

Chapter 1

Operating system interfaces

The job of an operating system is to share a computer among multiple programs and to provide a more useful set of services than the hardware alone supports. An operating system manages and abstracts the low-level hardware, so that, for example, a word processor need not concern itself with which type of disk hardware is being used. An operating system shares the hardware among multiple programs so that they run (or appear to run) at the same time. Finally, operating systems provide controlled ways for programs to interact, so that they can share data or work together.

An operating system provides services to user programs through an interface. Designing a good interface turns out to be difficult. On the one hand, we would like the interface to be simple and narrow because that makes it easier to get the implementation right. On the other hand, we may be tempted to offer many sophisticated features to applications. The trick in resolving this tension is to design interfaces that rely on a few mechanisms that can be combined to provide much generality.

This book uses a single operating system as a concrete example to illustrate operating system concepts. That operating system, xv6, provides the basic interfaces introduced by Ken Thompson and Dennis Ritchie’s Unix operating system [17], as well as mimicking Unix’s internal design. Unix provides a narrow interface whose mechanisms combine well, offering a surprising degree of generality. This interface has been so successful that modern operating systems—BSD, Linux, macOS, Solaris, and even, to a lesser extent, Microsoft Windows—have Unix-like interfaces. Understanding xv6 is a good start toward understanding any of these systems and many others.

As Figure 1.1 shows, xv6 takes the traditional form of a *kernel*, a special program that provides services to running programs. Each running program, called a *process*, has memory containing instructions, data, and a stack. The instructions implement the program’s computation. The data are the variables on which the computation acts. The stack organizes the program’s procedure calls. A given computer typically has many processes but only a single kernel.

When a process needs to invoke a kernel service, it invokes a *system call*, one of the calls in the operating system’s interface. The system call enters the kernel; the kernel performs the service and returns. Thus a process alternates between executing in *user space* and *kernel space*.

As described in detail in subsequent chapters, the kernel uses the hardware protection mechanisms provided by a CPU¹ to ensure that each process executing in user space can access only

¹This text generally refers to the hardware element that executes a computation with the term *CPU*, an acronym

- a. Kernel is a program just like user programs
- b. User programs do not have privilege to do certain task so they use System Calls (known as Interface) to request Kernel to do those tasks

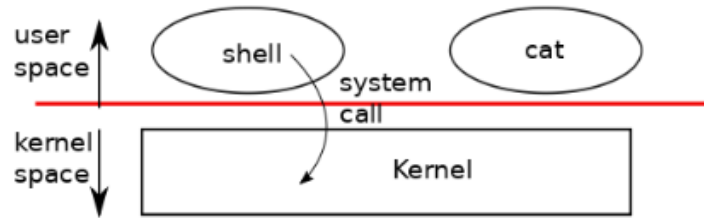


Figure 1.1: A kernel and two user processes.

What does Kernel offer to user programs?

- a. Processes
- b. Memory
- c. File Descriptors
- d. Pipes
- e. Filesystem

Shells in Ubuntu & XV6

```
mark@linux-desktop: /tmp/tutorial
File Edit View Search Terminal Help
mark@linux-desktop:~$ mkdir /tmp/tutorial
mark@linux-desktop:~$ cd /tmp/tutorial
mark@linux-desktop:/tmp/tutorial$ mkdir dir1 dir2 dir3
mark@linux-desktop:/tmp/tutorial$ mkdir
mkdir: missing operand
Try 'mkdir --help' for more information.
mark@linux-desktop:/tmp/tutorial$ cd /etc ~/Desktop
bash: cd: too many arguments
mark@linux-desktop:/tmp/tutorial$ ls
dir1 dir2 dir3
mark@linux-desktop:/tmp/tutorial$
```

```
salman@salman-ubuntu: ~/xv6-riscv
salman@salman-ubuntu:~$ cd xv6-riscv/
salman@salman-ubuntu:~/xv6-riscv$ make qemu
qemu-system-riscv64 -machine virt -bios none -kernel kernel/kernel -m 128M -smp
3 -nographic -global virtio-mmio.force-legacy=false -drive file=fs.img,if=none,f
ormat=raw,id=x0 -device virtio-blk-device,drive=x0,bus=virtio-mmio-bus.0

xv6 kernel is booting
hart 1 starting
hart 2 starting
init: starting sh
$
```

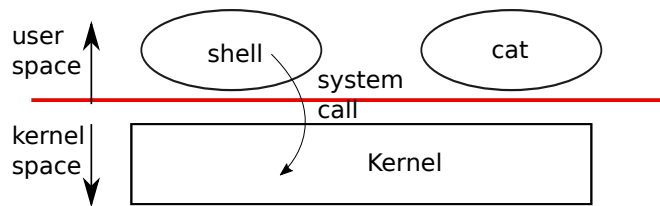


Figure 1.1: A kernel and two user processes.

its own memory. The kernel executes with the hardware privileges required to implement these protections; user programs execute without those privileges. When a user program invokes a system call, the hardware raises the privilege level and starts executing a pre-arranged function in the kernel.

The collection of system calls that a kernel provides is the interface that user programs see. The xv6 kernel provides a subset of the services and system calls that Unix kernels traditionally offer. Figure 1.2 lists all of xv6’s system calls.

The rest of this chapter outlines xv6’s services—processes, memory, file descriptors, pipes, and a file system—and illustrates them with code snippets and discussions of how the *shell*, Unix’s command-line user interface, uses them. The shell’s use of system calls illustrates how carefully they have been designed.

The shell is an ordinary program that reads commands from the user and executes them. The fact that the shell is a user program, and not part of the kernel, illustrates the power of the system call interface: there is nothing special about the shell. It also means that the shell is easy to replace; as a result, modern Unix systems have a variety of shells to choose from, each with its own user interface and scripting features. The xv6 shell is a simple implementation of the essence of the Unix Bourne shell. Its implementation can be found at (user/sh.c:1).

1.1 Processes and memory

An xv6 process consists of user-space memory (instructions, data, and stack) and per-process state private to the kernel. Xv6 *time-shares* processes: it transparently switches the available CPUs among the set of processes waiting to execute. When a process is not executing, xv6 saves the process’s CPU registers, restoring them when it next runs the process. The kernel associates a process identifier, or `PID`, with each process.

