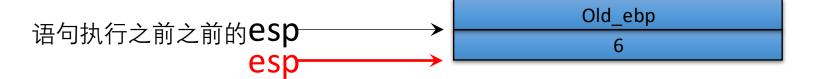
push ebp mov_ebp,esp

push 6 push 5 call AFunc add esp,8

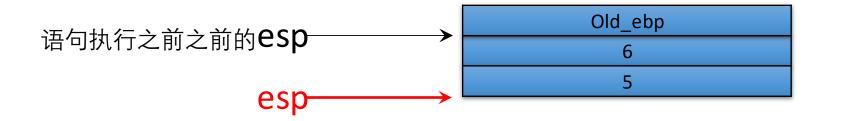
PS: 执行语句之前的EBP在此栈空间的更高处

push ebp mov ebp,esp push 6

push 5 call AFunc add esp,8

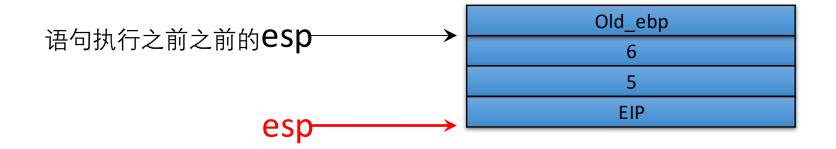


push ebp mov ebp,esp push 6 push 5 call AFunc add esp,8



栈底

push ebp mov ebp,esp push 6 push 5 call AFunc add esp,8



AFunc(5,6); push 6 push 5 call AFunc add esp,8 AFunc push ebp

mov ebp,esp

sub esp,0x10

call _BFunc

add esp,0x8

mov eax,0x8

leave

ret

mov DWORD PTR [ebp-0x4],0x3

mov DWORD PTR [ebp-0x8],0x4

mov eax, DWORD PTR [ebp+0x8]

mov DWORD PTR [ebp-0x4],eax

mov eax, DWORD PTR [ebp+0xc]

mov DWORD PTR [ebp-0x8],eax

push DWORD PTR [ebp-0x8]

push DWORD PTR [ebp-0x4]

AFunc(5,6); push 6 push 5 call AFunc add esp,8 AFunc(5,6); EIP EBP Old_ebp 核底 Figure 1 Kinc 1 Kinc 2 Kinc 2 Kinc 3 Kinc 4 Kinc 3 Kinc 4 K

