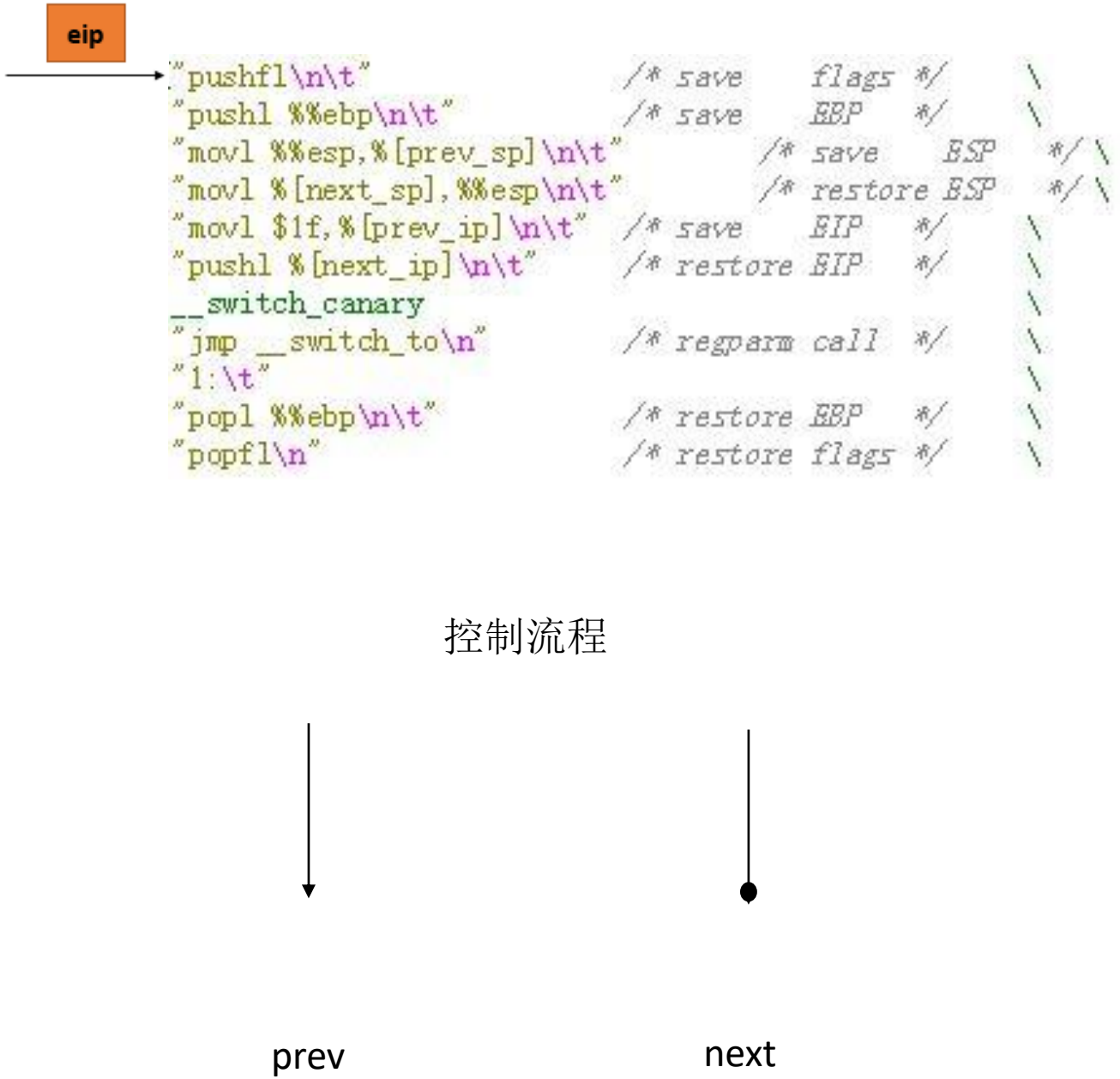
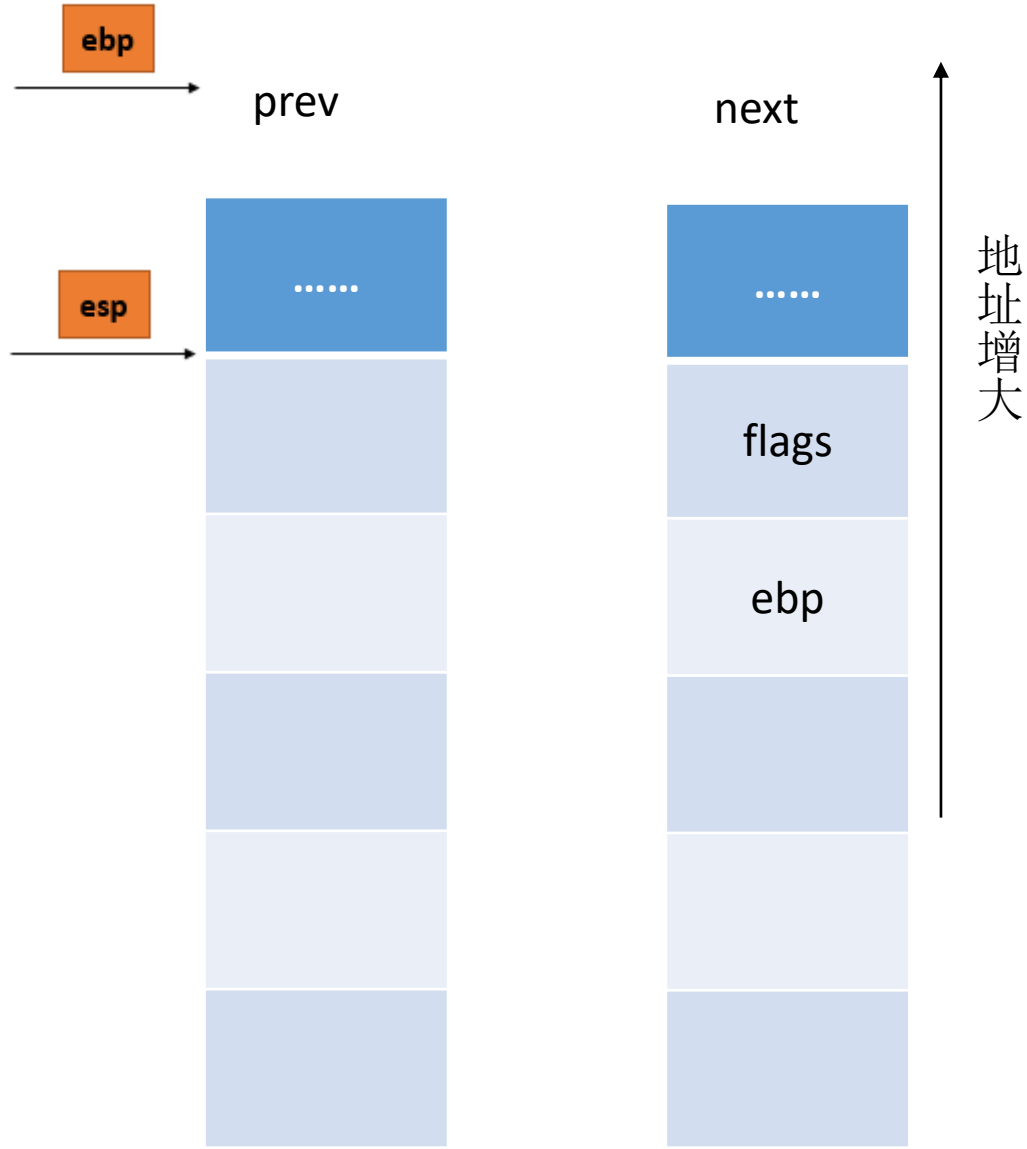

