120 Limit = 000F	00200048

a. What is the base address and limit of the global descriptor table? How many descriptors does this table contain?

Solution: The base address and limit of the GDT are stored in the GDTR—the upper 4 bytes contain the base address (***00200000H***); the lower 2 bytes contain the limit (***001FH***).

To determine the number of descriptors, recall that:

- Each descriptor uses 8 bytes
- The size of the table, in bytes, is (limit + 1) = 001FH + 1 = 0020H = 32 bytes

Therefore, this table contains 32 / 8 = ***4 descriptors***

b. What is the base address and limit of the current local descriptor table? How many descriptors does this table contain?

Solution: The base address and limit of the current LDT are stored in the LDT cache, which must be loaded from the appropriate descriptor in the GDT. The LDTR is a selector that points to the correct descriptor. Recall that, in a selector:

- The lowest 2 bits give the requested priority level
- The next bit (table indicator) indicates either global (0) or local (1) memory access
- The upper 13 bits index into the appropriate descriptor table to choose a descriptor.

LDTR = 000BH = 0000 0000 0000 1011_2

→ Priority = 11_2, table indicator = 0, index = 0000 0000 0000 1_2 = 1

→ GDT descriptor 1 (the second descriptor in the GDT) describes current LDT

Therefore, the ***LDT base address = 00200020H,*** its ***limit = 0017H,*** and the number of descriptors = (0017H+1) / 8 = 0018H / 8 = 24 / 8 ***= 3 descriptors.***

c. What are the starting and ending addresses for the current data and stack segments?

Solution: In protected mode, the segment registers are selectors pointing either to the GDT or current LDT, as shown in (b). Therefore, the starting (base) and ending (base + limit) addresses for each segment can be determined after finding the right descriptor.

DS = 0017H = 0000 0000 0001 0111_2

→ Priority = 11_2, table indicator = 1, index = 0000 0000 0001 0 = 2

→ Descriptor #2 (3^{rd} descriptor) in LDT describes data segment

→ ***DS base address = 03170200H, ending address = 03170200 + 03F7 = 031705F7H***

SS = 0018H = 0000 0000 0001 1000_2

→ Priority = 00_2, table indicator = 0, index = 0000 0000 0001 1 = 3

→ Descriptor #3 (4^{th} descriptor) in GDT describes stack segment

→ ***SS base address = 1200C000H, ending address = 1200C000 + FFFF = 1201BFFFH***

d. What address is accessed by each of the following instructions?

Recall that protected mode addresses are calculated by adding the base address of the requested segment to the effective address calculated from the instruction. Part (c) of this problem helped you determine the starting address of each segment used.

i. `MOV AX, [0100H]`

Solution: Address = DS:0100H = 03170200H + 0100H = ***03170300H***

ii. `ADD DX, [SI]`

Solution: Address = DS:SI = DS:1000H = 03170200H + 1000H = ***03171200H***

iii. `MOV AX, SS:[SI+EF00]`

Solution: Address = SS:SI+EF00 = SS:1000H+EF00H
= 1200C000H + 1000H + EF00H = ***1201BF00H***

iv. `SUB SS:[A200], CX`

Solution: Address = SS:A200 = 1200C000H + A200H = ***12016200H***

v. `MOV DX, [BX+SI]`

Solution: Address = DS:BX+SI = DS:1120H+1000H
= 03170200H + 1120H + 1000H = ***03172320H***

vi. `MOV CX, [BX+SI+1EH]`

Solution: Address = DS:BX+SI+1EH = DS:1120H+1000H +1EH
= 03170200H + 1120H + 1000H + 1EH = ***0317233EH***