AFunc

push ebp

add esp,0x8

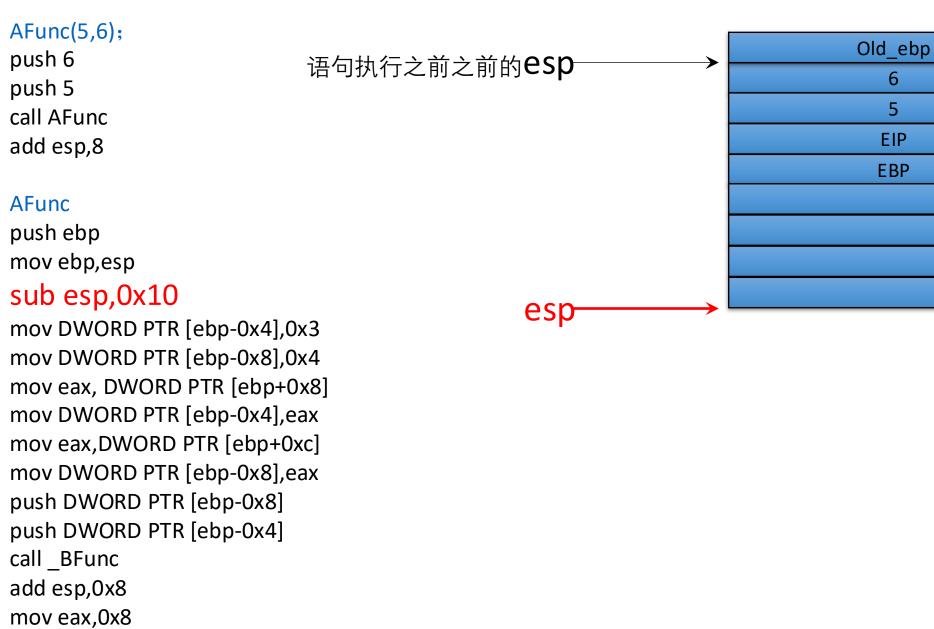
mov eax,0x8

leave

ret

mov ebp,esp

sub esp,0x10
mov DWORD PTR [ebp-0x4],0x3
mov DWORD PTR [ebp-0x8],0x4
mov eax, DWORD PTR [ebp+0x8]
mov DWORD PTR [ebp-0x4],eax
mov eax,DWORD PTR [ebp+0xc]
mov DWORD PTR [ebp-0x8],eax
push DWORD PTR [ebp-0x8]
push DWORD PTR [ebp-0x4]
call BFunc

