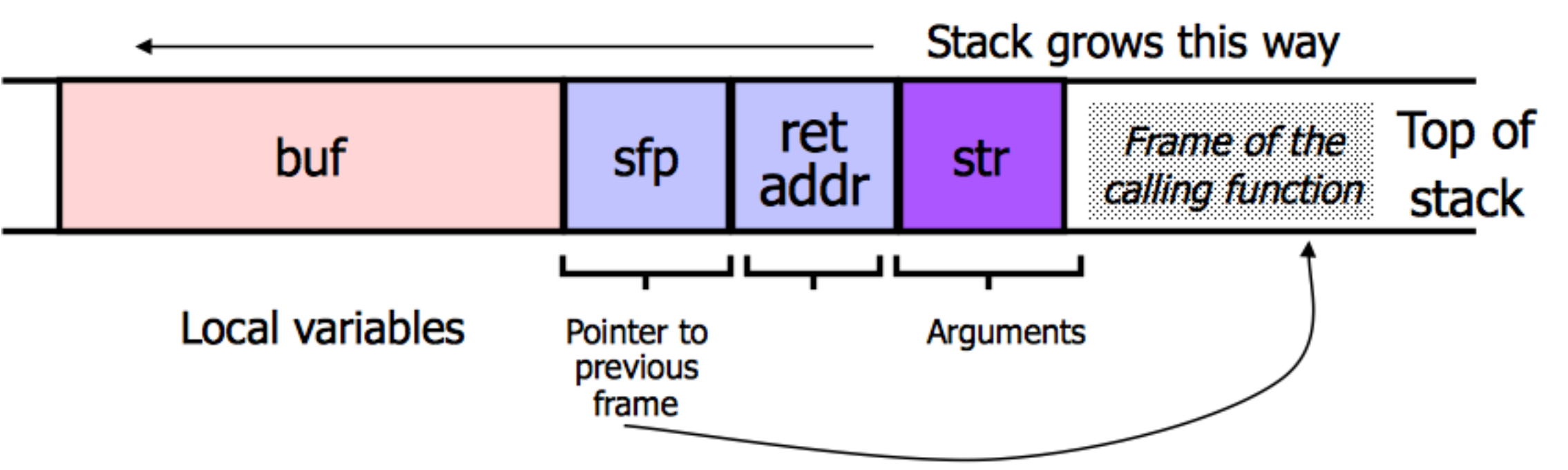
Stack execution


Allocate local buffer
(126 bytes in the stack)


Copy argument into local buffer

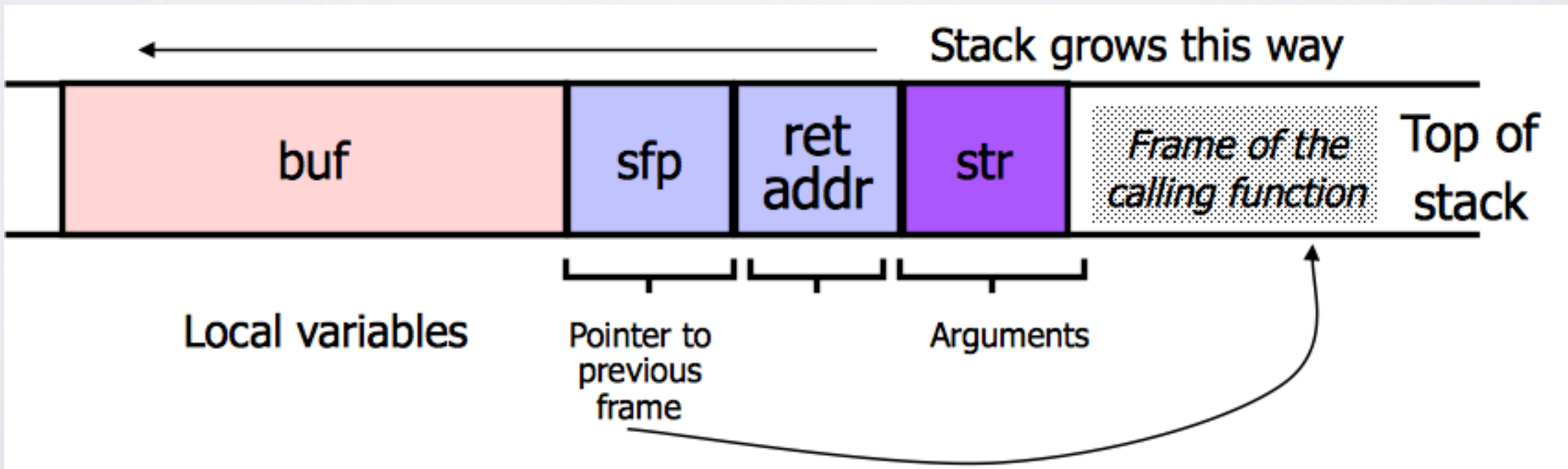

Stack grows this way
buf
sfp
ret addr
str
Frame of the calling function
Top of stack
Local variables
Pointer to previous frame
Arguments

```
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 ...