

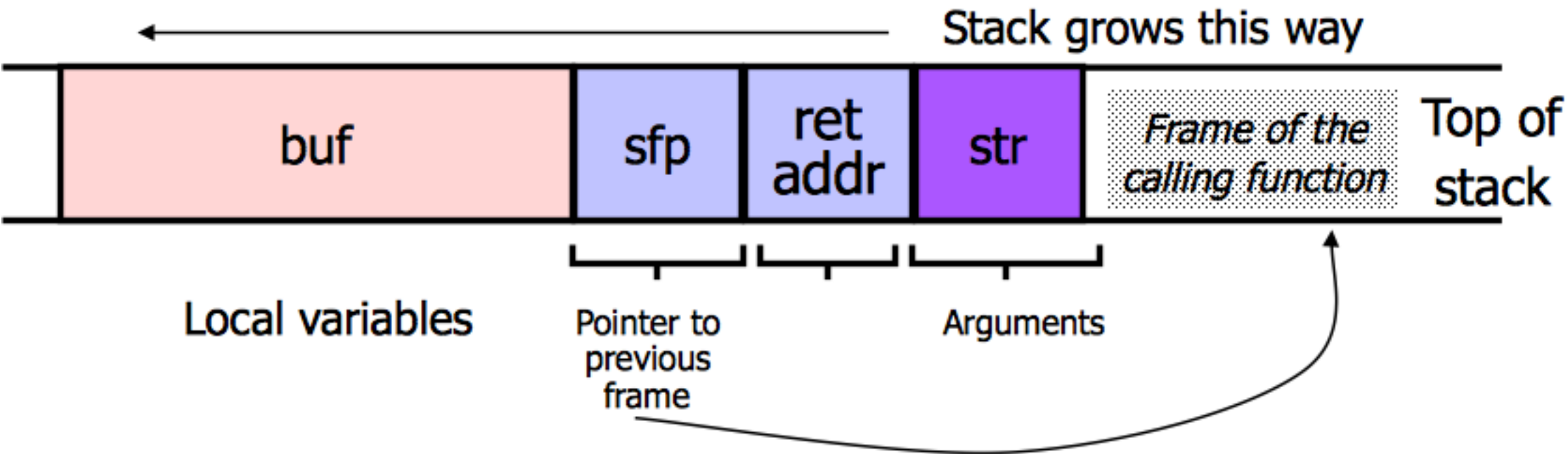
stackexchange



Allocate local buffer
(126 bytes in the stack)



Copy argument into local buffer

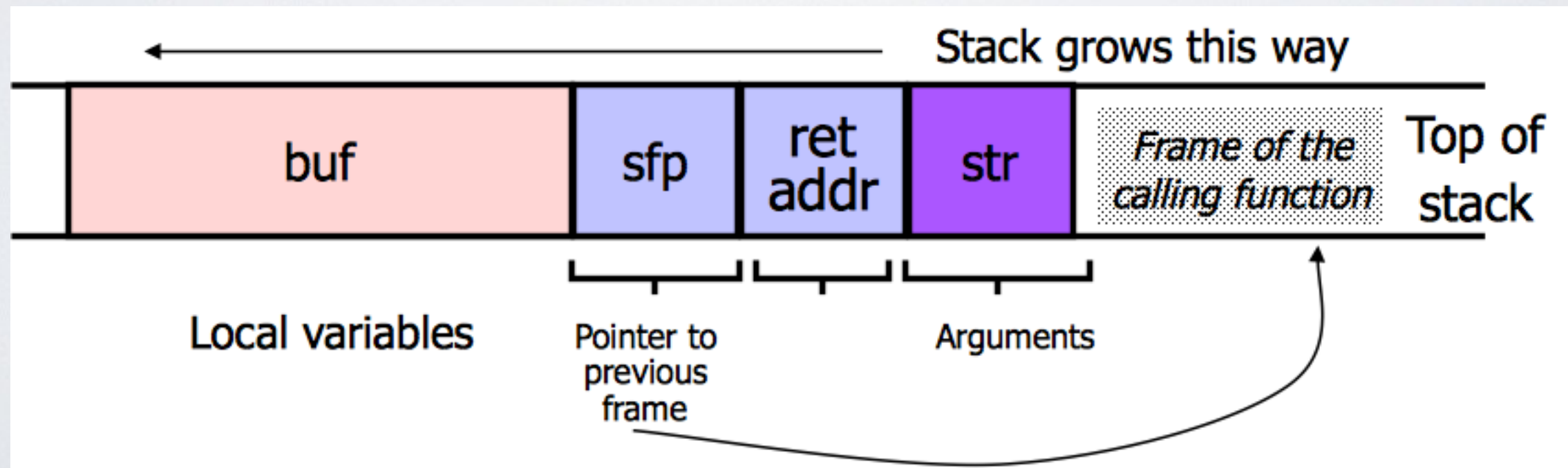


```
void func(char *str) {  
    char buf[126];  
    strcpy(buf, str);  
}
```

Stack execution

```
void func(char *str) {  
    char buf[126];  
    strcpy(buf, str);  
}
```

Copy argument into local buffer



What if the buffer is overstuffed?

strcpy **does not check** whether the string at *str contains fewer than 126 characters ...