eip
"pushfl\n\t" /* save flags */ \
"pushl %%ebp\n\t" /* save EBP */ \
"movl %%esp,%[prev_sp]\n\t" /* save ESP */ \
"movl %[next_sp],%%esp\n\t" /* restore ESP */ \
"movl $1f,%[prev_ip]\n\t" /* save EIP */ \
"pushl %[next_ip]\n\t" /* restore EIP */ \
__switch_canary \
"jmp __switch_to\n" /* regparm call */ \
"1:\t" \
"popl %%ebp\n\t" /* restore EBP */ \
"popfl\n" /* restore flags */ \
控制流程
prev
next


ebp
esp
prev
next
.....
.....
flags
ebp
地址增大

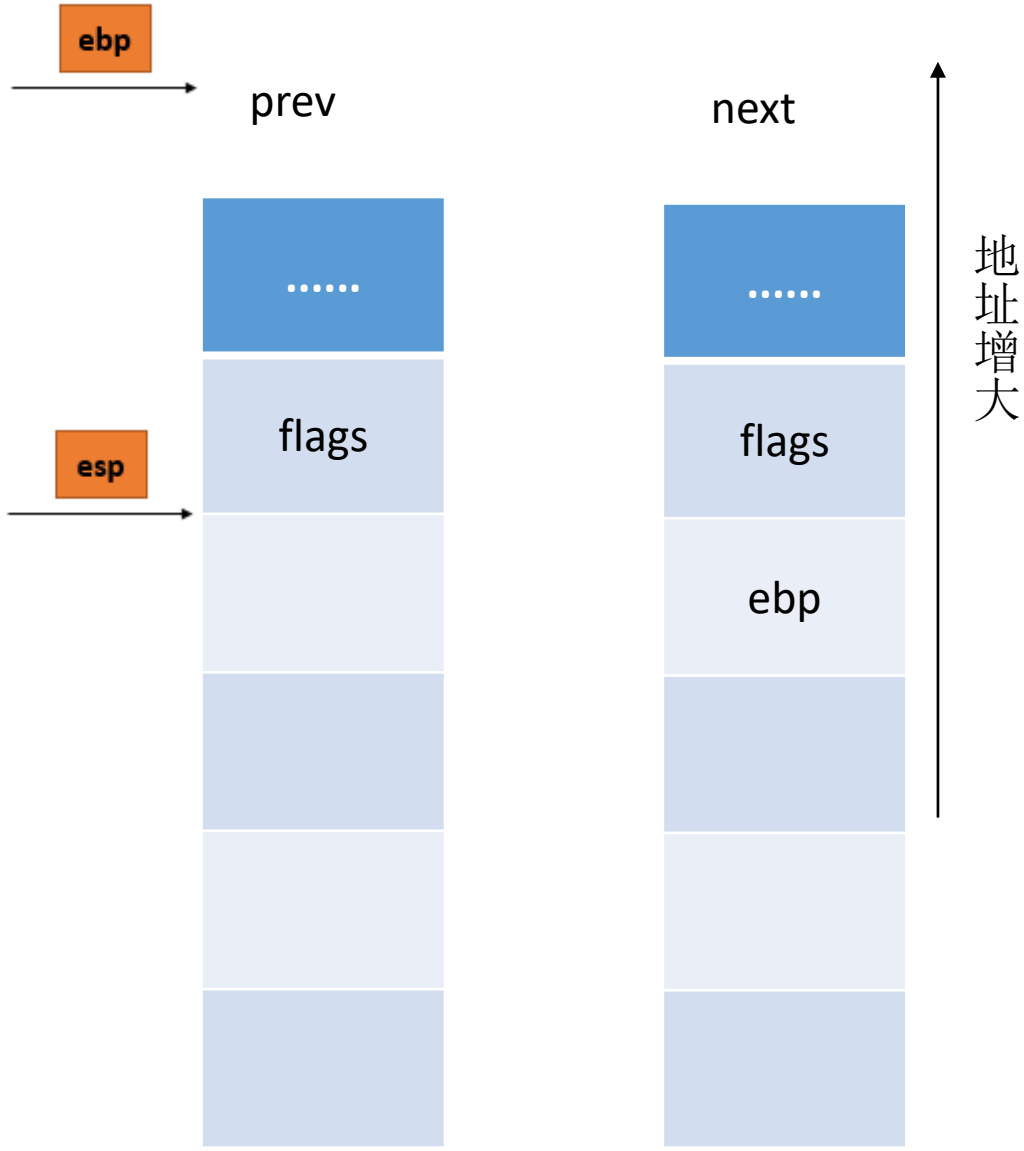
eip

```
"pushfl\n\t"                    /* save    flags */     \
"pushl %%ebp\n\t"               /* save    EBP   */     \
"movl %%esp,%[prev_sp]\n\t"          /* save    ESP   */ \
"movl %[next_sp],%%esp\n\t"          /* restore ESP   */ \
"movl $1f,%[prev_ip]\n\t"       /* save    EIP   */     \
"pushl %[next_ip]\n\t"          /* restore EIP   */     \
__switch_canary                                         \
"jmp __switch_to\n"             /* regparm call  */     \
"1:\t"                                                  \
"popl %%ebp\n\t"                /* restore EBP   */     \
"popfl\n"                       /* restore flags */     \
```

