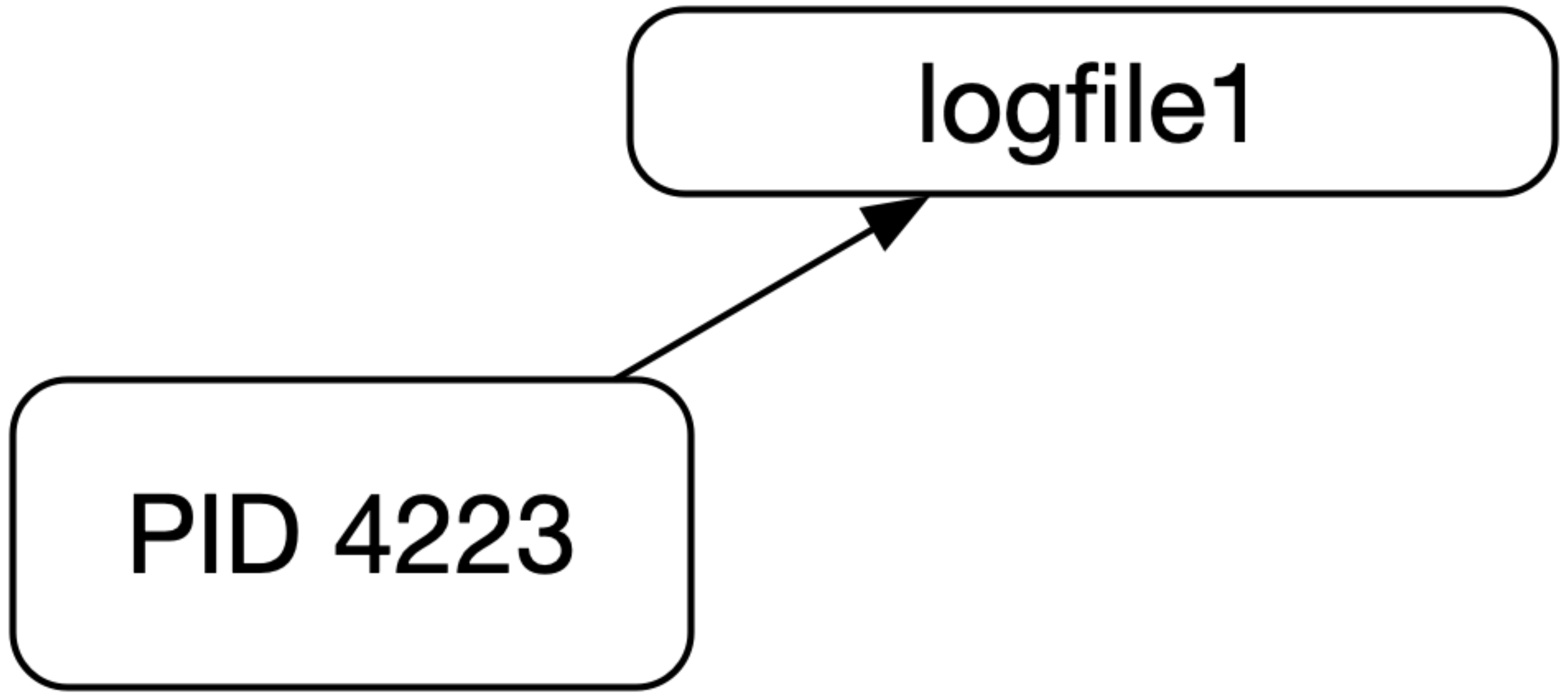
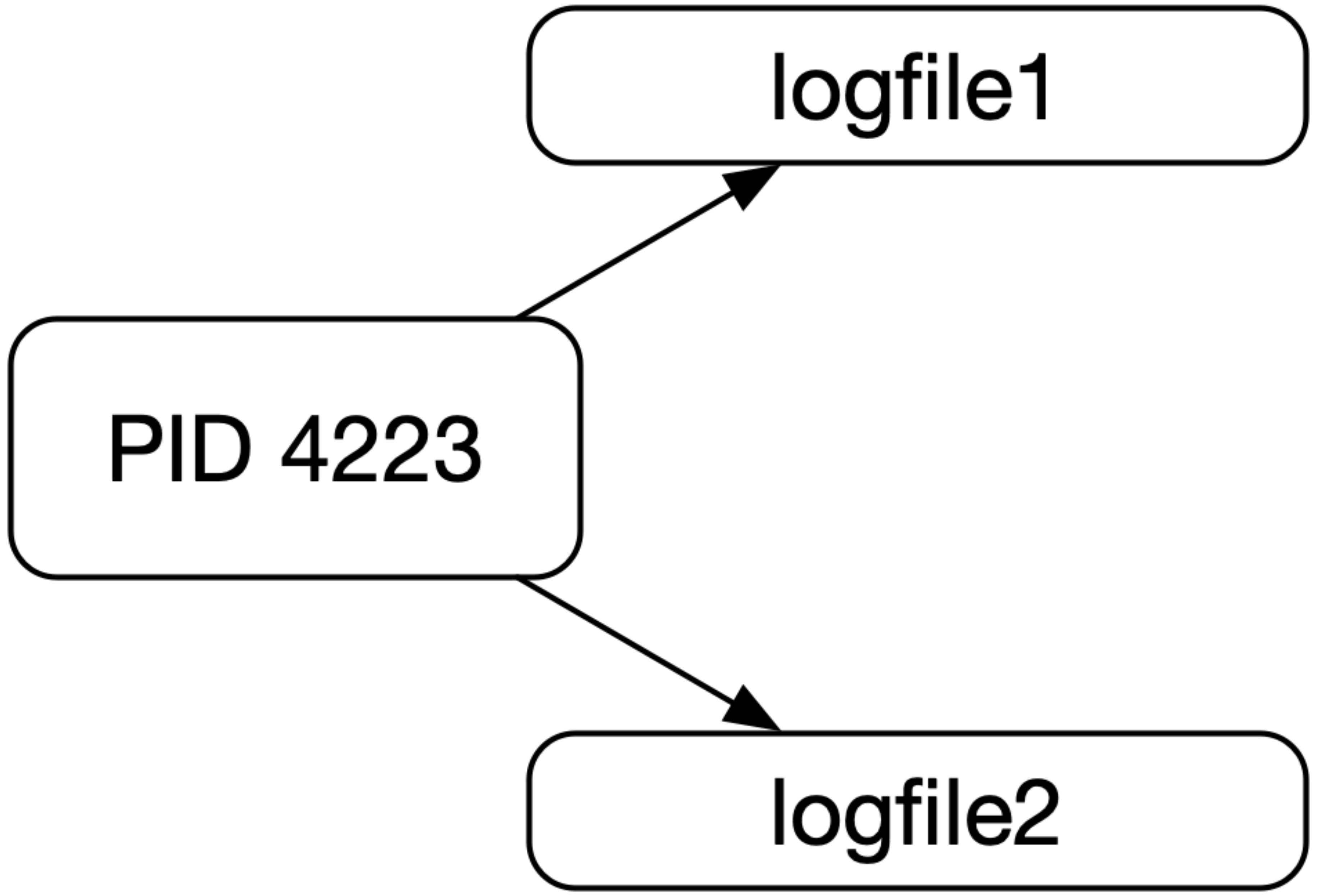
Advanced Programming in the UNIX Environment