A process may create a new process using the `fork` system call. `fork` gives the new process an exact copy of the calling process’s memory, both instructions and data. `fork` returns in both the original and new processes. In the original process, `fork` returns the new process’s `PID`. In the new process, `fork` returns zero. The original and new processes are often called the *parent* and *child*.

for central processing unit. Other documentation (e.g., the RISC-V specification) also uses the words processor, core, and hart instead of CPU.

Virtual user address spaces are created when an executable file is run

User Address Space (Virtual)

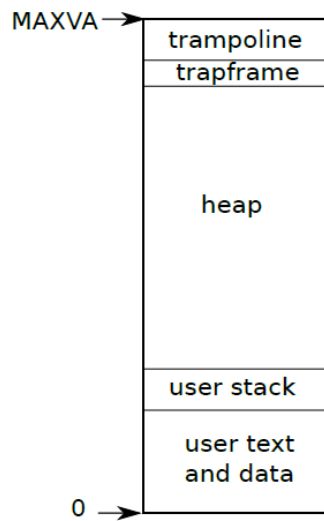


Figure 2.3: Layout of a process's virtual address space

Kernel Address Space (Virtual)

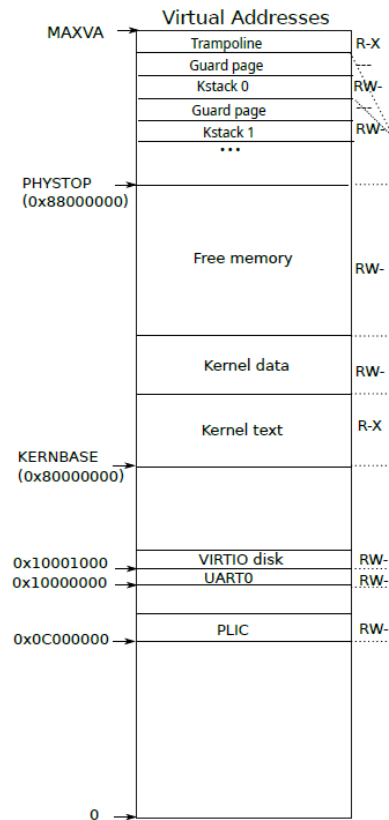


Figure 3.3: On the left, xv6's kernel address space.

Fork system call replicates a user address spaces but with a new process identifier

System call	Description
<code>int fork()</code>	Create a process, return child's PID.
<code>int exit(int status)</code>	Terminate the current process; status reported to <code>wait()</code> . No return.
<code>int wait(int *status)</code>	Wait for a child to exit; exit status in <code>*status</code> ; returns child PID.
<code>int kill(int pid)</code>	Terminate process PID. Returns 0, or -1 for error.
<code>int getpid()</code>	Return the current process's PID.
<code>int sleep(int n)</code>	Pause for <code>n</code> clock ticks.
<code>int exec(char *file, char *argv[])</code>	Load a file and execute it with arguments; only returns if error.
<code>char *sbrk(int n)</code>	Grow process's memory by <code>n</code> bytes. Returns start of new memory.
<code>int open(char *file, int flags)</code>	Open a file; flags indicate read/write; returns an fd (file descriptor).
<code>int write(int fd, char *buf, int n)</code>	Write <code>n</code> bytes from <code>buf</code> to file descriptor <code>fd</code> ; returns <code>n</code> .
<code>int read(int fd, char *buf, int n)</code>	Read <code>n</code> bytes into <code>buf</code> ; returns number read; or 0 if end of file.
<code>int close(int fd)</code>	Release open file <code>fd</code> .
<code>int dup(int fd)</code>	Return a new file descriptor referring to the same file as <code>fd</code> .
<code>int pipe(int p[])</code>	Create a pipe, put read/write file descriptors in <code>p[0]</code> and <code>p[1]</code> .
<code>int chdir(char *dir)</code>	Change the current directory.
<code>int mkdir(char *dir)</code>	Create a new directory.
<code>int mknod(char *file, int, int)</code>	Create a device file.
<code>int fstat(int fd, struct stat *st)</code>	Place info about an open file into <code>*st</code> .
<code>int stat(char *file, struct stat *st)</code>	Place info about a named file into <code>*st</code> .
<code>int link(char *file1, char *file2)</code>	Create another name (file2) for the file file1.
<code>int unlink(char *file)</code>	Remove a file.

Figure 1.2: Xv6 system calls. If not otherwise stated, these calls return 0 for no error, and -1 if there's an error.

For example, consider the following program fragment written in the C programming language [7]:

```
int pid = fork();
if(pid > 0){
    printf("parent: child=%d\n", pid);
    pid = wait((int *) 0);
    printf("child %d is done\n", pid);
} else if(pid == 0){
    printf("child: exiting\n");
    exit(0);
} else {
    printf("fork error\n");
}
```

The `exit` system call causes the calling process to stop executing and to release resources such as memory and open files. Exit takes an integer status argument, conventionally 0 to indicate success and 1 to indicate failure. The `wait` system call returns the PID of an exited (or killed) child of

Fork & Wait System Calls

```

1 #include "kernel/fcntl.h"
2 #include "kernel/types.h"
3 #include "user/user.h"
4
5
6
7 int main() {
8     int pid = fork();
9     if (pid > 0) {
10         printf("parent: child=%d\n", pid);
11         pid = wait((int *) 0);
12         printf("child %d is done\n", pid);
13     } else if (pid == 0) {
14         printf("child: exiting\n");
15         exit(0);
16     } else {
17         printf("fork error\n");
18     }
19     return 0;
20 }
21

```

```

Open ▾ [n]
1 #include "kernel/types.h"
2 #include "user/user.h"
3
4
5
6 int main(void) {
7     int pld=fork();
8     if (pld>0){
9         //printf("parent: child=%d\n",pld);
10        pld=wait((int *)0);
11        printf("parent: child=%d\n",pld);
12        printf("child %d is done\n",pld);
13    }
14    else if(pld==0){
15        printf("child:exiting\n");
16        exit(0);
17    }
18    else{
19        printf("fork error\n");
20    }
21    return 0;
22 }

```

```

xv6 kernel is booting
hart 1 starting
hart 2 starting
init: starting sh
$ mytest
child:exiting
parent: child=4
child 4 is done
$