控制流程

prev

next



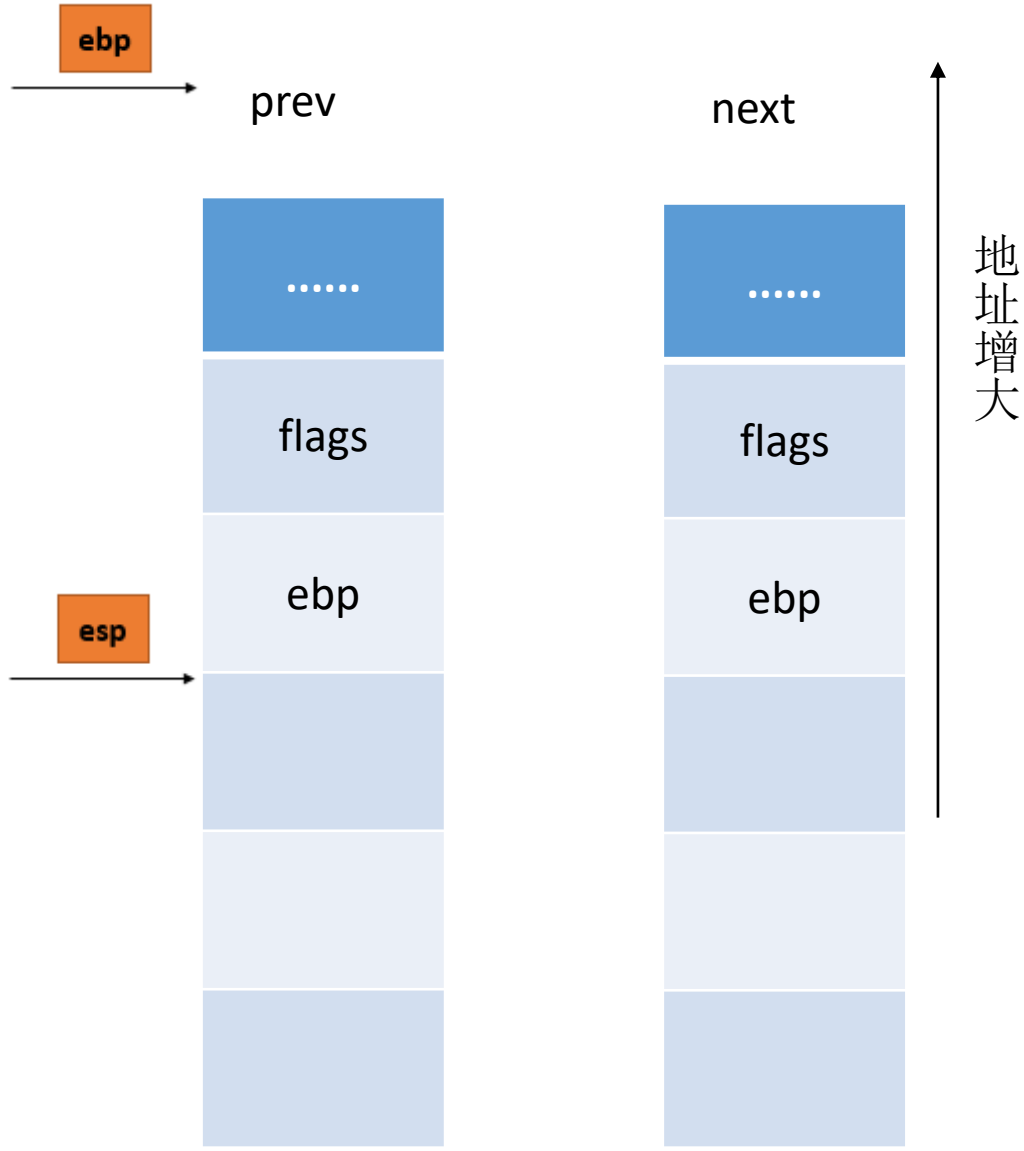
eip

```
"pushfl\n\t"                    /* save    flags */     \
"pushl %%ebp\n\t"               /* save    EBP   */     \
"movl %%esp,%[prev_sp]\n\t"             /* save    ESP   */ \
"movl %[next_sp],%%esp\n\t"             /* restore ESP   */ \
"movl $1f,%[prev_ip]\n\t"       /* save    EIP   */     \
"pushl %[next_ip]\n\t"          /* restore EIP   */     \
__switch_canary                                         \
"jmp __switch_to\n"             /* regparm call  */     \
"1:\t"                                                  \
"popl %%ebp\n\t"                /* restore EBP   */     \
"popfl\n"                       /* restore flags */     \
```

