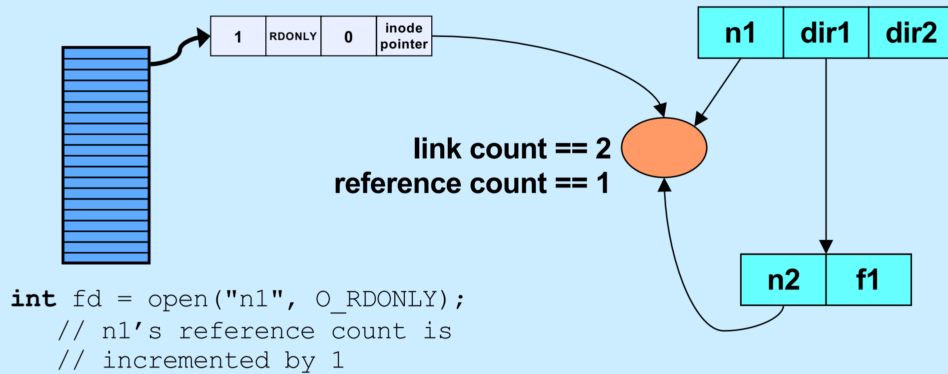
CS 33

Files Part 4

Copyright © 2023 Thomas W. Doeppner. All rights reserved.

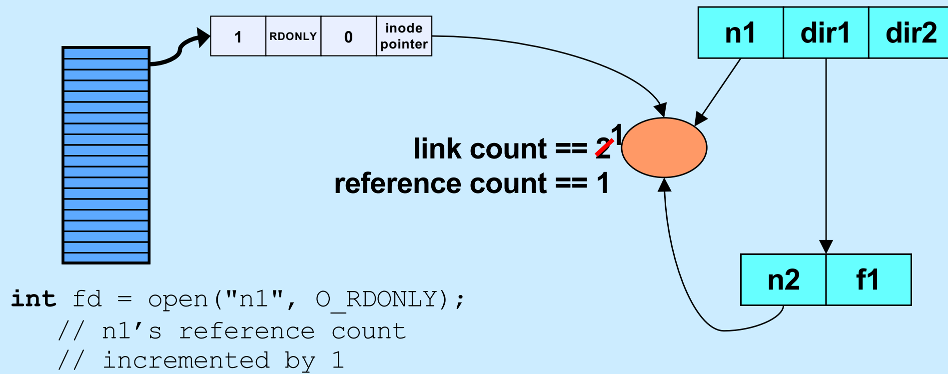
Link and Reference Counts



 Copyright © 2023 Thomas W. Doeppner. All rights reserved.

A file's link count is the number of directory entries that refer to it. There's a separate reference count that's the number of file context structures that refer to it (via the inode pointer – see slide XVII-9). These counts are maintained in the file's inode, which contains all information used by the operating system to refer to the file (on disk).

Link and Reference Counts

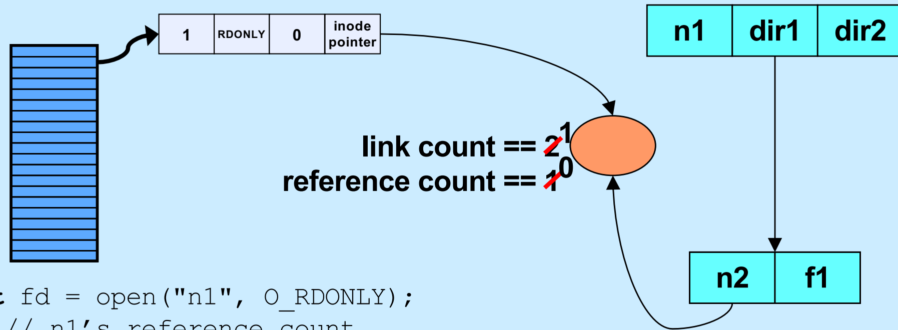



```
int fd = open("n1", O_RDONLY);
   // n1's reference count
   // incremented by 1

unlink("n1");
   // link count decremented by 1
   // same effect in shell via "rm n1"
```

 Copyright © 2023 Thomas W. Doeppner. All rights reserved.

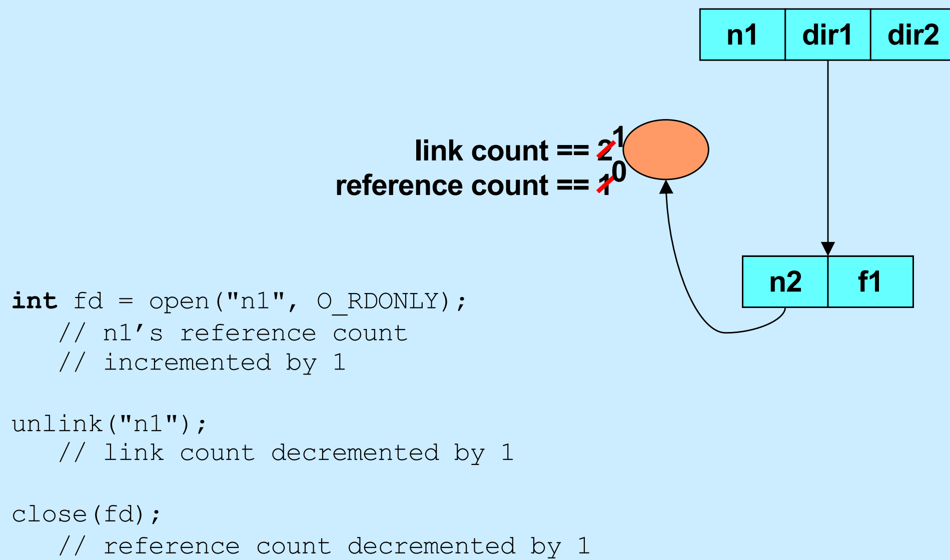
Note that the shell's rm command is implemented using unlink; it simply removes the directory entry, reducing the file's link count by 1.