```

```

salman@salman-ubuntu:~/xv6-riscv$ make qemu
qemu-system-riscv64 -machine virt -bios none
virtio-blk-device,drive=x0,bus=virtio-mmio-b

xv6 kernel is booting

hart 2 starting
hart 1 starting
init: starting sh
$ myprog1
pcahriledn:t : ecxhiiltidn=g4

child 4 is done
$

```

```

#include "kernel/fcntl.h"
#include "kernel/types.h"
#include "user/user.h"

int main(){
    int p = fork();
    if (p>0){
        wait((int *) 0);
        printf("Parent PID as an individual process=%d, Parent identification after fork = %d \n",getpid(),p);
    }
    else if (p==0){
        printf("Child PID as an individual process=%d, Child identification after fork = %d \n",getpid(),p);
        exit(0);
    }
    else
        printf("fork fail");
    return 0;
}

```

xv6 kernel is booting

hart 2 starting
hart 1 starting
init: starting sh
\$ myprog1

Child PID as an individual process=4, Child identification after fork = 0
Parent PID as an individual process=3, Parent identification after fork = 4
\$ parent individual pid independant

child identification to always 0

parent ki apni its not connected to any child indiudal pid= parent identifiacion wali pid

the current process and copies the exit status of the child to the address passed to `wait`; if none of the caller's children has exited, `wait` waits for one to do so. If the caller has no children, `wait` immediately returns -1. If the parent doesn't care about the exit status of a child, it can pass a 0 address to `wait`.

In the example, the output lines

```
parent: child=1234
child: exiting
```

might come out in either order (or even intermixed), depending on whether the parent or child gets to its `printf` call first. After the child exits, the parent's `wait` returns, causing the parent to print

```
parent: child 1234 is done
```

Although the child has the same memory contents as the parent initially, **the parent and child are executing with separate memory and separate registers: changing a variable in one does not affect the other.** For example, when the return value of `wait` is stored into `pid` in the parent process, it doesn't change the variable `pid` in the child. The value of `pid` in the child will still be zero.

The `exec` system call replaces the calling process's memory with a new memory image loaded from a file stored in the file system. The file must have a particular format, which specifies which part of the file holds instructions, which part is data, at which instruction to start, etc. Xv6 uses the ELF format, which Chapter 3 discusses in more detail. Usually the file is the result of compiling a program's source code. **When `exec` succeeds, it does not return to the calling program;** instead, the instructions loaded from the file start executing at the entry point declared in the ELF header. `exec` takes two arguments: the name of the file containing the executable and an array of string arguments. For example:

```
char *argv[3];

argv[0] = "echo";
argv[1] = "hello";
argv[2] = 0;
exec("/bin/echo", argv);
printf("exec error\n");
```

This fragment replaces the calling program with an instance of the program `/bin/echo` running with the argument list `echo hello`. Most programs ignore the first element of the argument array, which is conventionally the name of the program.

The xv6 shell uses the above calls to run programs on behalf of users. The main structure of the shell is simple; see `main` (`user/sh.c:146`). The main loop reads a line of input from the user with `getcmd`. Then it calls `fork`, which creates a copy of the shell process. The parent calls `wait`, while the child runs the command. For example, if the user had typed “`echo hello`” to the shell, `runcmd` would have been called with “`echo hello`” as the argument. `runcmd` (`user/sh.c:55`) runs the actual command. For “`echo hello`”, it would call `exec` (`user/sh.c:79`). If `exec` succeeds then the child will execute instructions from `echo` instead of `runcmd`. At some point `echo` will call `exit`, which will cause the parent to return from `wait` in `main` (`user/sh.c:146`).

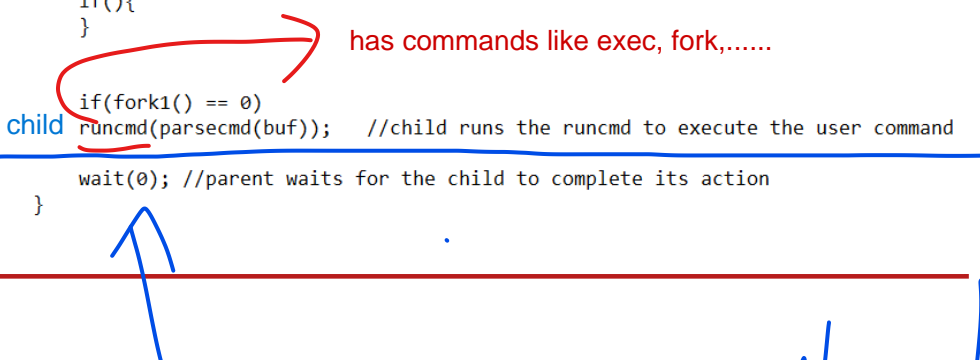
How a command is executed from the shell?

--Remember that shell is itself a process

```
main()
{
    while(getcmd(buf, sizeof(buf)) >= 0)    //getcmd reads the user command from buf
    {
        if(){
        }

        if(fork1() == 0)
        child runcmd(parsecmd(buf));    //child runs the runcmd to execute the user command

        wait(0); //parent waits for the child to complete its action
    }
}
```



Parent me when $fork1 > 0$

see how shell me bhe forking huvi we parent waits for child
and child me runcmd wich parses the command gaven by user and runs it

Getting user command

xv6-riscv / user / sh.c in riscv

Edit Preview

```
134 int
135 getcmd(char *buf, int nbuf)
136 {
137     write(2, "$ ", 2); // An error message $ is written on the file descriptor 2
138     memset(buf, 0, nbuf); // Sets all the character bytes of buf as 0.
139     gets(buf, nbuf); // Stores the user command into the buffer buf
140     if(buf[0] == 0) // EOF
141         return -1;
142     return 0;
143 }
144 int
145 main(void)
146 {
147     static char buf[100]; //A 100-character buffer buf declared
148     int fd; //An integer file descriptor fd declared
149
150     // Ensure that three file descriptors are open.
151     while((fd = open("console", O_RDWR)) >= 0){
152         if(fd >= 3){
153             close(fd);
154             break;
155         }
156     }
157     // Read and run input commands.
158     while(getcmd(buf, sizeof(buf)) >= 0){ // getcmd() receives the user command as a string of characters.
159         // getcmd() provides buf size and expects the filled buf
160         if(buf[0] == 'c' && buf[1] == 'd' && buf[2] == ' '){
161             // Chdir must be called by the parent, not the child.
162             buf[strlen(buf)-1] = 0; // chop \n
163             if(chdir(buf+3) < 0)
164                 fprintf(2, "cannot cd %s\n", buf+3);
165             continue;
166         }
167         if(fork1() == 0)
168             runcmd(parsecmd(buf));
169         wait(0);
170     }
171     exit(0);
172 }
```