控制流程

prev

next



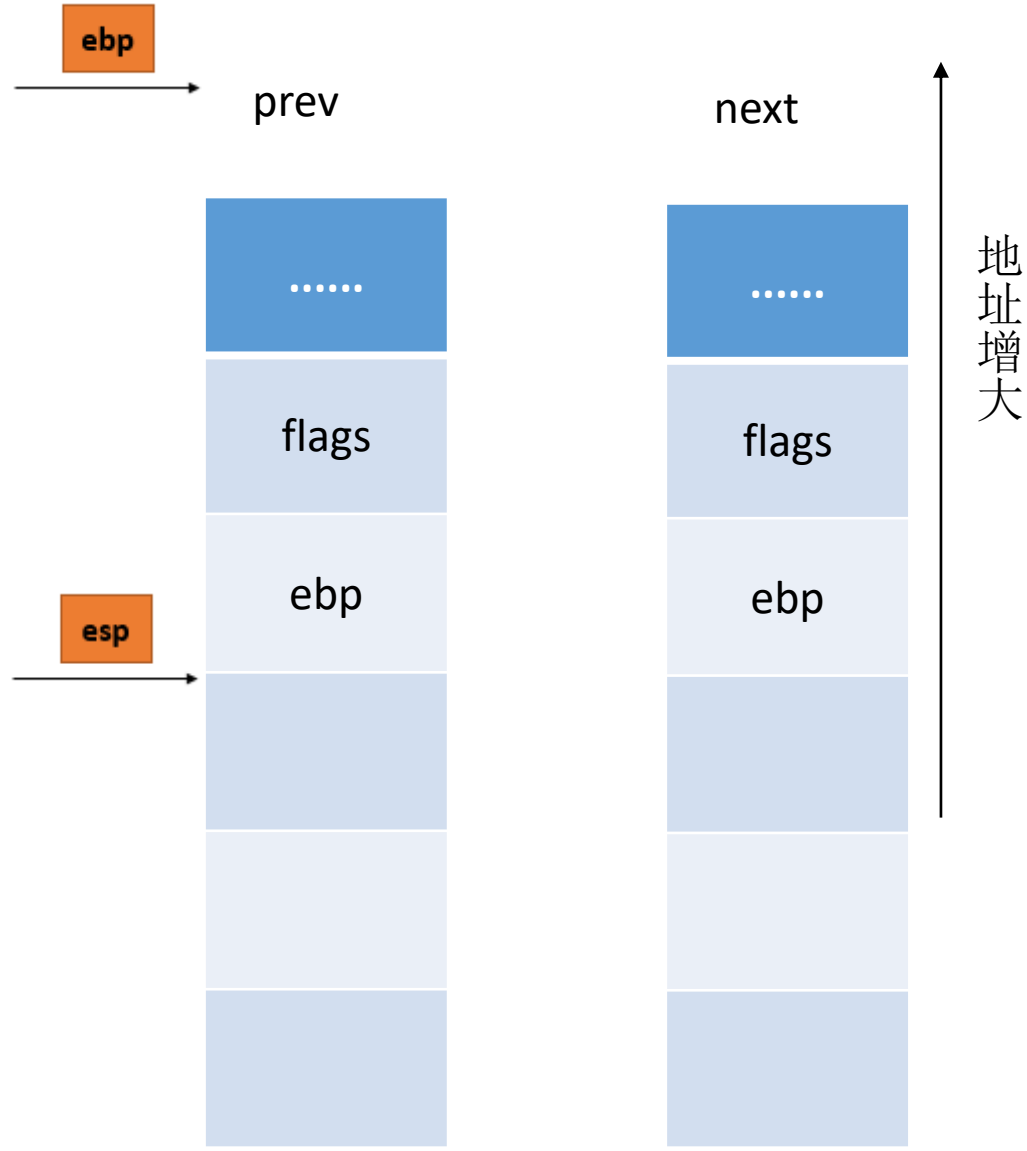
```
"pushfl\n\t"                    /* save    flags */     \
"pushl %%ebp\n\t"               /* save    EBP   */     \
"movl %%esp,%[prev_sp]\n\t"             /* save    ESP   */ \
"movl %[next_sp],%%esp\n\t"             /* restore ESP   */ \
"movl $1f,%[prev_ip]\n\t"       /* save    EIP   */     \
"pushl %[next_ip]\n\t"          /* restore EIP   */     \
__switch_canary                                         \
"jmp __switch_to\n"             /* regparm call  */     \
"1:\t"                                                  \
"popl %%ebp\n\t"                /* restore EBP   */     \
"popfl\n"                       /* restore flags */     \
```

eip

控制流程

prev

next




保存esp到prev->thread.sp

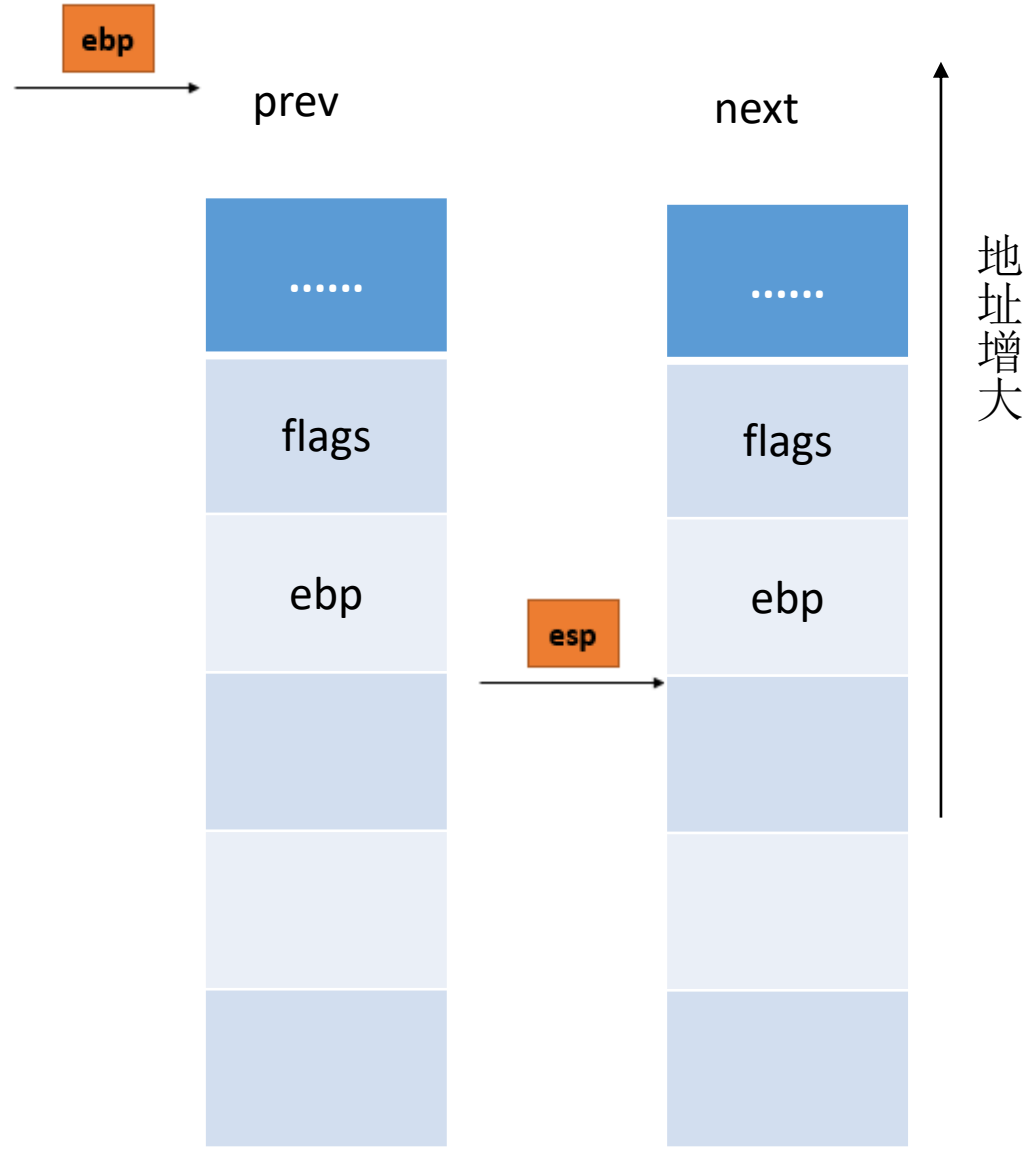
```
"pushfl\n\t"                    /* save    flags */     \
"pushl %%ebp\n\t"               /* save    EBP   */     \
"movl %%esp,%[prev_sp]\n\t"             /* save    ESP   */ \
"movl %[next_sp],%%esp\n\t"             /* restore ESP   */ \
"movl $1f,%[prev_ip]\n\t"       /* save    EIP   */     \
"pushl %[next_ip]\n\t"          /* restore EIP   */     \
__switch_canary                                         \
"jmp __switch_to\n"             /* regparm call  */     \
"1:\t"                                                  \
"popl %%ebp\n\t"                /* restore EBP   */     \
"popfl\n"                       /* restore flags */     \
```