Link and Reference Counts



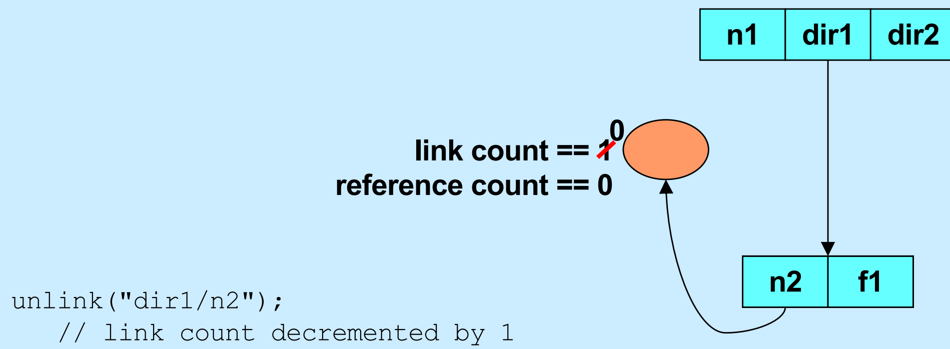

```
int fd = open("n1", O_RDONLY);
   // n1's reference count
   // incremented by 1

unlink("n1");
   // link count decremented by 1

close(fd);
   // reference count decremented by 1
```


Copyright © 2023 Thomas W. Doeppner. All rights reserved.



A file is deleted if and only if both its link and reference counts are zero.

Link and Reference Counts



Copyright © 2023 Thomas W. Doeppner. All rights reserved.

A file is deleted if and only if both its link and reference counts are zero.

Quiz 1

```
int main() {
  int fd = open("file", O_RDWR|O_CREAT, 0666);
  unlink("file");
  PutStuffInFile(fd);
  GetStuffFromFile(fd);
  return 0;
}
```

Assume that *PutStuffInFile* writes to the given file, and *GetStuffFromFile* reads from the file.

a) This program is doomed to failure, since the file is deleted before it's used

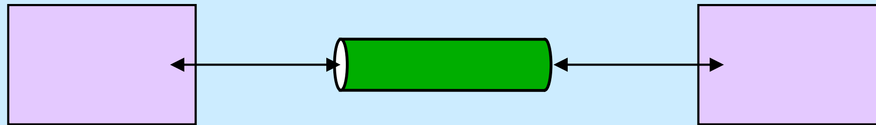
b) Because the file is used after the unlink call, it won't be deleted

c) The file will be deleted when the program terminates

 Copyright © 2023 Thomas W. Doeppner. All rights reserved.

Note that when a process terminates, all its open files are automatically closed.

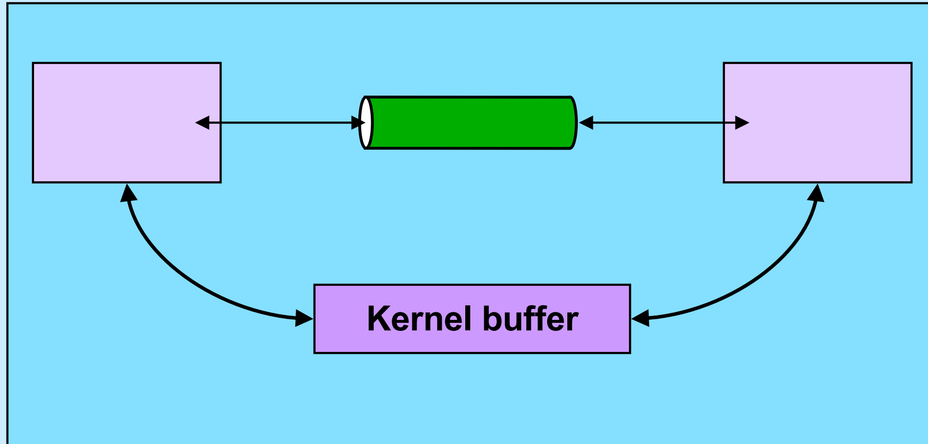
Interprocess Communication (IPC): Pipes



 Copyright © 2023 Thomas W. Doeppner. All rights reserved.

A rather elegant way for different processes to communicate is via a pipe: one process puts data into a pipe, another process reads the data from the pipe.