Running user command

xv6-riscv / user / sh.c in riscv

Edit Preview

```
56 // Execute cmd. Never returns.
57 void
58 runcmd(struct cmd *cmd)
59 {
60     int p[2];
61     struct backcmd *bcmd;
62     struct execcmd *ecmd;
63     struct listcmd *lcmd;
64     struct pipecmd *pcmd;
65     struct redircmd *rcmd;
66
67     if(cmd == 0)
68         exit(1);
69
70     switch(cmd->type){
71     default:
72         panic("runcmd");
73
74     case EXEC:
75         ecmd = (struct execcmd*)cmd;
76         if(ecmd->argv[0] == 0)
77             exit(1);
78         exec(ecmd->argv[0], ecmd->argv);
79         fprintf(2, "exec %s failed\n", ecmd->argv[0]);
80         break;
81
82     case REDIR:
83         rcmd = (struct redircmd*)cmd;
84         close(rcmd->fd);
85         if(open(rcmd->file, rcmd->mode) < 0){
86             fprintf(2, "open %s failed\n", rcmd->file);
87             exit(1);
88         }
89         runcmd(rcmd->cmd);
90         break;
91 }
```

You might wonder why `fork` and `exec` are not combined in a single call; we will see later that the shell exploits the separation in its implementation of I/O redirection. To avoid the wastefulness of creating a duplicate process and then immediately replacing it (with `exec`), operating kernels optimize the implementation of `fork` for this use case by using virtual memory techniques such as copy-on-write (see Section 4.6).

Xv6 allocates most user-space memory implicitly: `fork` allocates the memory required for the child's copy of the parent's memory, and `exec` allocates enough memory to hold the executable file. A process that needs more memory at run-time (perhaps for `malloc`) can call `sbrk(n)` to grow its data memory by `n` bytes; `sbrk` returns the location of the new memory.

1.2 I/O and File descriptors

A *file descriptor* is a small integer representing a kernel-managed object that a process may read from or write to. A process may obtain a file descriptor by opening a file, directory, or device, or by creating a pipe, or by duplicating an existing descriptor. For simplicity we'll often refer to the object a file descriptor refers to as a "file"; the file descriptor interface abstracts away the differences between files, pipes, and devices, making them all look like streams of bytes. We'll refer to input and output as *I/O*.

Internally, the xv6 kernel uses the file descriptor as an index into a per-process table, so that every process has a private space of file descriptors starting at zero. By convention, a process reads from file descriptor 0 (standard input), writes output to file descriptor 1 (standard output), and writes error messages to file descriptor 2 (standard error). As we will see, the shell exploits the convention to implement I/O redirection and pipelines. The shell ensures that it always has three file descriptors open (`user/sh.c:152`), which are by default file descriptors for the console.

The `read` and `write` system calls read bytes from and write bytes to open files named by file descriptors. The call `read(fd, buf, n)` reads at most `n` bytes from the file descriptor `fd`, copies them into `buf`, and returns the number of bytes read. Each file descriptor that refers to a file has an offset associated with it. `read` reads data from the current file offset and then advances that offset by the number of bytes read: a subsequent `read` will return the bytes following the ones returned by the first `read`. When there are no more bytes to read, `read` returns zero to indicate the end of the file.

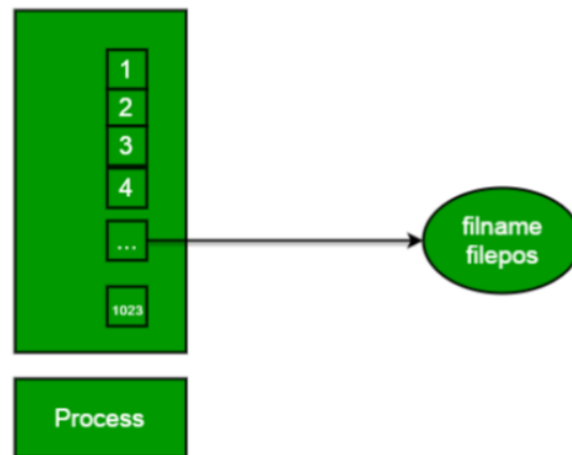
The call `write(fd, buf, n)` writes `n` bytes from `buf` to the file descriptor `fd` and returns the number of bytes written. Fewer than `n` bytes are written only when an error occurs. Like `read`, `write` writes data at the current file offset and then advances that offset by the number of bytes written: each `write` picks up where the previous one left off.

The following program fragment (which forms the essence of the program `cat`) copies data from its standard input to its standard output. If an error occurs, it writes a message to the standard error.

```
char buf[512];
int n;

for(;;){
```

File Descriptors: When any process starts, then that process file descriptors table's fd(file descriptor) 0, 1, 2 open automatically. 0 for standard input, 1 for standard output, and 2 for standard error display on the shell's console.



A file descriptor is a small integer representing a kernel-managed object that a process may read from or write to. A process may obtain a file descriptor by opening a file, directory, or device, or by creating pipe, or by duplicating an existing file descriptor.

`write(fd,buf,n);` //write to fd picking data from buf with n bytes at a time
`read (fd,buf,n);` //read from fd sending to buf with n bytes at a time

Note: An offset is incremented in each read call to n+1 until the whole file is read.

I/O Redirection

Children being able to reassign the file descriptors chosen by a parent process.

Parent process file descriptor assignments are unchanged by I/O redirection.

```
1 char *argv[2]; //pointer to character array
2
3 argv[0] = "cat"; //first element of array is a program name
4 argv[1] = 0;     //last element is always a null to signal the end of user command
5
6 if(fork() == 0) //child process
7 {
8     close(0);    //Release open file fd. child closes the file descriptor 0 from parent process
9     open("input.txt", O_RDONLY); //Load a file and execute it with arguments; only returns if error.
                                //child assigns this fd=0 to input.txt file.
10    exec("cat", argv); //Open a file; flags indicate read/write; returns an fd (file descriptor).
11 }
```

```

n = read(0, buf, sizeof buf);
if(n == 0)
    break;
if(n < 0){
    fprintf(2, "read error\n");
    exit(1);
}
if(write(1, buf, n) != n){
    fprintf(2, "write error\n");
    exit(1);
}
}

```

The important thing to note in the code fragment is that `cat` doesn't know whether it is reading from a file, console, or a pipe. Similarly `cat` doesn't know whether it is printing to a console, a file, or whatever. The use of file descriptors and the convention that file descriptor 0 is input and file descriptor 1 is output allows a simple implementation of `cat`.