eip

控制流程

prev

next



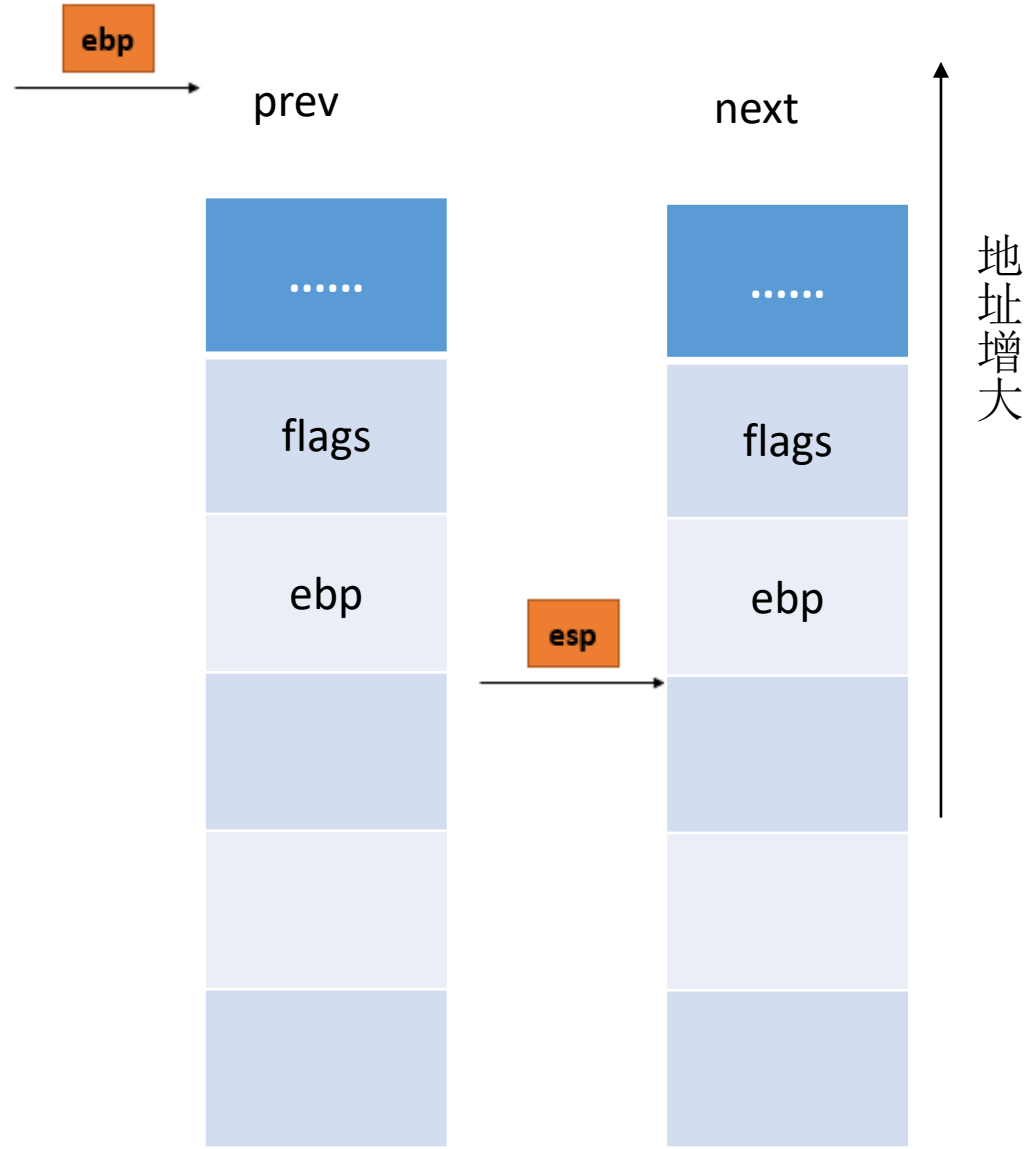
```
"pushfl\n\t"                    /* save    flags */     \
"pushl %%ebp\n\t"               /* save    EBP   */     \
"movl %%esp,%[prev_sp]\n\t"             /* save    ESP   */ \
"movl %[next_sp],%%esp\n\t"             /* restore ESP   */ \
"movl $1f,%[prev_ip]\n\t"       /* save    EIP   */     \
"pushl %[next_ip]\n\t"          /* restore EIP   */     \
__switch_canary                                         \
"jmp __switch_to\n"             /* regparm call  */     \
"1:\t"                                                  \
"popl %%ebp\n\t"                /* restore EBP   */     \
"popfl\n"                       /* restore flags */     \
```