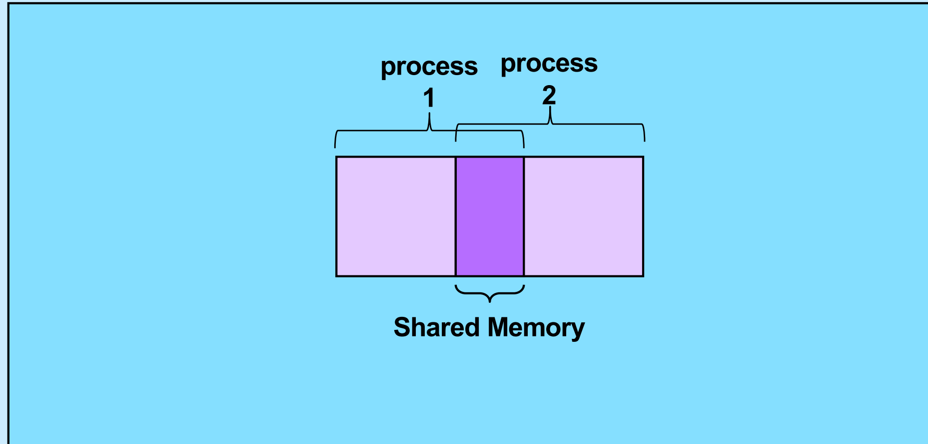
Interprocess Communication: Same Machine I



 Copyright © 2023 Thomas W. Doeppner. All rights reserved.

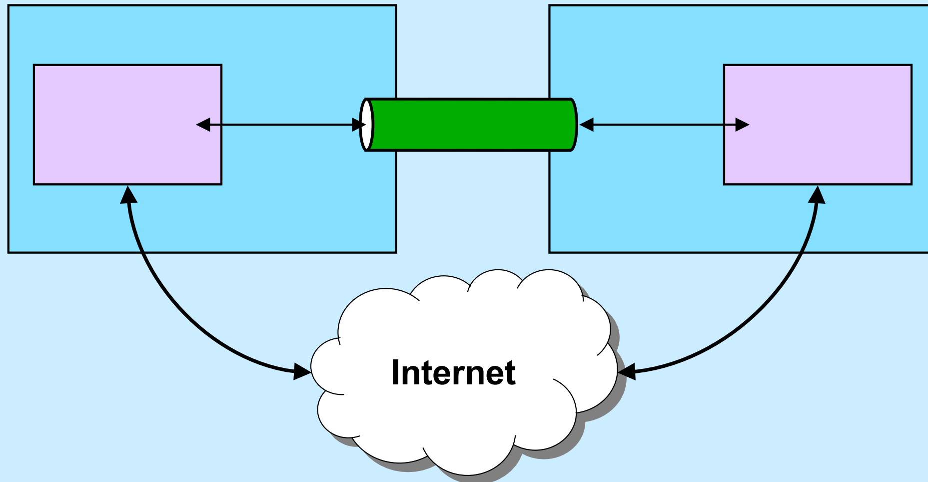
The implementation of a pipe involves the sending process using a write system call to transfer data into a kernel buffer. The receiving process fetches the data from the buffer via a read system call. We'll cover some of the details about how this works when we discuss multithreaded programming later in the semester.

Interprocess Communication: Same Machine II



 Copyright © 2023 Thomas W. Doeppner. All rights reserved.

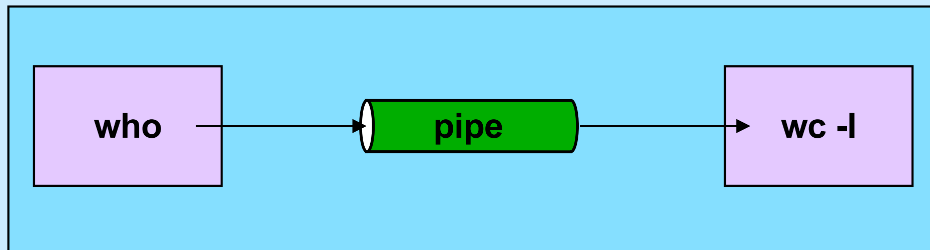
Another way for processes to communicate is for them to arrange to have some memory in common via which they share information. We discuss this approach later in the semester.



The pipe abstraction can also be made to work between processes on different machines. We discuss this later in the semester.

Pipes

`$cslab2e who | wc -l`



 Copyright © 2023 Thomas W. Doeppner. All rights reserved.

The vertical bar ("|") is the pipe symbol in the shell. The syntax shown above represents creating two processes, one running **who** and the other running **wc**. The standard output of **who** is setup to be the pipe; the standard input of **wc** is setup to be the pipe. Thus, the output of **who** becomes the input of **wc**. The "-l" argument to **wc** tells it to count and print out the number of lines that are input to it. The **who** command writes to standard output the login names of all logged in users. The combination of the two produces the number of users who are currently logged in.

Using Pipes in C

```
$cslab2e who | wc -l
```

```
int fd[2];
pipe(fd);
if (fork() == 0) {
  close(fd[0]);
  close(1);
  dup(fd[1]); close(fd[1]);
  execl("/usr/bin/who", "who", 0); // who sends output to pipe
}
if (fork() == 0) {
  close(fd[1]);
  close(0);
  dup(fd[0]); close(fd[0]);
  execl("/usr/bin/wc", "wc", "-l", 0); // wc's input is from pipe
}
close(fd[1]); close(fd[0]);
// …
```

 Copyright © 2023 Thomas W. Doeppner. All rights reserved.

The **pipe** system call creates a “pipe” in the kernel and sets up two file descriptors. One, in fd[1], is for writing to the pipe; the other, in fd[0], is for reading from the pipe. The input end of the pipe is set up to be **stdout** for the process running **who**, and the output end of the pipe is closed, since it’s not needed. Similarly, the input end of the pipe is set up to be **stdin** for the process running **wc**, and the input end is closed. Since the parent process (running the shell) has no further need for the pipe, it closes both ends. When neither end of the pipe is open by any process, the system deletes it. If a process reads from a pipe for which no process has the input end open, the read returns 0, indicating end of file. If a process writes to a pipe for which no process has the output end open, the write returns -1, indicating an error and **errno** is set to EPIPE; the process also receives the SIGPIPE signal, which we explain in the next lecture.