The `close` system call releases a file descriptor, making it free for reuse by a future `open`, `pipe`, or `dup` system call (see below). A newly allocated file descriptor is always the lowest-numbered unused descriptor of the current process.

File descriptors and `fork` interact to make I/O redirection easy to implement. `fork` copies the parent's file descriptor table along with its memory, so that the child starts with exactly the same open files as the parent. The system call `exec` replaces the calling process's memory but preserves its file table. This behavior allows the shell to implement *I/O redirection* by forking, re-opening chosen file descriptors in the child, and then calling `exec` to run the new program. Here is a simplified version of the code a shell runs for the command `cat < input.txt`:


```

char *argv[2];

argv[0] = "cat";
argv[1] = 0;
if(fork() == 0) {
    close(0);
    open("input.txt", O_RDONLY);
    exec("cat", argv);
}

```

fork me fd table bhe copy hota along with memory



After the child closes file descriptor 0, `open` is guaranteed to use that file descriptor for the newly opened `input.txt`: 0 will be the smallest available file descriptor. `cat` then executes with file descriptor 0 (standard input) referring to `input.txt`. The parent process's file descriptors are not changed by this sequence, since it modifies only the child's descriptors.

The code for I/O redirection in the xv6 shell works in exactly this way (`user/sh.c:83`). Recall that at this point in the code the shell has already forked the child shell and that `runcmd` will call `exec` to load the new program.

The second argument to `open` consists of a set of flags, expressed as bits, that control what `open` does. The possible values are defined in the file control (`fcntl`) header (`kernel/fcntl.h:1-5`):

`O_RDONLY`, `O_WRONLY`, `O_RDWR`, `O_CREATE`, and `O_TRUNC`, which instruct `open` to open the file for reading, or for writing, or for both reading and writing, to create the file if it doesn't exist, and to truncate the file to zero length.

Now it should be clear why it is helpful that `fork` and `exec` are separate calls: between the two, the shell has a chance to redirect the child's I/O without disturbing the I/O setup of the main shell. One could instead imagine a hypothetical combined `forkexec` system call, but the options for doing I/O redirection with such a call seem awkward. The shell could modify its own I/O setup before calling `forkexec` (and then un-do those modifications); or `forkexec` could take instructions for I/O redirection as arguments; or (least attractively) every program like `cat` could be taught to do its own I/O redirection.

Although `fork` copies the file descriptor table, each underlying file offset is shared between parent and child. Consider this example:

```
if(fork() == 0) {
    write(1, "hello ", 6);
    exit(0);
} else {
    wait(0);
    write(1, "world\n", 6);
}
```

At the end of this fragment, the file attached to file descriptor 1 will contain the data `hello world`. The `write` in the parent (which, thanks to `wait`, runs only after the child is done) picks up where the child's `write` left off. This behavior helps produce sequential output from sequences of shell commands, like `(echo hello; echo world) > output.txt`.

The `dup` system call duplicates an existing file descriptor, returning a new one that refers to the same underlying I/O object. Both file descriptors share an offset, just as the file descriptors duplicated by `fork` do. This is another way to write `hello world` into a file:

```
fd = dup(1);
write(1, "hello ", 6);
write(fd, "world\n", 6);
```

Two file descriptors share an offset if they were derived from the same original file descriptor by a sequence of `fork` and `dup` calls. Otherwise file descriptors do not share offsets, even if they resulted from `open` calls for the same file. `dup` allows shells to implement commands like this: `ls existing-file non-existing-file > tmp1 2>&1`. The `2>&1` tells the shell to give the command a file descriptor 2 that is a duplicate of descriptor 1. Both the name of the existing file and the error message for the non-existing file will show up in the file `tmp1`. The xv6 shell doesn't support I/O redirection for the error file descriptor, but now you know how to implement it.

File descriptors are a powerful abstraction, because they hide the details of what they are connected to: a process writing to file descriptor 1 may be writing to a file, to a device like the console, or to a pipe.

pipe() System call

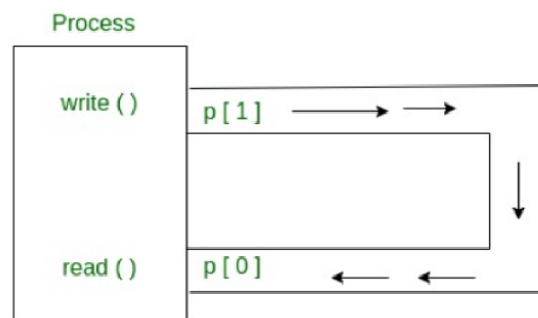
Last Updated : 15 Sep, 2023



Prerequisite : [I/O System calls](#)

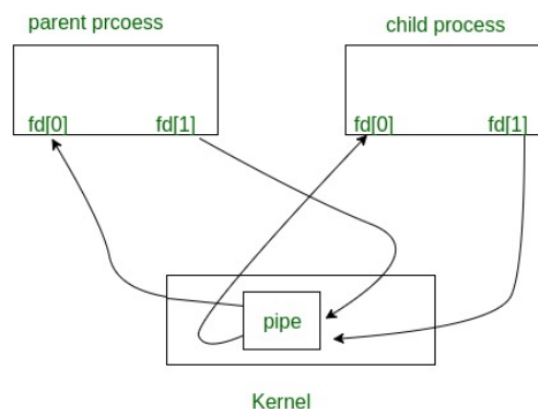
Conceptually, a pipe is a connection between two processes, such that the standard output from one process becomes the standard input of the other process. In UNIX Operating System, Pipes are useful for communication between related processes(inter-process communication).

- Pipe is one-way communication only i.e we can use a pipe such that One process write to the pipe, and the other process reads from the pipe. It opens a pipe, which is an area of main memory that is treated as a **“virtual file”**.
- The pipe can be used by the creating process, as well as all its child processes, for reading and writing. One process can write to this “virtual file” or pipe and another related process can read from it.
- If a process tries to read before something is written to the pipe, the process is suspended until something is written.
- The pipe system call finds the first two available positions in the process's open file table and allocates them for the read and write ends of the pipe.