eip

控制流程

prev

next




标号1地址保存到prev->thread.ip

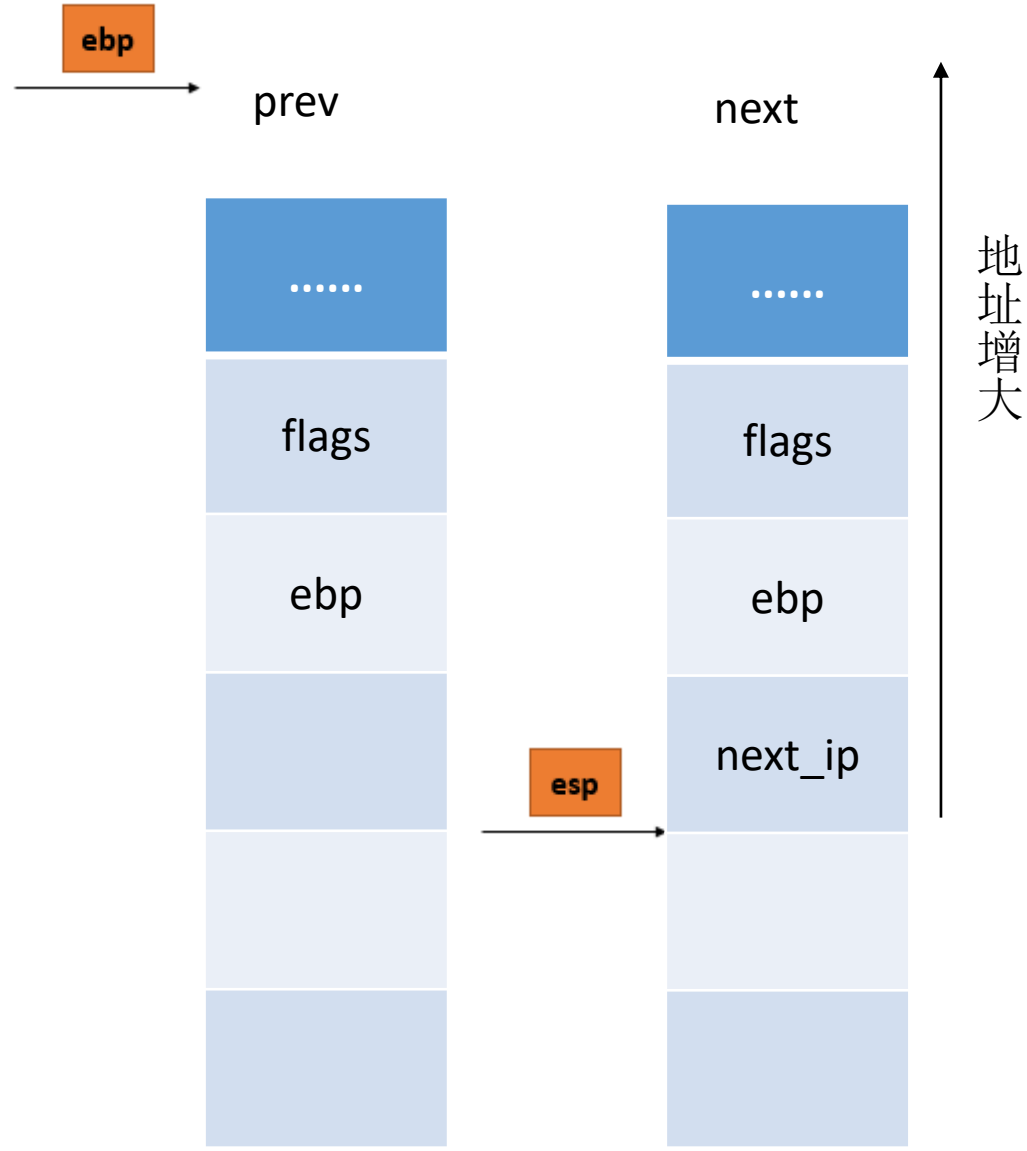
```
"pushfl\n\t"                    /* save    flags */     \
"pushl %%ebp\n\t"               /* save    EBP   */     \
"movl %%esp,%[prev_sp]\n\t"             /* save    ESP   */ \
"movl %[next_sp],%%esp\n\t"             /* restore ESP   */ \
"movl $1f,%[prev_ip]\n\t"       /* save    EIP   */     \
"pushl %[next_ip]\n\t"          /* restore EIP   */     \
__switch_canary                                         \
"jmp __switch_to\n"             /* regparm call  */     \
"1:\t"                                                  \
"popl %%ebp\n\t"                /* restore EBP   */     \
"popfl\n"                       /* restore flags */     \
```