Shell 1: Artisanal Coding

```
while ((line = get_a_line()) != 0) {
    tokens = parse_line(line);
    for (int i=0; i < ntokens; i++) {
        if (strcmp(tokens[i], ">") == 0) {
            // handle output redirection
        } else if (strcmp(tokens[i], "<") == 0) {
            // handle input redirection
        } else if (strcmp(tokens[i], "&") == 0) {
            // handle "no wait"
        } ... else {
            // handle other cases
        }
    }
    if (fork() == 0) {
        // ...
        execv(...);
    }
    // ...
}
```

 Copyright © 2023 Thomas W. Doeppner. All rights reserved.

This is, of course, over simplified. The complete program should be 200 or so lines long.

Note that "handle x" might simply involve taking note of x, then dealing with it later.

Also note that “artisanal” anything is always better than “non-artisanal” anything.

Shell 1: Non-Artisanal Coding (1)

```
while ((line = get_a_line()) != 0) {
    tokens = parse_line(line);
    for (int i=0; i < ntokens; i++) {
        // handle "normal" case
    }
    if (fork() == 0) {
        // ...
        execv(...);
    }
    // ...
}
```

 Copyright © 2023 Thomas W. Doeppner. All rights reserved.

One first writes the code assuming no redirection symbols and no &s. That's perfectly reasonable.

Shell 1: Non-Artisanal Coding (2)

```
next_line: while ((line = get_a_line()) != 0) {
    tokens = parse_line(line);
    for (int i=0; i < ntokens; i++) {
        if (redirection_symbol(token[i])) {
            // ...
            if (fork() == 0) {
                // ...
                execv(...);      whoops!
            }
            // ...
            goto next_line;
        }
        // handle "normal" case
    }
    if (fork() == 0) {
        // ...          (whoops!)
        execv(...);
    }
    // ...
}
```


Copyright © 2023 Thomas W. Doeppner. All rights reserved.

The next step is to deal with redirection symbols. Rather than modify the fork/exec code so as to work for both cases, it's copied into the new case and modified there. Thus, we now have two versions of the fork/exec code to maintain. If we find a bug in one, we need to remember to fix it in both.

At this point it's becoming difficult for you to debug your code, and really difficult for TAs to figure out what you're doing so they can help you.

Shell 1: Non-Artisanal Coding (3)

```
next_line: while ((line = get_a_line()) != 0) {
    tokens = parse_line(line);
    for (int i=0; i < ntokens; i++) {
        if (redirection_symbol(token[i])) {
            // ...
            if (fork() == 0) {
                // ...
                execv(...);
            }
            // ... deal with &
            goto next_line;
        }
        // handle "normal" case
    }
    if (fork() == 0) {
        // ...
        execv(...);
    }
    // ... also deal with & here!
}
```

 Copyright © 2023 Thomas W. Doeppner. All rights reserved.

We now have to handle & in multiple places.

If done this way, you could well have a 700-line program (the artisanal code took around 200 lines).

Shell 1: Non-Artisanal Coding (Worse)

```
next_line: while ((line = get_a_line()) != 0) {
tokens = parse_line(line);
for (int i=0; i < ntokens; i++) {
if (redirection_symbol(token[i])) {
// ...
if (fork() == 0) {
// ...
execv(...);
}
// ... deal with &
goto next_line;
}
// handle "normal" case
}
if (fork() == 0) {
// ...
execv(...);
}
// ... also deal with & here!
}
```

 Copyright © 2023 Thomas W. Doeppner. All rights reserved.

If the code is poorly formatted, it's even tougher to understand.

Artisanal Programming

- Factor your code!
  - A; D | B; D | C; D = (A | B | C); D
- Format as you write!
  - don't run the formatter only just before handing it in
  - your code should always be well formatted
- If you have a tough time understanding your code, you'll have a tougher time debugging it and TAs will have an even tougher time helping you

Copyright © 2023 Thomas W. Doeppner. All rights reserved.

It's Your Code

- Be proud of it!
  - it not only works; it shows skillful artisanship
- It's not enough to merely work
  - others have to understand it
    - (not to mention you ...)
  - you (and others) have to maintain it
    - shell 2 is coming soon!

Copyright © 2023 Thomas W. Doeppner. All rights reserved.

CS 33

Signals Part 1

 Copyright © 2023 Thomas W. Doeppner. All rights reserved.

An Interlude Between Shells

- Shell 1
  - it can run programs
  - it can redirect I/O
- Signals
  - a mechanism for coping with exceptions and external events
  - the mechanism needed for shell 2
- Shell 2
  - it can control running programs

 Copyright © 2023 Thomas W. Doeppner. All rights reserved.

Whoops ...

```
$ SometimesUsefulProgram xyz
Are you sure you want to proceed? Y
Are you really sure? Y
Reformatting of your disk will begin
in 3 seconds.
Everything you own will be deleted.
There's little you can do about it.
Too bad …
```

Copyright © 2023 Thomas W. Doeppner. All rights reserved.

A Gentler Approach

- Signals
  - get a process's attention
    - » send it a signal
  - process must either deal with it or be terminated
    - » in some cases, the latter is the only option

Copyright © 2023 Thomas W. Doeppner. All rights reserved.