Parent and child sharing a pipe

When we use [fork](#) in any process, file descriptors remain open across child process and also parent process. If we call fork after creating a pipe, then the parent and child can communicate via the pipe.



```
// C program to illustrate
// pipe system call in C
#include <stdio.h>
#include <unistd.h>
#define MSGSIZE 16
char* msg1 = "hello, world #1";
char* msg2 = "hello, world #2";
char* msg3 = "hello, world #3";

int main()
{
    char inbuf[MSGSIZE];
    int p[2], i;

    if (pipe(p) < 0)
        exit(1);

    /* continued */
    /* write pipe */

    write(p[1], msg1, MSGSIZE);
    write(p[1], msg2, MSGSIZE);
    write(p[1], msg3, MSGSIZE);

    for (i = 0; i < 3; i++) {
        /* read pipe */
        read(p[0], inbuf, MSGSIZE);
        printf("%s\n", inbuf);
    }
    return 0;
}
```

Output:

```
hello, world #1
hello, world #2
hello, world #3
```

```
// C program to illustrate
// pipe system call in C
// shared by Parent and Child
#include <stdio.h>
#include <unistd.h>
#define MSGSIZE 16
char* msg1 = "hello, world #1";
char* msg2 = "hello, world #2";
char* msg3 = "hello, world #3";

int main()
{
    char inbuf[MSGSIZE];
    int p[2], pid, nbytes;

    if (pipe(p) < 0)
        exit(1);

    /* continued */
    if ((pid = fork()) > 0) {
        write(p[1], msg1, MSGSIZE);
        write(p[1], msg2, MSGSIZE);
        write(p[1], msg3, MSGSIZE);

        // Adding this line will kam hogya writting ka so
        // not hang the program close fd with p[1]
        // close(p[1]);
        wait(NULL); // in xv6 it would be wait ( 0 )
    }

    else {
        // Adding this line will
        // not hang the program
        // close(p[1]);
        while ((nbytes = read(p[0], inbuf, MSGSIZE)) > 0)
            printf("%s\n", inbuf);
        if (nbytes != 0)
            exit(2);
        printf("Finished reading\n");
    }
    return 0;
}
```

Output:

```
hello world, #1
hello world, #2
hello world, #3
(hangs) //program does not terminate but hangs
```

Here, In this code After finishing reading/writing, both parent and child block instead of terminating the process and that's why program hangs. This happens because read system call gets as much data it requests or as much data as the pipe has, whichever is less.

Further Pipes & Filedescriptors

```
main.c // Online C compiler to run C program online
1 #include <stdio.h>
2 #include <stdlib.h>
3 #include <string.h>
4 #include <sys/types.h>
5 #include <sys/wait.h>
6 #include <unistd.h>
7
8
9- int main() {
10     int p[2];
11     pipe(p);
12- if(fork() == 0) {
13 //close(0);
14 printf("%d,%d,%d\n",dup(p[1]),dup(p[0]), p[0],p[1]);
15 write(p[1], "hello world\n", 12); // or write(dup(p[1]), "hello world\n", 12
    ); or write(4, "hello world\n", 12); or write(6, "hello world\n", 12);
16 exit(0);
17- } else {
18     wait(0);
19     char *buf[12];
20     read(p[0],buf,12); // or read(p[0],buf,12);
21     printf("%s",buf);
22 }
23 }
24 }
~c
```

Output

```
/tmp/JXdY9pcqr1.o
5,5,3,4
hello world

=== Code Execution Successful ===
```

```
main.c // Online C compiler to run C program online
1 #include <stdio.h>
2 #include <stdlib.h>
3 #include <string.h>
4 #include <sys/types.h>
5 #include <sys/wait.h>
6 #include <unistd.h>
7
8
9- int main() {
10     int p[2];
11     pipe(p);
12- if(fork() == 0) {
13 close(0); to add it also means scanf wont work usme se kuch read ni hoga
14 printf("%d,%d,%d,%d\n",dup(p[1]),dup(p[0]), p[0],p[1]);
15 write(p[1], "hello world\n", 12); // or write(dup(p[1]), "hello world\n", 12
    ); or write(4, "hello world\n", 12); or write(6, "hello world\n", 12);
16 exit(0);
17- } else {
18     wait(0);
19     char *buf[12];
20     read(p[0],buf,12); // or read(p[0],buf,12);
21     printf("%s",buf);
22 }
23 }
24 }
~c
```

Output

```
/tmp/3kbn0KVKEA.o
5,0,3,4
hello world

bqi number wali chiiz u already know

=== Code Execution Successful ===
```

```
main.c // Online C compiler to run C program online
1 #include <stdio.h>
2 #include <stdlib.h>
3 #include <string.h>
4 #include <sys/types.h>
5 #include <sys/wait.h>
6 #include <unistd.h>
7
8
9- int main() {
10     int p[2];
11     pipe(p);
12- if(fork() == 0) {
13 close(2);
14 printf("%d,%d,%d,%d\n",dup(p[1]),dup(p[0]), p[0],p[1]);
15 write(p[1], "hello world\n", 12); // or write(dup(p[1]), "hello world\n", 12
    ); or write(4, "hello world\n", 12); or write(6, "hello world\n", 12);
16 exit(0);
17- } else {
18     wait(0);
19     char *buf[12];
20     read(p[0],buf,12); // or read(p[0],buf,12);
21     printf("%s",buf);
22 }
23 }
24 }
~c
```

Output

```
/tmp/dnltJR2oG7.o
5,2,3,4
hello world

=== Code Execution Successful ===
```

```
main.c // Online C compiler to run C program online
1 #include <stdio.h>
2 #include <stdlib.h>
3 #include <string.h>
4 #include <sys/types.h>
5 #include <sys/wait.h>
6 #include <unistd.h>
7
8
9- int main() {
10     int p[2];
11     pipe(p);
12- if(fork() == 0) {
13 close(1);
14 printf("%d,%d,%d,%d,%d\n",dup(p[1]),dup(p[0]), p[0],p[1]);
15 write(p[1], "hello world\n", 12); // or write(dup(p[1]), "hello world\n", 12
    ); or write(4, "hello world\n", 12); or write(6, "hello world\n", 12);
16 exit(0);
17- } else {
18     wait(0);
19     char *buf[12];
20     read(p[0],buf,12); // or read(p[0],buf,12);
21     printf("%s",buf);
22 }
23 }
24 }
~c
```

Output

```
/tmp/MipVbJYfVh.o
hello world

=== Code Execution Successful ===

altho backend me
p0=3
p1=4
dup0=1
dup1=5

printf wont work u just closed fd=1 so print f (standard output ka hota)
```


1.3 Pipes

A *pipe* is a small kernel buffer exposed to processes as a pair of file descriptors, one for reading and one for writing. Writing data to one end of the pipe makes that data available for reading from the other end of the pipe. Pipes provide a way for processes to communicate.