eip

控制流程

prev

next



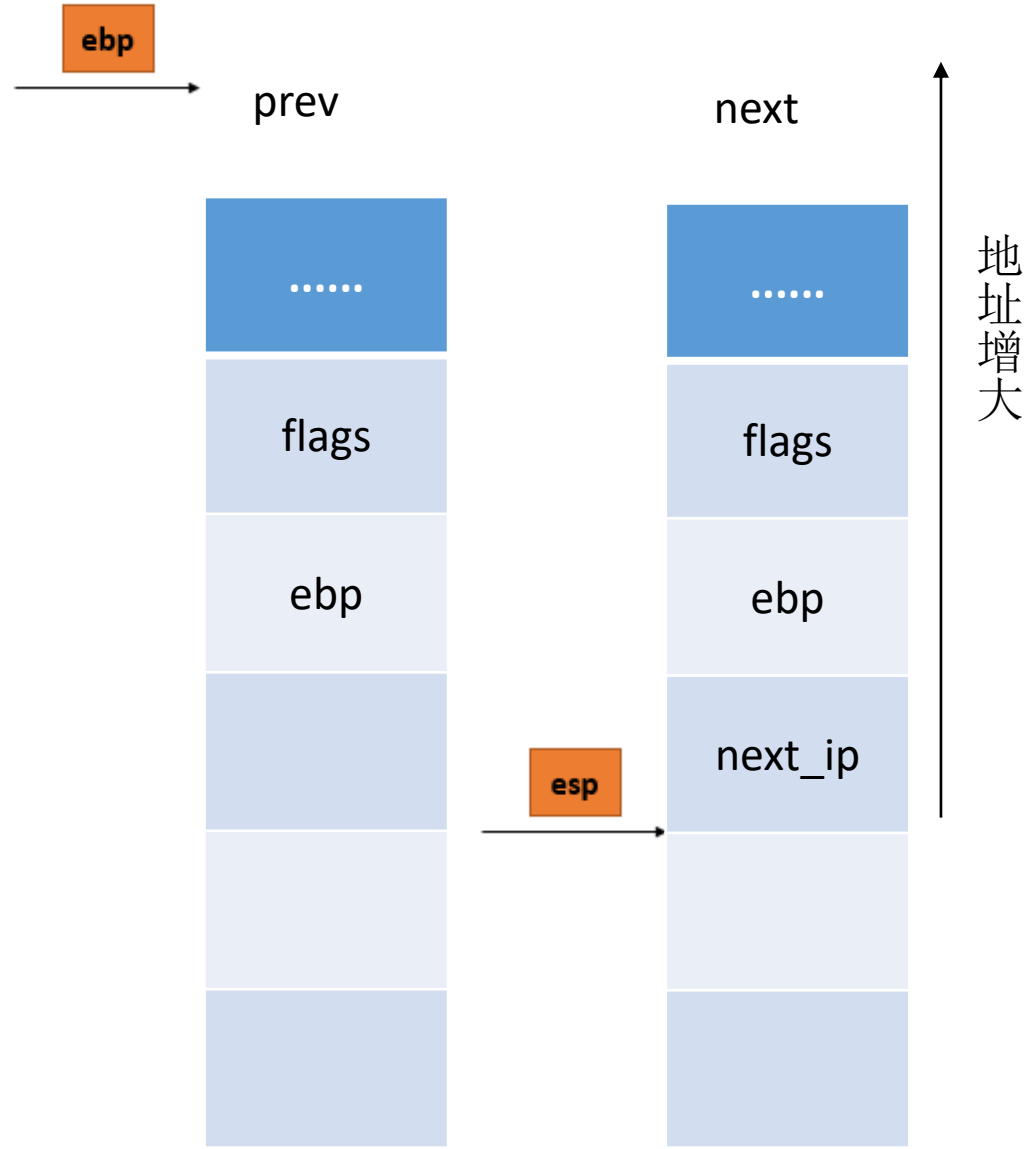
```
"pushfl\n\t"                    /* save    flags */     \
"pushl %%ebp\n\t"               /* save    EBP   */     \
"movl %%esp,%[prev_sp]\n\t"             /* save    ESP   */ \
"movl %[next_sp],%%esp\n\t"             /* restore ESP   */ \
"movl $1f,%[prev_ip]\n\t"       /* save    EIP   */     \
"pushl %[next_ip]\n\t"          /* restore EIP   */     \
__switch_canary                                         \
"jmp __switch_to\n"             /* regparm call  */     \
"1:\t"                                                  \
"popl %%ebp\n\t"                /* restore EBP   */     \
"popfl\n"                       /* restore flags */     \
```

eip

控制流程

prev

next

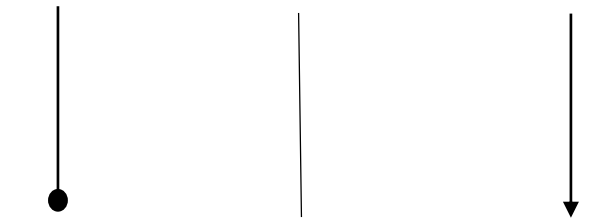



执行了宏定义__switch_canary，
至于作用是什么还没明白

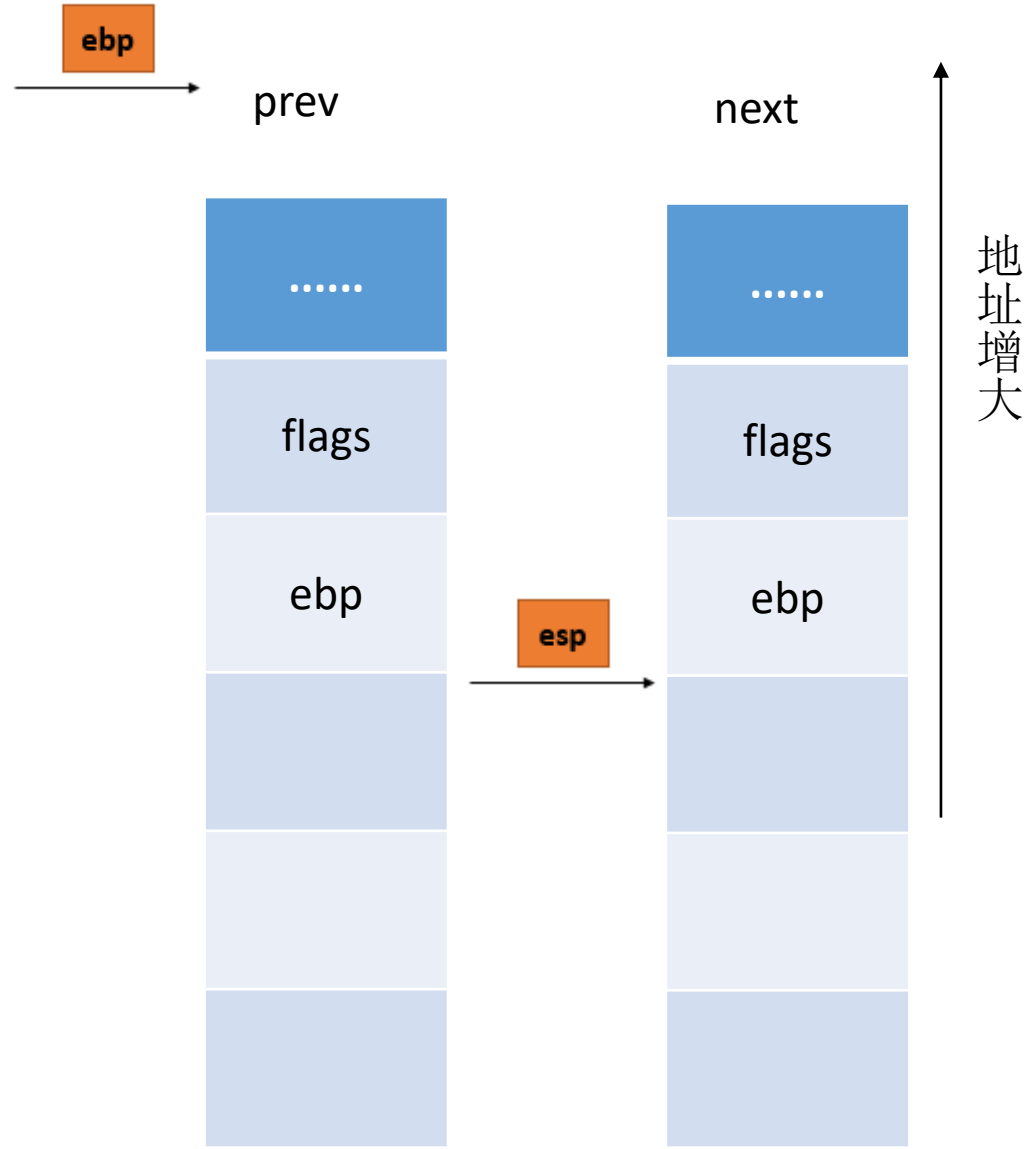
```
"pushfl\n\t"                    /* save    flags */     \
"pushl %%ebp\n\t"               /* save    EBP   */     \
"movl %%esp,%[prev_sp]\n\t"             /* save    ESP   */ \
"movl %[next_sp],%%esp\n\t"             /* restore ESP   */ \
"movl $1f,%[prev_ip]\n\t"       /* save    EIP   */     \
"pushl %[next_ip]\n\t"          /* restore EIP   */     \
__switch_canary                                         \
"jmp __switch_to\n"             /* regparm call  */     \
"1:\t"                                                  \
"popl %%ebp\n\t"                /* restore EBP   */     \
"popfl\n"                       /* restore flags */     \
```