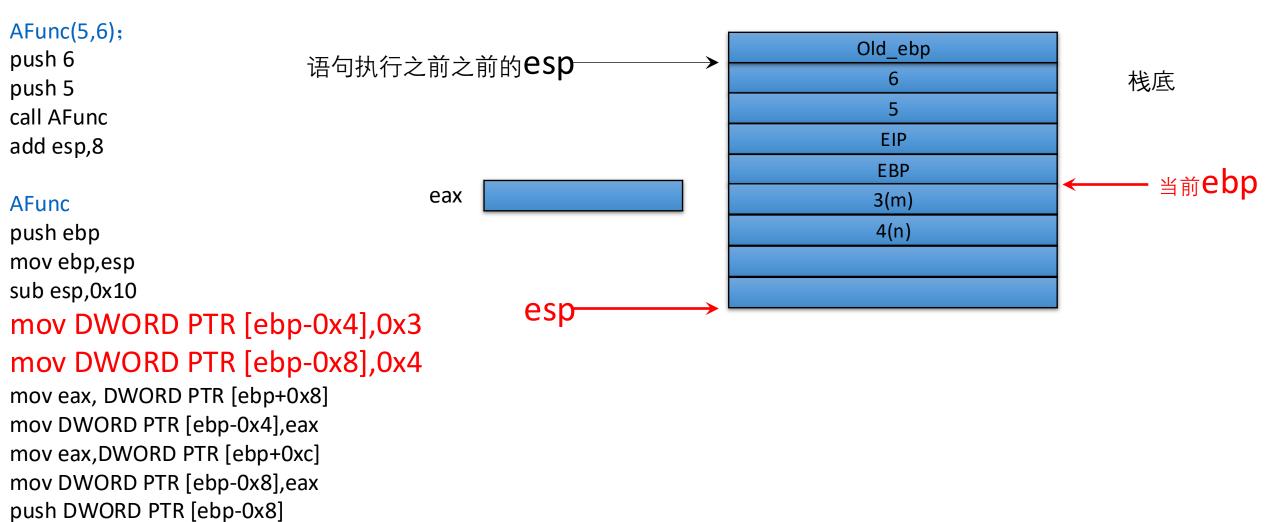


leave

ret

栈底

当前ebp

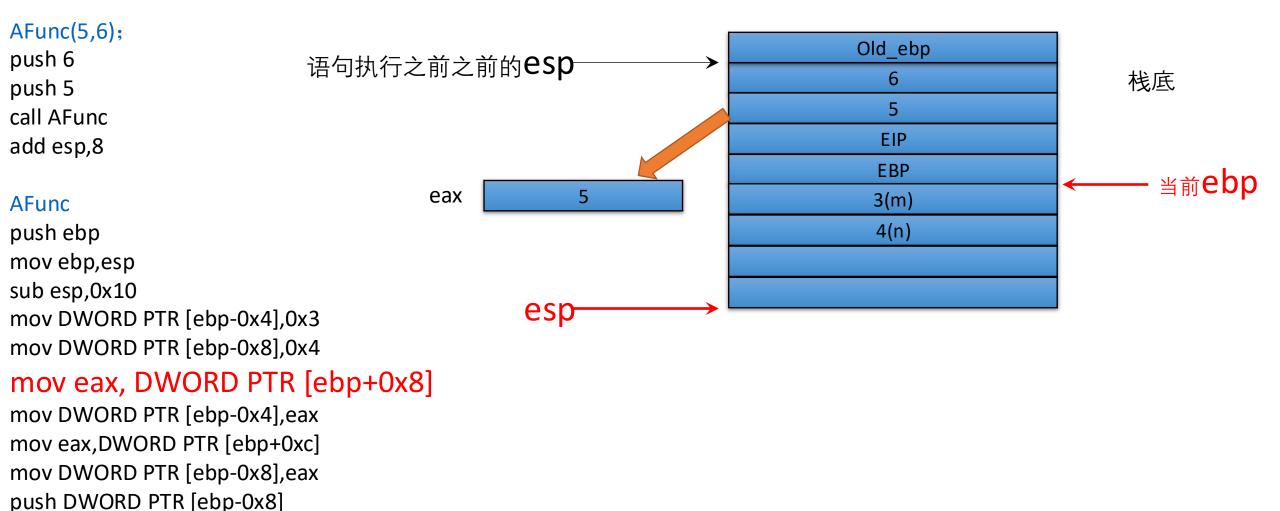


call _BFunc

add esp,0x8

mov eax,0x8

leave

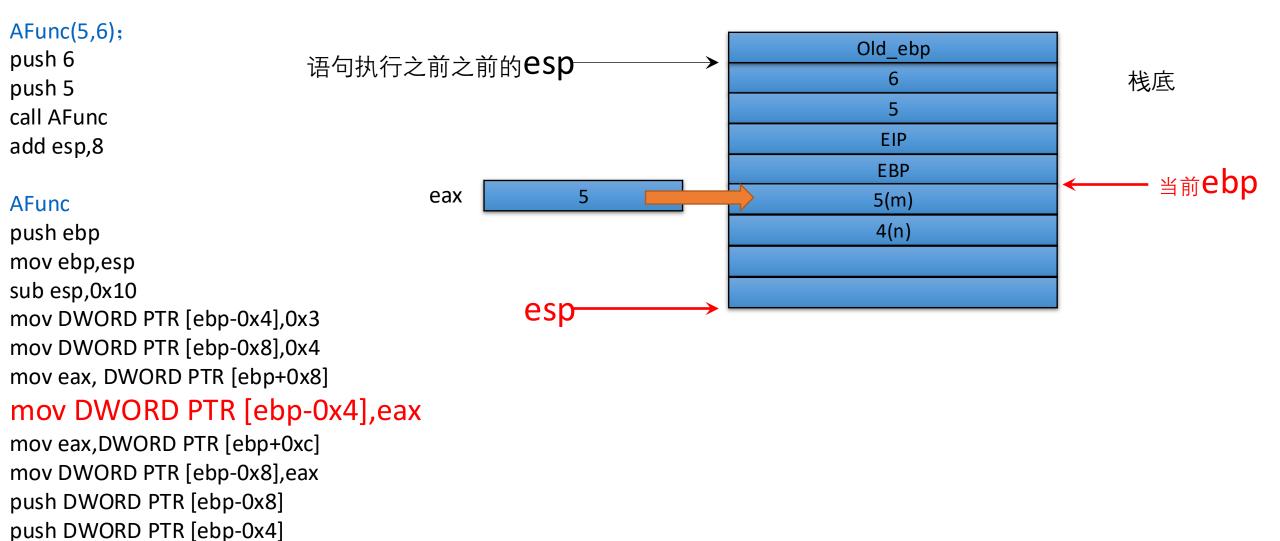


call _BFunc

add esp,0x8

mov eax,0x8

leave

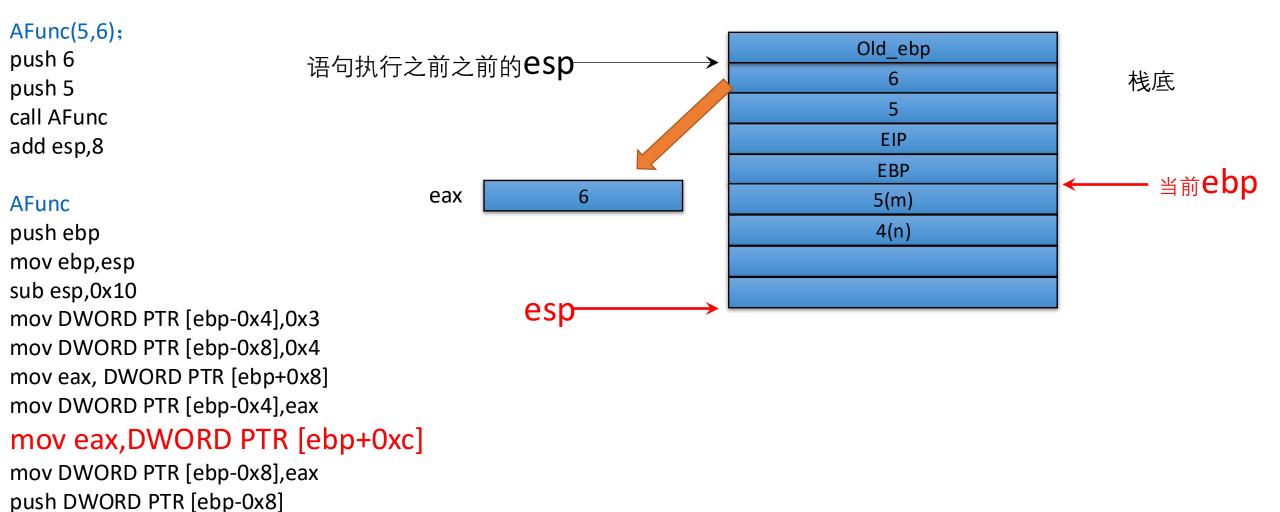


call _BFunc

add esp,0x8

mov eax,0x8

leave

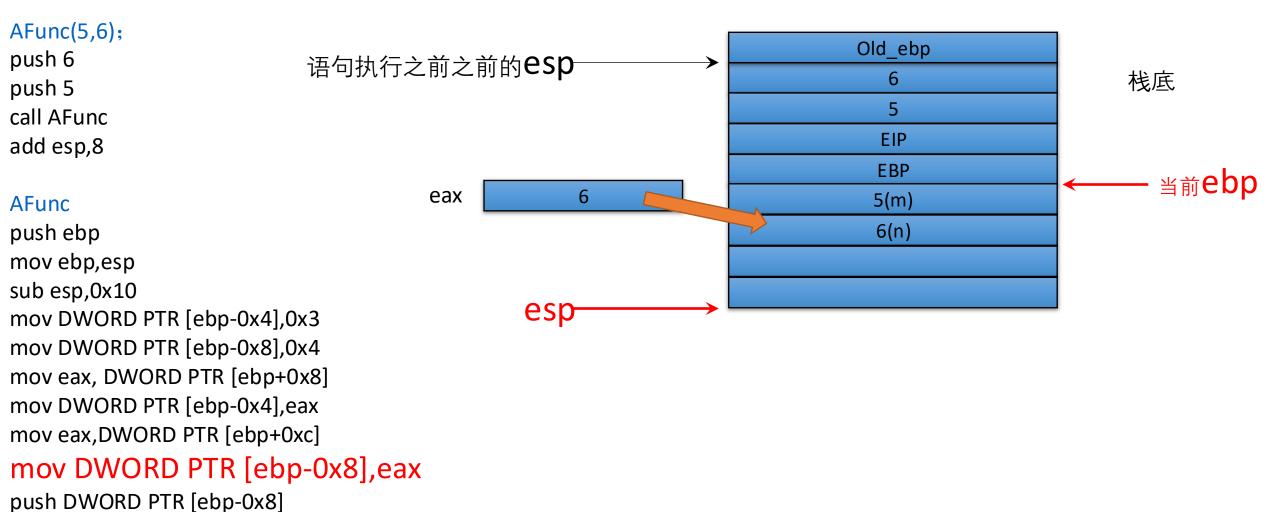


