1. 地址空间和栈

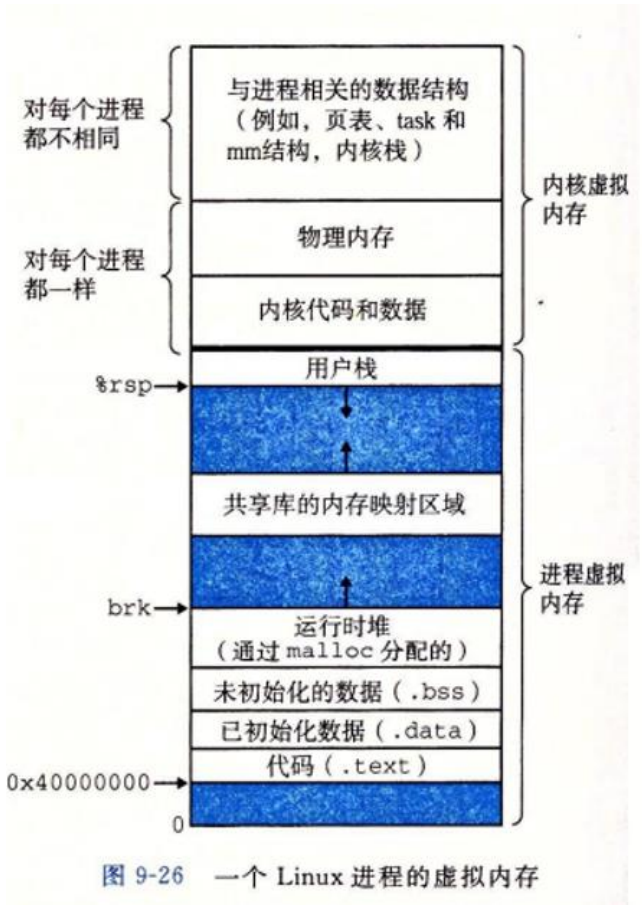

图 9-26 一个 Linux 进程的虚拟内存

内核地址空间：
栈：
共享映射
堆：
bss 和 data 段：
代码段：

2. 在 x86-64、Linux 操作系统下有如下 C 定义：

```
struct A {
    char CC1[6];
    int II1;
    long LL1;
    char CC2[10];
    long LL2;
    int II2;
};
```

(1) sizeof(A) = _____

(2) 将 A 重排后，令结构体尽可能小，那么得到的新的结构体大小为_____字节。

得分

第三题（20 分）

请分析下面的 C 语言程序和对应的 x86-64 汇编代码。

1.其中，有一部分缺失的代码（用标号标出），请在标号对应的横线上填写缺失的内容。注:汇编与机器码中的数字用 16 进制数填写。

C 语言代码如下：

```
typedef struct _parameters {
    int n;
    int product;
} parameters;
int bar(parameters *params, int x) {
    params->product *= x;
}
void foo (parameters *params) {
    if (params->n <= 1)
        ___（1）___                          （1）_____________
    bar(params, ___（2）__);                 （2）_____________
    params->n--;
    foo(params);
}
```

x86-64 汇编代码如下（为简单起见，函数内指令地址只给出后四位，需要时可补全）：

```
0x0000555555555189 <bar>:
    5189: f3 0f 1e fa   endbr64
    518d: 55            push   %rbp
    518e: 48 89 e5      mov    %rsp,%rbp
    5191: 48 89 7d f8   mov    _（3）_,-0x8(%rbp)  （3）__________
    5195: 89 75 f4      mov    %esi,-0xc(%rbp)
    5198: 48 8b 45 f8   mov    -0x8(%rbp),%rax
    519c: 8b 40 04      mov    0x4(%rax),%eax
    519f: 0f af 45 f4   imul   _（4）_(%rbp),%eax  （4）__________
    51a3: 89 c2         mov    %eax,%edx
    51a5: 48 8b 45 f8   mov    -0x8(%rbp),%rax
```

```
    51a9: 89 50 04      mov    %edx,0x4(%rax)
    51ac: 90            nop
    51ad: 5d            pop    _(5)_           (5)_________
    51ae: c3            retq

00005555555551af <foo>:
    51af: f3 0f 1e fa   endbr64
    51b3: 55            push   %rbp
    51b4: 48 89 e5      mov    %rsp,%rbp
    51b7: 48 83 ec 10   _(6)_  $0x10,%rsp       (6)_________
    51bb: 48 89 7d f8   mov    %rdi,-0x8(%rbp)
    51bf: 48 8b 45 f8    mov    -0x8(%rbp),%rax
    51c3: 8b 00         mov    (%rax),%eax
    51c5: 83 f8 01      cmp    $0x1,%eax
    51c8: 7e 31         _(7)_ 51fb <foo+0x4c>   (7)_________
    51ca: 48 8b 45 f8    mov    -0x8(%rbp),%rax
    51ce: 8b 10         mov    (%rax),%edx
    51d0: 48 8b 45 f8    mov    -0x8(%rbp),%rax
    51d4: 89 d6         mov    %edx,%esi
    51d6: 48 89 c7      mov    %rax,%rdi
    51d9: e8 ab ff ff ff   callq  0x0000555555555189 <bar>
    51de: 48 8b 45 f8    mov    -0x8(%rbp),%rax
    51e2: 8b 00         mov    (%rax),%eax
    51e4: 8d 50 ff      lea  -0x1(_(8)_),%edx   (8)_________
    51e7: 48 8b 45 f8   mov    -0x8(%rbp),%rax
    51eb: 89 10         mov   _(9)_,(%rax)      (9)__________
    51ed: 48 8b 45 f8   mov  _(10)_ ,%rax      (10)_________
    51f1: 48 89 c7      mov    %rax,%rdi
    51f4: e8 b6 ff ff ff   callq   _(11)_       (11)_________
    51f9: eb 01         jmp    51fc <foo+0x4d>
    51fb: 90            nop
    51fc: c9            leaveq
    51fd: c3            retq
```

2.在程序执行到 0x000055555555518e 时（该指令还未执行），此时的栈帧如下，请填写空格中对应的值。

地址	值
0x7fffffffe308	0xffffe340
0x7fffffffe304	0x00000000
0x7fffffffe300	0x00000000
0x7fffffffe2fc	0x00005555
0x7fffffffe2f8	（12）_____
0x7fffffffe2f4	0x00007fff
0x7fffffffe2f0	0xffffe310
0x7fffffffe2ec	0x00007fff
0x7fffffffe2e8	0xffffe340
0x7fffffffe2e4	0x00000004
0x7fffffffe2e0	0xffffe350
0x7fffffffe2dc	0x00005555
0x7fffffffe2d8	（13）_____
0x7fffffffe2d4	0x00007fff
0x7fffffffe2d0	（14）_____

3.当 params={n,1}时， foo(&params)函数的功能是什么？