eip

控制流程



prev　　__switch_to　　next



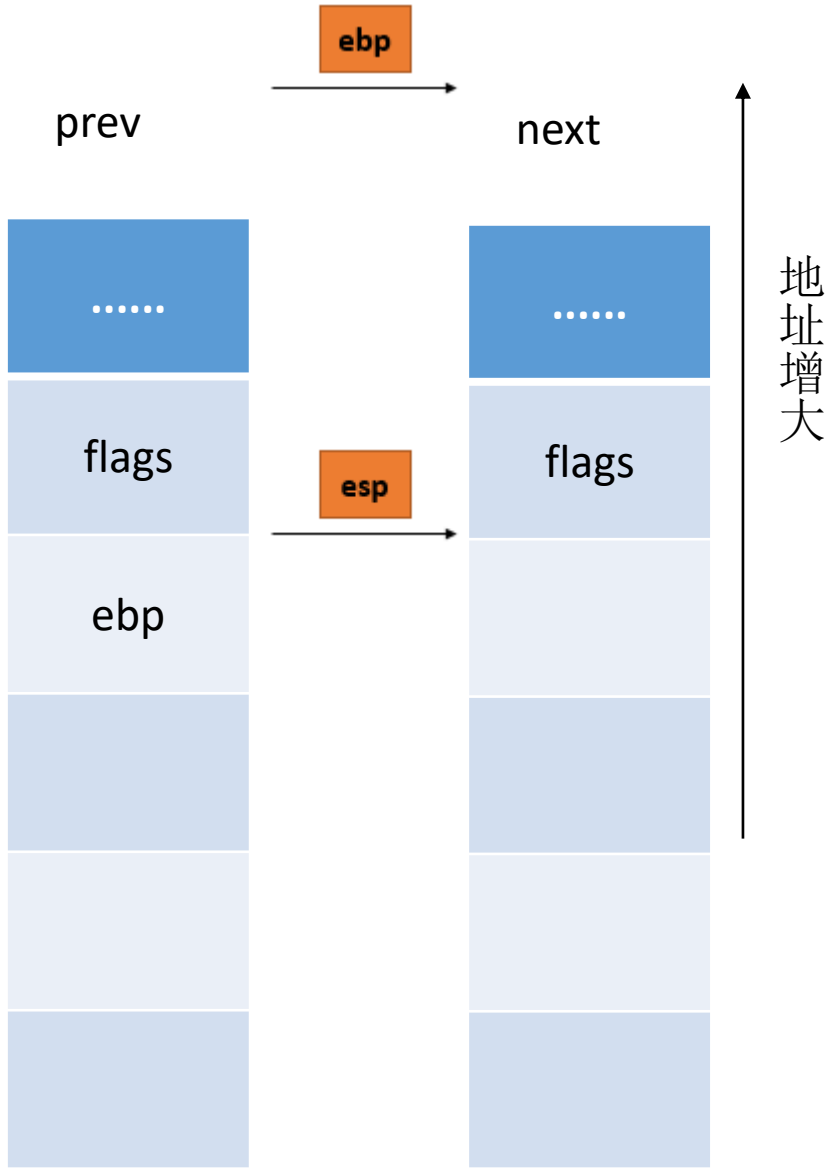

切换到了next进程

```
"pushfl\n\t"                    /* save    flags */     \
"pushl %%ebp\n\t"               /* save    EBP   */     \
"movl %%esp,%[prev_sp]\n\t"          /* save    ESP   */ \
"movl %[next_sp],%%esp\n\t"          /* restore ESP   */ \
"movl $1f,%[prev_ip]\n\t"       /* save    EIP   */     \
"pushl %[next_ip]\n\t"          /* restore EIP   */     \
__switch_canary                                         \
"jmp __switch_to\n"             /* regparm call  */     \
"1:\t"                                                  \
"popl %%ebp\n\t"                /* restore EBP   */     \
"popfl\n"                       /* restore flags */     \
```

eip

控制流程

prev　　__switch_to　　next



```
"pushfl\n\t"                    /* save    flags */     \
"pushl %%ebp\n\t"               /* save    EBP   */     \
"movl %%esp,%[prev_sp]\n\t"             /* save    ESP   */ \
"movl %[next_sp],%%esp\n\t"             /* restore ESP   */ \
"movl $1f,%[prev_ip]\n\t"       /* save    EIP   */     \
"pushl %[next_ip]\n\t"          /* restore EIP   */     \
__switch_canary                                         \
"jmp __switch_to\n"             /* regparm call  */     \
"1:\t"                                                  \
"popl %%ebp\n\t"                /* restore EBP   */     \
"popfl\n"                       /* restore flags */     \
```

eip

控制流程

prev　　__switch_to　　next