call _BFunc

add esp,0x8

mov eax,0x8

leave

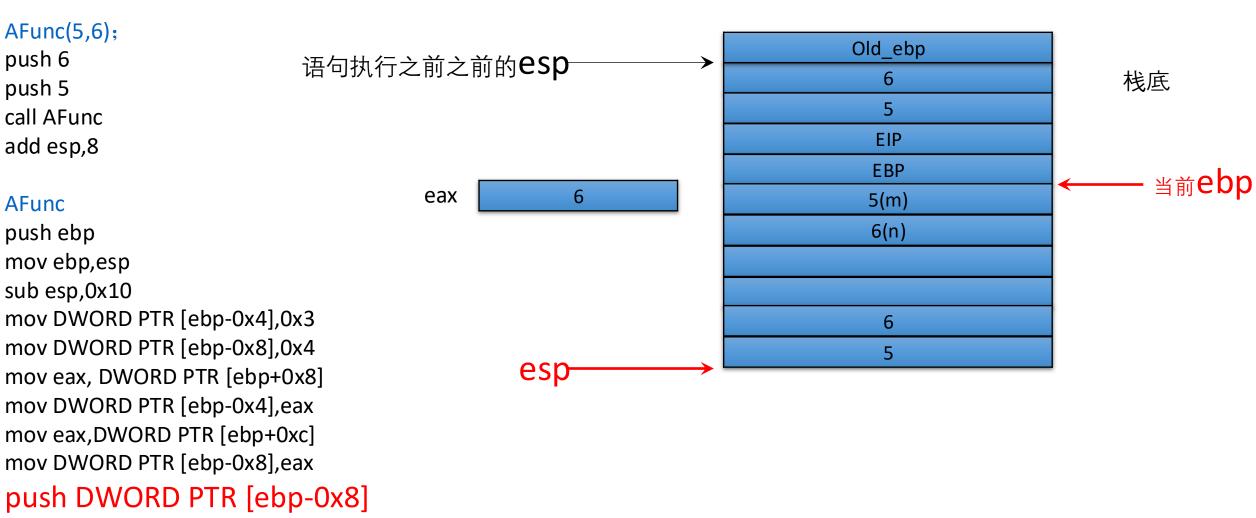


call _BFunc

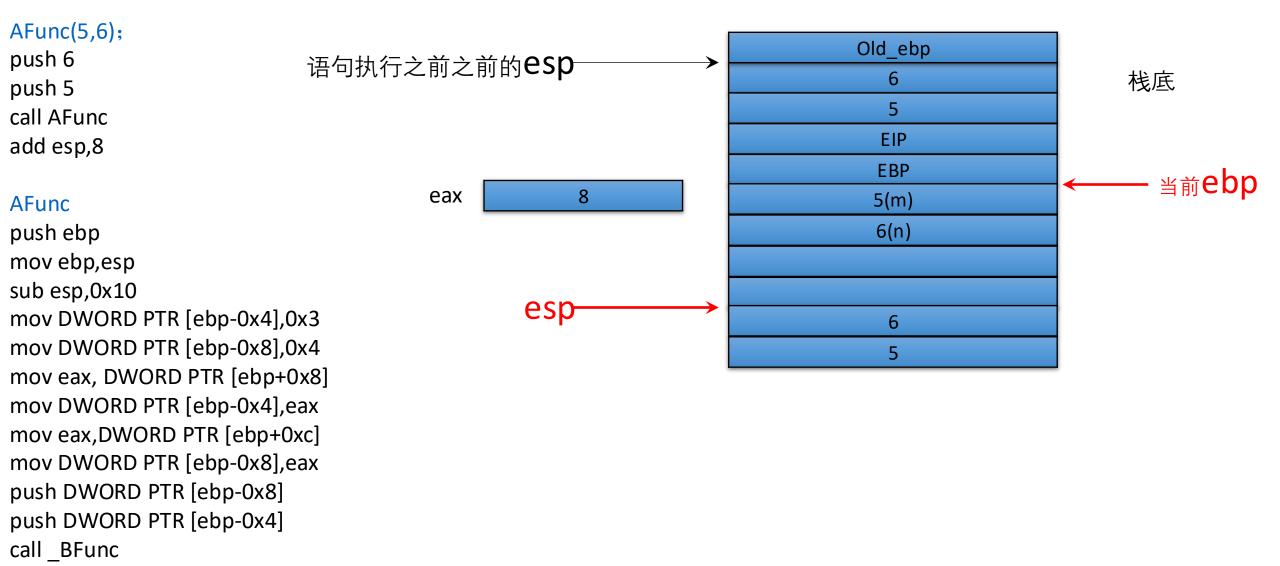
add esp,0x8

mov eax,0x8

leave



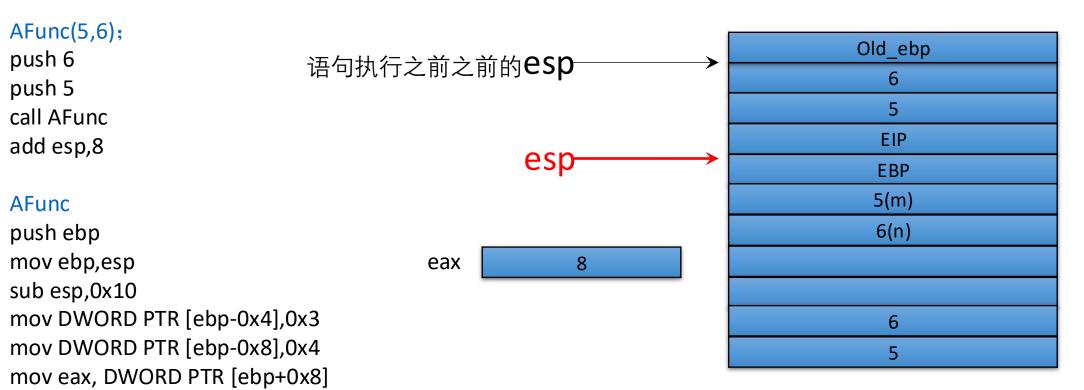
call _BFunc add esp,0x8 mov eax,0x8 leave



add esp,0x8

mov eax,0x8

leave ret



mov DWORD PTR [ebp-0x4],eax