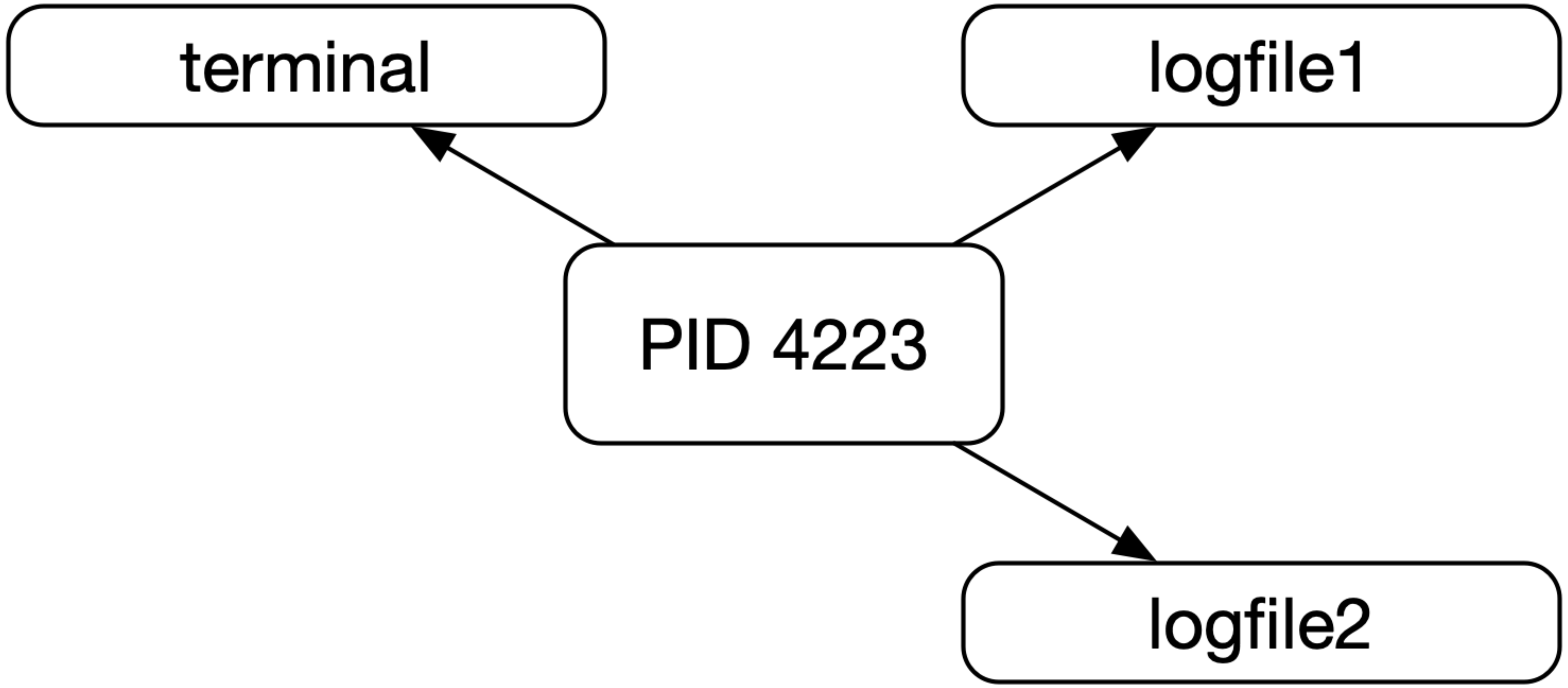
Week 12, Segment 1:
syslogd(8)