The following example code runs the program `wc` with standard input connected to the read end of a pipe.

```
int p[2];
char *argv[2];

argv[0] = "wc";
argv[1] = 0;

pipe(p);
if(fork() == 0) {
    close(0); 0 closed so free
    dup(p[0]); assigned to 0
    close(p[0]);
    close(p[1]);
    exec("/bin/wc", argv);
} else {
    close(p[0]); 3 is free now
    write(p[1], "hello world\n", 12); 4 ke thru pipe pe written
    close(p[1]); 4 closed so free
}
```

The program calls `pipe`, which creates a new pipe and records the read and write file descriptors in the array `p`. After `fork`, both parent and child have file descriptors referring to the pipe. The child calls `close` and `dup` to make file descriptor zero refer to the read end of the pipe, closes the file descriptors in `p`, and calls `exec` to run `wc`. When `wc` reads from its standard input, it reads from the pipe. The parent closes the read side of the pipe, writes to the pipe, and then closes the write side.

If no data is available, a `read` on a pipe waits for either data to be written or for all file descriptors referring to the write end to be closed; in the latter case, `read` will return 0, just as if the end of a data file had been reached. The fact that `read` blocks until it is impossible for new data to arrive is one reason that it's important for the child to close the write end of the pipe before executing `wc` above: if one of `wc`'s file descriptors referred to the write end of the pipe, `wc` would never see end-of-file.

The xv6 shell implements pipelines such as `grep fork sh.c | wc -l` in a manner similar to the above code (user/sh.c:101). The child process creates a pipe to connect the left end of the pipeline with the right end. Then it calls `fork` and `runcmd` for the left end of the pipeline and `fork` and `runcmd` for the right end, and waits for both to finish. The right end of the pipeline may be a command that itself includes a pipe (e.g., `a | b | c`), which itself forks two new child processes (one for `b` and one for `c`). Thus, the shell may create a tree of processes. The leaves

of this tree are commands and the interior nodes are processes that wait until the left and right children complete.

Pipes may seem no more powerful than temporary files: the pipeline

```
echo hello world | wc
```

could be implemented without pipes as

```
echo hello world >/tmp/xyz; wc </tmp/xyz
```

clean themselves
large data askta
parallel execution of pipeline

Pipes have at least three advantages over temporary files in this situation. First, pipes automatically clean themselves up; with the file redirection, a shell would have to be careful to remove `/tmp/xyz` when done. Second, pipes can pass arbitrarily long streams of data, while file redirection requires enough free space on disk to store all the data. Third, pipes allow for parallel execution of pipeline stages, while the file approach requires the first program to finish before the second starts.

1.4 File system

The xv6 file system provides data files, which contain uninterpreted byte arrays, and directories, which contain named references to data files and other directories. The directories form a tree, starting at a special directory called the *root*. A *path* like `/a/b/c` refers to the file or directory named `c` inside the directory named `b` inside the directory named `a` in the root directory `/`. Paths that don't begin with `/` are evaluated relative to the calling process's *current directory*, which can be changed with the `chdir` system call. Both these code fragments open the same file (assuming all the directories involved exist):

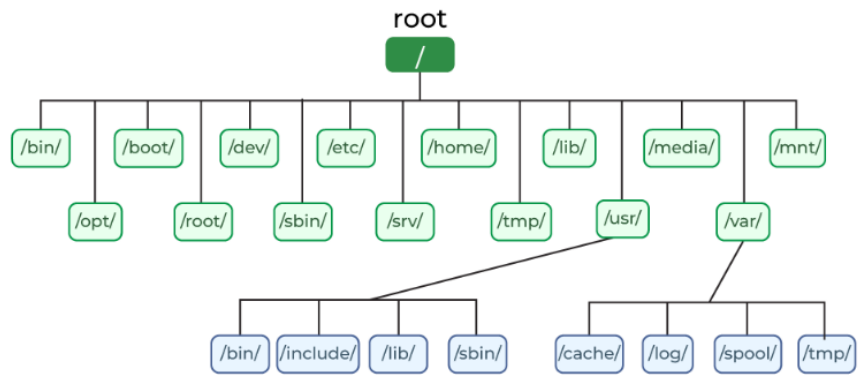
```
chdir("/a");  
chdir("b");  
open("c", O_RDONLY);  
  
open("/a/b/c", O_RDONLY);
```

The first fragment changes the process's current directory to `/a/b`; the second neither refers to nor changes the process's current directory.

There are system calls to create new files and directories: `mkdir` creates a new directory, `open` with the `O_CREATE` flag creates a new data file, and `mknod` creates a new device file. This example illustrates all three:

```
mkdir("/dir");  
fd = open("/dir/file", O_CREATE|O_WRONLY);  
close(fd);  
mknod("/console", 1, 1);
```

`mknod` creates a special file that refers to a device. Associated with a device file are the major and minor device numbers (the two arguments to `mknod`), which uniquely identify a kernel device. When a process later opens a device file, the kernel diverts `read` and `write` system calls to the kernel device implementation instead of passing them to the file system.



A file's name is distinct from the file itself; the same underlying file, called an *inode*, can have multiple names, called *links*. Each link consists of an entry in a directory; the entry contains a file name and a reference to an inode. An inode holds *metadata* about a file, including its type (file or directory or device), its length, the location of the file's content on disk, and the number of links to a file.