Stepping Back …

- What are we trying to do?
  - interrupt the execution of a program
    - » cleanly terminate it

      or
    - » cleanly change its course
  - not for the faint of heart
    - » it's difficult
    - » it gets complicated
    - » (not done in Windows)

Copyright © 2023 Thomas W. Doeppner. All rights reserved.

Signals

- Generated (by OS) in response to
  - exceptions (e.g., arithmetic errors, addressing problems)
    - » synchronous signals
  - external events (e.g., timer expiration, certain keystrokes, actions of other processes)
    - » asynchronous signals
- Effect on process:
  - termination (possibly producing a core dump)
  - invocation of a function that has been set up to be a signal handler
  - suspension of execution
  - resumption of execution

 Copyright © 2023 Thomas W. Doeppner. All rights reserved.

Signals are a kernel-supported mechanism for reporting events to user code and forcing a response to them. There are actually two sorts of such events, to which we sometimes refer as **exceptions** and **interrupts**. The former occur typically because the program has done something wrong. The response, the sending of a signal, is immediate; such signals are known as **synchronous** signals. The latter are in response to external actions, such as a timer expiring, an action at the keyboard, or the explicit sending of a signal by another process. Signals send in response to these events can seemingly occur at any moment and are referred to as **asynchronous** signals.

Processes react to signals using the actions shown in the slide. The action taken depends partly on the signal and partly on arrangements made in the process beforehand.

A core dump is the contents of a process's address space, written to a file (called **core**), reflecting what the situation was when it was terminated by a signal. They can be used by gdb to see what happened (e.g., to get a backtrace). Since they're fairly large and rarely looked at, they're normally disabled. We'll look at them further shortly.

Signal Types

SIGABRT	*abort* called	term, core
SIGALRM	alarm clock	term
SIGCHLD	death of a child	ignore
SIGCONT	continue after stop	cont
SIGFPE	erroneous arithmetic operation	term, core
SIGHUP	hangup on controlling terminal	term
SIGILL	illegal instruction	term, core
SIGINT	interrupt from keyboard	term
SIGKILL	kill	forced term
SIGPIPE	write on pipe with no one to read	term
SIGQUIT	quit	term, core
SIGSEGV	invalid memory reference	term, core
SIGSTOP	stop process	forced stop
SIGTERM	software termination signal	term
SIGTSTP	stop signal from keyboard	stop
SIGTTIN	background read attempted	stop
SIGTTOU	background write attempted	stop
SIGUSR1	application-defined signal 1	stop
SIGUSR2	application-defined signal 2	stop

 Copyright © 2023 Thomas W. Doeppner. All rights reserved.

This slide shows the complete list of signals required by POSIX 1003.1, the official Unix specification. In addition, many Unix systems support other signals, some of which we'll mention in the course. The third column of the slide lists the default actions in response to each of the signals. **term** means the process is terminated, **core** means there is also a core dump; **ignore** means that the signal is ignored; **stop** means that the process is stopped (suspended); **cont** means that a stopped process is resumed (continued); **forced** means that the default action cannot be changed and that the signal cannot be blocked or ignored.

Sending a Signal

- **int** kill(**pid_t** pid, **int** sig)
  - **send signal *sig* to process *pid***
- **Also**
  - ***kill* shell command**
  - **type ctrl-c**
    - » **sends signal 2 (SIGINT) to current process**
  - **type ctrl-**
    - » **sends signal 3 (SIGQUIT) to current process**
  - **type ctrl-z**
    - » **sends signal 20 (SIGTSTP) to current process**
  - **do something bad**
    - » **bad address, bad arithmetic, etc.**

 Copyright © 2023 Thomas W. Doeppner. All rights reserved.

Note that the signals generated by typing control characters on the keyboard are actually sent to the current process group of the terminal, a concept we discuss soon.

Handling Signals

```
#include <signal.h>

typedef void (*sighandler_t)(int);
sighandler_t signal(int signo,
    sighandler_t handler);

sighandler_t OldHandler;

OldHandler = signal(SIGINT, NewHandler);
```

 Copyright © 2023 Thomas W. Doeppner. All rights reserved.

The **signal** function establishes a new handler for the given signal and returns the address of the previous handler.

Special Handlers

- **SIG_IGN**
  - **ignore the signal**
  - `signal(SIGINT, SIG_IGN);`
- **SIG_DFL**
  - **use the default handler**
    - » **usually terminates the process**
  - `signal(SIGINT, SIG_DFL);`

 Copyright © 2023 Thomas W. Doeppner. All rights reserved.

Example

```
void sigloop() {
  while(1)
    ;
}

int main() {
  void handler(int);
  signal(SIGINT, handler);
  sigloop();
  return 1;
}
void handler(int signo) {
  printf("I received signal %d. "
     "Whoopee!!\n", signo);
}
```

 Copyright © 2023 Thomas W. Doeppner. All rights reserved.

Note that the C compiler implicitly concatenates two adjacent strings, as done in printf above.

Digression: Core Dumps

- **Core dumps**
  - files (called "core") that hold the contents of a process's address space after termination by a signal
  - they're large and rarely used, so they're often disabled by default
  - use the ulimit command in bash to enable them

```
ulimit -c unlimited
```

  - use gdb to examine the process (post-mortem debugging)

```
gdb sig core
```


Copyright © 2023 Thomas W. Doeppner. All rights reserved.