mov eax, DWORD PTR [ebp+0xc]

mov DWORD PTR [ebp-0x8],eax

push DWORD PTR [ebp-0x8]

push DWORD PTR [ebp-0x4]

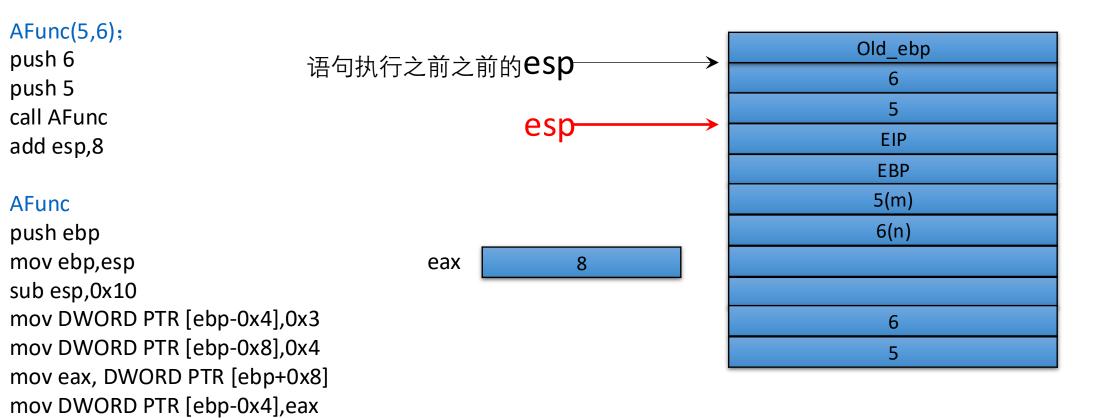
call _BFunc

add esp,0x8

mov eax,0x8

leave

ret



mov eax, DWORD PTR [ebp+0xc]

mov DWORD PTR [ebp-0x8],eax

push DWORD PTR [ebp-0x8]

push DWORD PTR [ebp-0x4]

call _BFunc

add esp,0x8

mov eax,0x8

leave

ret

栈底

AFunc(5,6); push 6 push 5 call AFunc add esp,8

AFunc push ebp mov ebp,esp sub esp,0x10 mov DWORD PTR [ebp-0x4],0x3 mov DWORD PTR [ebp-0x8],0x4 mov eax, DWORD PTR [ebp+0x8] mov DWORD PTR [ebp-0x4],eax mov eax, DWORD PTR [ebp+0xc] mov DWORD PTR [ebp-0x8],eax push DWORD PTR [ebp-0x8] push DWORD PTR [ebp-0x4] call _BFunc add esp,0x8 mov eax,0x8 leave ret