The `fstat` system call retrieves information from the inode that a file descriptor refers to. It fills in a `struct stat`, defined in `stat.h` (`kernel/stat.h`) as:

```
#define T_DIR      1    // Directory
#define T_FILE     2    // File
#define T_DEVICE   3    // Device

struct stat {
    int dev;        // File system's disk device
    uint ino;       // Inode number
    short type;     // Type of file
    short nlink;    // Number of links to file
    uint64 size;    // Size of file in bytes
};
```

The `link` system call creates another file system name referring to the same inode as an existing file. This fragment creates a new file named both `a` and `b`.

```
open("a", O_CREATE|O_WRONLY);
link("a", "b");
```

Reading from or writing to `a` is the same as reading from or writing to `b`. Each inode is identified by a unique *inode number*. After the code sequence above, it is possible to determine that `a` and `b` refer to the same underlying contents by inspecting the result of `fstat`: both will return the same inode number (`ino`), and the `nlink` count will be set to 2.

The `unlink` system call removes a name from the file system. The file's inode and the disk space holding its content are only freed when the file's link count is zero and no file descriptors refer to it. Thus adding

```
unlink("a");
```

to the last code sequence leaves the inode and file content accessible as `b`. Furthermore,

```
fd = open("/tmp/xyz", O_CREATE|O_RDWR);
unlink("/tmp/xyz");
```

is an idiomatic way to create a temporary inode with no name that will be cleaned up when the process closes `fd` or exits.

Unix provides file utilities callable from the shell as user-level programs, for example `mkdir`, `ln`, and `rm`. This design allows anyone to extend the command-line interface by adding new user-level programs. In hindsight this plan seems obvious, but other systems designed at the time of Unix often built such commands into the shell (and built the shell into the kernel).

One exception is `cd`, which is built into the shell (`user/sh.c:161`). `cd` must change the current working directory of the shell itself. If `cd` were run as a regular command, then the shell would

Unix's Strength

The combination of Unix's standard file descriptors, pipes, and convenient shell syntax gave rise to several foundational software tools that became integral to the Unix philosophy. Some of the very first and most influential tools created in this environment include:

1. `cat` (concatenate and display files)**

- **Function:** Reads files sequentially, writing their contents to the standard output.
- **Significance:** Often used in combination with pipes to feed data from one command to another.

2. `grep` (global regular expression print)**

- **Function:** Searches for patterns within text files using regular expressions.
- **Significance:** Allows users to filter the output of other commands by searching for specific strings or patterns.

3. `ls` (list directory contents)**

- **Function:** Lists the files and directories within a directory.
- **Significance:** Essential for navigating the filesystem, especially when combined with other tools using pipes.

4. `sort`**

- **Function:** Sorts lines of text files.
- **Significance:** When used with pipes, it allows users to easily sort data generated or processed by other commands.

5. `wc` (word count)**

- **Function:** Counts the number of lines, words, and characters in a file.
- **Significance:** Useful for getting quick statistics on text data, often used in combination with other tools through pipes.

6. `awk`**

- **Function:** A programming language designed for text processing and typically used for data extraction and reporting.
- **Significance:** It is powerful for pattern scanning and processing, often used in pipelines for complex text processing tasks.

7. `sed` (stream editor)**

- **Function:** A stream editor for filtering and transforming text.
- **Significance:** Allows for advanced text manipulation directly within command-line pipelines.

8. `find`**

- **Function:** Searches for files in a directory hierarchy.
- **Significance:** Provides a powerful way to locate files based on a variety of criteria, often combined with other tools for further processing.

9. `sh` (the Bourne Shell)**

- **Function:** The original Unix shell interpreter, which provides the command-line interface.
- **Significance:** It allowed users to string together commands using pipes, and its syntax formed the foundation for shell scripting.

10. `ps` (process status)**

- **Function:** Reports a snapshot of current processes.
- **Significance:** Useful for monitoring and managing system processes, often combined with other tools to filter or sort the output.

These tools, in combination with Unix's design of standard input, output, and error streams, as well as the concept of piping output from one command into another, enabled a modular approach to building complex workflows and scripts. This approach is central to the Unix philosophy of creating small, single-purpose programs that can be combined in flexible ways to perform complex tasks.

fork a child process, the child process would run `cd`, and `cd` would change the *child*’s working directory. The parent’s (i.e., the shell’s) working directory would not change.

1.5 Real world

Unix’s combination of “standard” file descriptors, pipes, and convenient shell syntax for operations on them was a major advance in writing general-purpose reusable programs. The idea sparked a culture of “software tools” that was responsible for much of Unix’s power and popularity, and the shell was the first so-called “scripting language.” The Unix system call interface persists today in systems like BSD, Linux, and macOS.

The Unix system call interface has been standardized through the Portable Operating System Interface (POSIX) standard. Xv6 is *not* POSIX compliant: it is missing many system calls (including basic ones such as `lseek`), and many of the system calls it does provide differ from the standard. Our main goals for xv6 are simplicity and clarity while providing a simple UNIX-like system-call interface. Several people have extended xv6 with a few more system calls and a simple C library in order to run basic Unix programs. Modern kernels, however, provide many more system calls, and many more kinds of kernel services, than xv6. For example, they support networking, windowing systems, user-level threads, drivers for many devices, and so on. Modern kernels evolve continuously and rapidly, and offer many features beyond POSIX.

Unix unified access to multiple types of resources (files, directories, and devices) with a single set of file-name and file-descriptor interfaces. This idea can be extended to more kinds of resources; a good example is Plan 9 [16], which applied the “resources are files” concept to networks, graphics, and more. However, most Unix-derived operating systems have not followed this route.

The file system and file descriptors have been powerful abstractions. Even so, there are other models for operating system interfaces. Multics, a predecessor of Unix, abstracted file storage in a way that made it look like memory, producing a very different flavor of interface. The complexity of the Multics design had a direct influence on the designers of Unix, who aimed to build something simpler.

Xv6 does not provide a notion of users or of protecting one user from another; in Unix terms, all xv6 processes run as root.

This book examines how xv6 implements its Unix-like interface, but the ideas and concepts apply to more than just Unix. Any operating system must multiplex processes onto the underlying hardware, isolate processes from each other, and provide mechanisms for controlled inter-process communication. After studying xv6, you should be able to look at other, more complex operating systems and see the concepts underlying xv6 in those systems as well.

1.6 Exercises

1. Write a program that uses UNIX system calls to “ping-pong” a byte between two processes over a pair of pipes, one for each direction. Measure the program’s performance, in exchanges per second.