Don't forget to delete the core files when you're finished with them! Note that neither OSX nor Windows supports core dumps.

Some details on the **ulimit** command: its supports both a hard limit (which can't be modified) and a soft limit (which can later be modified). By default, **ulimit** sets both the hard and soft limits. Thus typing

```
ulimit -c 0
```

sets both the hard and soft limits of core file size to 0, meaning that you can't increase the limit later (within the execution of the current invocation of this shell).

But if you type

```
ulimit -Sc 0
```

then just the soft limit is modified, allowing you to type

```
ulimit -c unlimited
```

later.

sigaction

```
int sigaction(int sig, const struct sigaction *new,
              struct sigaction *old);
struct sigaction {
   void (*sa_handler)(int);
   void (*sa_sigaction)(int, siginfo_t *, void *);
   sigset_t sa_mask;
   int sa_flags;
};

int main() {
   struct sigaction act; void myhandler(int);
   sigemptyset(&act.sa_mask); // zeroes the mask
   act.sa_flags = 0;
   act.sa_handler = myhandler;
   sigaction(SIGINT, &act, NULL);
   …
}
```

 Copyright © 2023 Thomas W. Doeppner. All rights reserved.

The **sigaction** system call is the the more general means for establishing a process's response to a particular signal. Its first argument is the signal for which a response is being specified, the second argument is a pointer to a **sigaction** structure defining the response, and the third argument is a pointer to memory in which a **sigaction** structure will be stored containing the specification of what the response was prior to this call. If the third argument is null, the prior response is not returned.

The **sa_handler** member of **sigaction** is either a pointer to a user-defined handler function for the signal or one of SIG_DFL (meaning that the default action is taken) or SIG_IGN (meaning that the signal is to be ignored). The **sig_action** member is an alternative means for specifying a handler function; we won't get a chance to discuss it, but it's used when more information about the cause of a signal is needed.

When a user-defined signal-handler function is entered in response to a signal, the signal itself is masked until the function returns. Using the **sa_mask** member, one can specify additional signals to be masked while the handler function is running. On return from the handler function, the process's previous signal mask is restored.

The **sa_flags** member is used to specify various other things that we describe in upcoming slides.

Example

```
int main() {
  void handler(int);
  struct sigaction act;
  act.sa_handler = handler;
  sigemptyset(&act.sa_mask);
  act.sa_flags = 0;
  sigaction(SIGINT, &act, 0);

  while(1)
    ;
  return 1;
}

void handler(int signo) {
  printf("I received signal %d. "
     "Whoopee!!\n", signo);
}
```

 Copyright © 2023 Thomas W. Doeppner. All rights reserved.

This has behavior identical to the previous example; we're using **sigaction** rather than *signal* to set up the signal handler.

Quiz 1

```
int main() {
  void handler(int);
  struct sigaction act;
  act.sa_handler = hand
  sigemptyset(&act.sa_m
  act.sa_flags = 0;
  sigaction(SIGINT, &ac

  while(1)
    ;
  return 1;
}

void handler(int signo) {
  printf("I received signal %d. "
     "Whoopee!!\n", signo);
}
```

You run the example program, then quickly type ctrl-C. What is the most likely explanation if the program then terminates?

a) **this “can’t happen”; thus there’s a problem with the system**
b) **you’re really quick or the system is really slow (or both)**
c) **what we’ve told you so far isn’t quite correct**

 Copyright © 2023 Thomas W. Doeppner. All rights reserved.

Waiting for a Signal …

```
signal(SIGALRM, RespondToSignal);

…

struct timeval waitperiod = {0, 1000};
      /* seconds, microseconds */
struct timeval interval = {0, 0};
struct itimerval timerval;
timerval.it_value = waitperiod;
timerval.it_interval = interval;

setitimer(ITIMER_REAL, &timerval, 0);
      /* SIGALRM sent in ~one millisecond */
pause();  /* wait for it */
printf("success!\n");
```

 Copyright © 2023 Thomas W. Doeppner. All rights reserved.

Here we use the **setitimer** system call to arrange so that a SIGALRM signal is generated in one millisecond. (The system call takes three arguments: the first indicates how time should be measured; what's specified here is to use real time. See its man page for other possibilities. The second argument contains a **struct itimerval** that itself contains two **struct timevals**. One (named **it_value**) indicates how much time should elapse before a SIGALRM is generated for the process. The other (named **it_interval**), if non-zero, indicates that a SIGALRM should be sent again, repeatedly, every **it_interval** period of time. Each process may have only one pending timer, thus when a process calls **setitimer**, the new value replaces the old. If the third argument to **setitimer** is non-zero, the old value is stored at the location it points to.)

The **pause** system call causes the process to block (go to sleep) and not resume until **some** signal that is not ignored is delivered.

Quiz 2

This program is guaranteed to print "success!".

a) no

b) yes

```
signal(SIGALRM, RespondToSignal);

…

struct timeval waitperiod = {0, 1000};
      /* seconds, microseconds */
struct timeval interval = {0, 0};
struct itimerval timerval;
timerval.it_value = waitperiod;
timerval.it_interval = interval;

setitimer(ITIMER_REAL, &timerval, 0);
      /* SIGALRM sent in ~one millisecond */
pause();  /* wait for it */
printf("success!\n");
```


Copyright © 2023 Thomas W. Doeppner. All rights reserved.

