Advanced Optional Topic 1-USES operator

The USES operator is a powerful tool that can be used to save and restore registers at the beginning and end of a procedure.

However, it should not be used when declaring procedures that access their stack parameters using constant offsets such as [ebp + 8].

The following MySub1 procedure employs the USES operator to save and restore ECX and EDX:

```
1604 MySub1 PROC USES ecx edx
1605 ret
1606 MySub1 ENDP
```

The following code is generated by MASM when it assembles MySub1:

```
1610 push ecx
1611 push edx
1612 pop edx
1613 pop ecx
1614 ret
```

Suppose we combine USES with a stack parameter, as does the following MySub2 procedure. Its parameter is expected to be located on the stack at EBP+8:

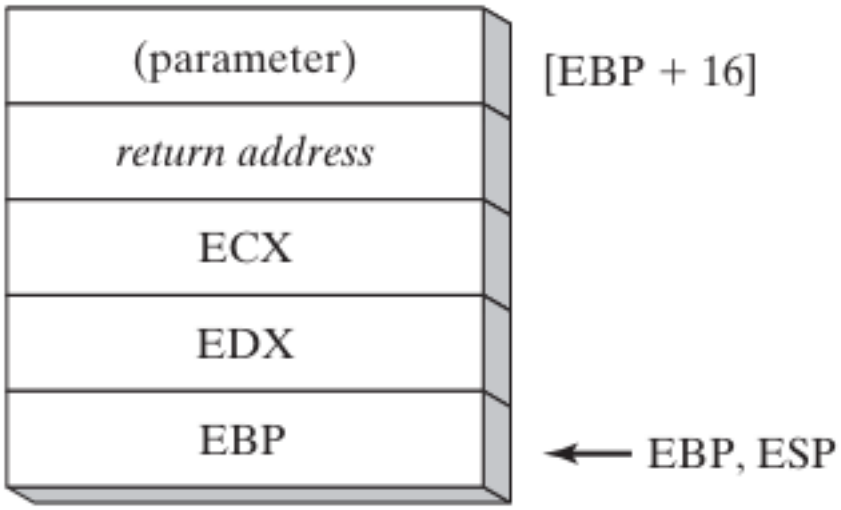
```
1620 MySub2 PROC USES ecx edx
1621 push ebp
1622 mov ebp,esp
1623 mov eax,[ebp+8]
1624 ; this is wrong!
1625 pop ebp
1626 ret 4
1627 MySub2 ENDP
```

Here is the corresponding code generated by MASM for MySub2:

```
1630 push ecx
1631 push edx
1632 push ebp
1633 mov ebp,esp
1634 mov eax,dword ptr [ebp+8]
1635 pop ebp
1636 pop edx
1637 pop ecx
1638 ret 4
```

An error results because the assembler inserted the PUSH instructions for ECX and EDX at the beginning of the procedure, altering the offset of the stack parameter.

Figure 8-6 below shows how the stack parameter must now be referenced as [EBP+16]. USES modifies the stack before saving EBP, which corrupts the standard prologue code commonly used for subroutines.



This is why it is important to avoid using the USES operator when declaring procedures that access their stack parameters using constant offsets.

If you need to save and restore registers in such a procedure, you can use the PUSH and POP instructions explicitly.

Here is a more in-depth explanation of why the USES operator causes problems in this case:
When a procedure is called, the caller pushes the procedure's arguments onto the stack.

The procedure then saves its caller-saved registers (EBP, ESI, EDI, and EBX) onto the stack. The procedure's base pointer (EBP) is set to point to the top of the stack frame.

The USES operator tells the assembler to save and restore the specified registers at the beginning and end of the procedure.

When the USES operator is used in a procedure that accesses its stack parameters using constant offsets, the assembler inserts the PUSH and POP instructions for the specified registers at the beginning and end of the procedure.

This corrupts the standard prologue code commonly used for subroutines, which relies on the stack pointer (ESP) to be pointing to the top of the stack frame.

In the example of MySub2, the USES operator is used to save and restore ECX and EDX. When MySub2 is called, its argument is pushed onto the stack.

The USES operator then causes the assembler to push ECX and EDX onto the stack. This corrupts the stack frame, because the stack pointer is now pointing to the wrong location.

To avoid this problem, you should not use the USES operator in procedures that access their stack parameters using constant offsets.

If you need to save and restore registers in such a procedure, you can use the PUSH and POP instructions explicitly.