Masking Signals

```
setitimer(ITIMER_REAL, &timerval, 0);
      /* SIGALRM sent in ~one millisecond */
```

No signals here, please!

```
pause();  /* wait for it */
```

 Copyright © 2023 Thomas W. Doeppner. All rights reserved.

Masking Signals

mask SIGALRM

```
setitimer(ITIMER_REAL, &timerval, 0);
      /* SIGALRM sent in ~one millisecond */
```

No signals here

unmask and wait for SIGALRM

 Copyright © 2023 Thomas W. Doeppner. All rights reserved.

If a signal is masked, then, if it occurs, it's not immediately applied to the process, but will be applied when it's no longer masked.

Doing It Safely

```
sigset_t set, oldset;
sigemptyset(&set);
sigaddset(&set, SIGALRM);
sigprocmask(SIG_BLOCK, &set, &oldset);
      /* SIGALRM now masked */
…
setitimer(ITIMER_REAL, &timerval, 0);
      /* SIGALRM sent in ~one millisecond */

sigsuspend(&oldset);    /* unmask sig and wait */
/* SIGALRM masked again */

sigprocmask(SIG_SETMASK, &oldset, (sigset_t *)0);
      /* SIGALRM unmasked */
printf("success!\n");
```

 Copyright © 2023 Thomas W. Doeppner. All rights reserved.

Here's a safer way of doing what was attempted in the earlier slide. We mask the SIGALRM signal before calling **setitimer**. Then, rather than calling *pause*, we call **sigsuspend**, which sets the set of masked signals to its argument and, at the same instant, blocks the calling process. Thus if the SIGALRM is generated before our process calls **sigsuspend**, it won't be delivered right away. Since the call to **sigsuspend** reinstates the previous mask (which, presumably, did not include SIGALRM), the SIGALRM signal will be delivered and the process will return (after invoking the handler). When **sigsuspend** returns, the signal mask that was in place just before it was called is restored. Thus we have to restore **oldset** explicitly.

As with **pause**, **sigsuspend** returns only if an unmasked signal that is not ignored is delivered.

Signal Sets

- **To clear a set:**

```
int sigemptyset(sigset_t *set);
```

- **To add or remove a signal from the set:**

```
int sigaddset(sigset_t *set, int signo);
int sigdelset(sigset_t *set, int signo);
```

- **Example: to refer to both SIGHUP and SIGINT:**

```
sigset_t set;

sigemptyset(&set);
sigaddset(&set, SIGHUP);
sigaddset(&set, SIGINT);
```


Copyright © 2023 Thomas W. Doeppner. All rights reserved.

A number of signal-related operations involve sets of signals. These sets are normally represented by a bit vector of type **sigset_t**.

Masking (Blocking) Signals

```
#include <signal.h>
int sigprocmask(int how, const sigset_t *set,
      sigset_t *old);
```

- used to examine or change the signal mask of the calling process
  - » *how* is one of three commands:
    - SIG_BLOCK
      - the new signal mask is the union of the current signal mask and set
    - SIG_UNBLOCK
      - the new signal mask is the intersection of the current signal mask and the complement of set
    - SIG_SETMASK
      - the new signal mask is set

 Copyright © 2023 Thomas W. Doeppner. All rights reserved.

In addition to ignoring signals, you may specify that they are to be blocked (that is, held pending or masked). When a signal type is masked, signals of that type remains pending and do not interrupt the process until they are unmasked. When the process unblocks the signal, the action associated with any pending signal is performed. This technique is most useful for protecting critical code that should not be interrupted. Also, as we've already seen, when the handler for a signal is entered, subsequent occurrences of that signal are automatically masked until the handler is exited, hence the handler never has to worry about being invoked to handle another instance of the signal it's already handling.

Signal Handlers and Masking

- **What if a signal occurs while a previous instance is being handled?**
  - **inconvenient …**
- **Signals are masked while being handled**
  - **may mask other signals as well:**

```
struct sigaction act; void myhandler(int);
sigemptyset(&act.sa_mask); // zeroes the mask
sigaddset(&act.sa_mask, SIGQUIT);
   // also mask SIGQUIT
act.sa_flags = 0;
act.sa_handler = myhandler;
sigaction(SIGINT, &act, NULL);
```


Copyright © 2023 Thomas W. Doeppner. All rights reserved.

Timed Out!

```
int TimedInput( ) {
   signal(SIGALRM, timeout);
   …
   alarm(30);    /* send SIGALRM in 30 seconds */
   GetInput();   /* possible long wait for input */
   alarm(0);     /* cancel SIGALRM request */
   HandleInput();
   return(0);
nogood:
   return(1);
}

void timeout( ) {
   goto nogood;   /* not legal but straightforward */
}
```

 Copyright © 2023 Thomas W. Doeppner. All rights reserved.

This slide sketches something that one might want to try to do: give a user a limited amount of time (in this case, 30 seconds — the **alarm** function causes the system to send the process a SIGALRM signal in the given number of seconds) to provide some input, then, if no input, notify the caller that there is a problem. Here we'd like our timeout handler to transfer control to someplace else in the program, but we can't do this. (Note also that we should cancel the call to **alarm** if there is input. So that we can fit all the code in a single slide, we've left this part out.)

Doing It Legally (but Weirdly)

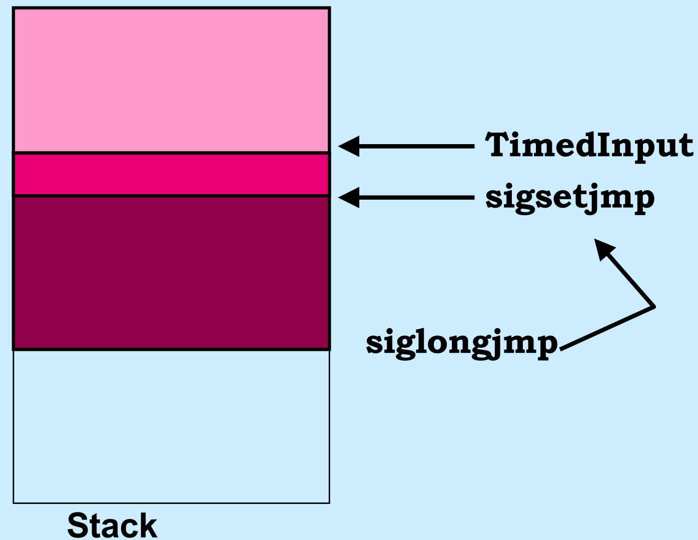
```
sigjmp_buf context;

int TimedInput( ) {
   signal(SIGALRM, timeout);
   if (sigsetjmp(context, 1) == 0) {
      alarm(30);  // cause SIGALRM in 30 seconds
      GetInput(); // possible long wait for input
      alarm(0);   // cancel SIGALRM request
      HandleInput();
      return 0;
   } else
      return 1;
}

void timeout() {
   siglongjmp(context, 1);    /* legal but weird */
}
```

 Copyright © 2023 Thomas W. Doeppner. All rights reserved.

To get around the problem of not being able to use a **goto** statement to get out of a signal handler, we introduce the **setjmp/longjmp** facility, also known as the ***nonlocal goto***. A call to **sigsetjmp** stores context information (about the current locus of execution) that can be restored via a call to **siglongjmp**. A bit more precisely: **sigsetjmp** stores into its first argument the values of the program-counter (instruction-pointer), stack-pointer, and other registers representing the process's current execution context. If the second argument is non-zero, the current signal mask is saved as well. The call returns 0. When **siglongjmp** is called with a pointer to this context information as its first argument, the current register values are replaced with those that were saved. If the signal mask was saved, that is restored as well. The effect of doing this is that the process resumes execution where it was when the context information was saved: inside of **sigsetjmp**. However, this time, rather than returning zero, it returns the second argument passed to **siglongjmp** (1 in the example).

To use this facility, you must include the header file **setjmp.h**.

sigsetjmp/siglongjmp



Stack

 Copyright © 2023 Thomas W. Doeppner. All rights reserved.

The effect of **sigsetjmp** is to save the registers relevant to the current stack frame; in particular, the instruction pointer, the base pointer (if used), and the stack pointer, as well as the return address and the current signal mask. A subsequent call to **siglongjmp** restores the stack to what it was at the time of the call to **sigsetjmp**. Note that **siglongjmp** should be called only from a stack frame that is farther on the stack than the one in which **sigsetjmp** was called.

Exceptions

- **Other languages support exception handling**

```
try {
  something_a_bit_risky();
} catch(ArithmeticException e) {
  deal_with_it(e);
}
```

- **Can we do something like this in C?**

Copyright © 2023 Thomas W. Doeppner. All rights reserved.

Exception Handling in C

```
void Exception(int sig) {
  THROW(sig)
}

int computation(int a) {
  return a/(a-a);
}
```

```
int main() {
  signal(SIGFPE, Exception);
  signal(SIGSEGV, Exception);
  TRY {
    computation(1);
  } CATCH(SIGFPE) {
    fprintf(stderr,
      "SIGFPE\n");
  } CATCH(SIGSEGV) {
    fprintf(stderr,
      "SIGSEGV\n");
  } END

  return 0;
}
```

 Copyright © 2023 Thomas W. Doeppner. All rights reserved.

The slide suggests a C syntax for exception handling. The TRY/CATCH/END behave as the try/catch does in the previous slide. The signal handler (called “Exception” in the slide) responds to exceptions, then THROWs the exception, to be caught in the TRY/CATCH/END construct. The big question, of course, is can we implement this?

Exception Handling in C

```
#define TRY \
 { \
   int excp; \
   if ((excp = \
     sigsetjmp(ctx, 1)) == 0)

#define CATCH(a_excp) \
   else if (excp == a_excp)

#define END }

#define THROW(excp) \
  siglongjmp(ctx, excp);
```

 Copyright © 2023 Thomas W. Doeppner. All rights reserved.

Here's an implementation of TRY, CATCH, END, and THROW using macros. Note that since #define statements are restricted to one line, we "escape" the ends of lines with back slashes.

Exception Handling in C

```
sigjmp_buf ctx;                          void exception(int sig) {
                                  THROW    siglongjmp(ctx, sig);
int main() {                             }
 ...
 {
   int excp;
   if ((excp = sigsetjmp(ctx, 1)) == 0) {  TRY
     computation(1);
   } else if (excp == SIGFPE) {  CATCH
     fprintf(stderr, "SIGFPE\n");
   } else if (excp == SIGSEGV) {  CATCH
     fprintf(stderr, "SIGFPE\n");
   }
 }                               END
 return 0;
}
```

 Copyright © 2023 Thomas W. Doeppner. All rights reserved.

And here is the code with the macros expanded.