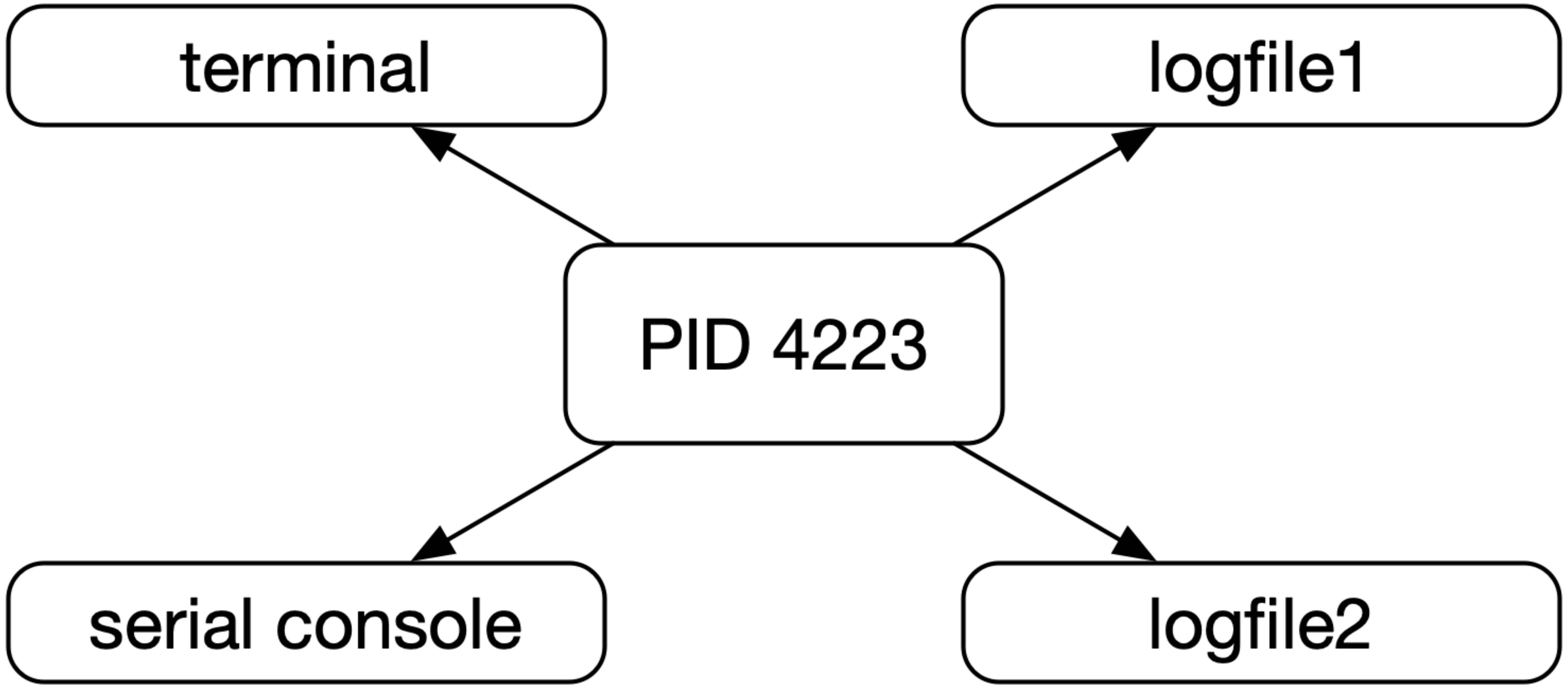
Department of Computer Science
Stevens Institute of Technology

Jan Schaumann
jschauma@stevens.edu
https://stevens.netmeister.org/631/


logfile1
PID 4223


logfile1
PID 4223
logfile2


terminal
logfile1
PID 4223
logfile2



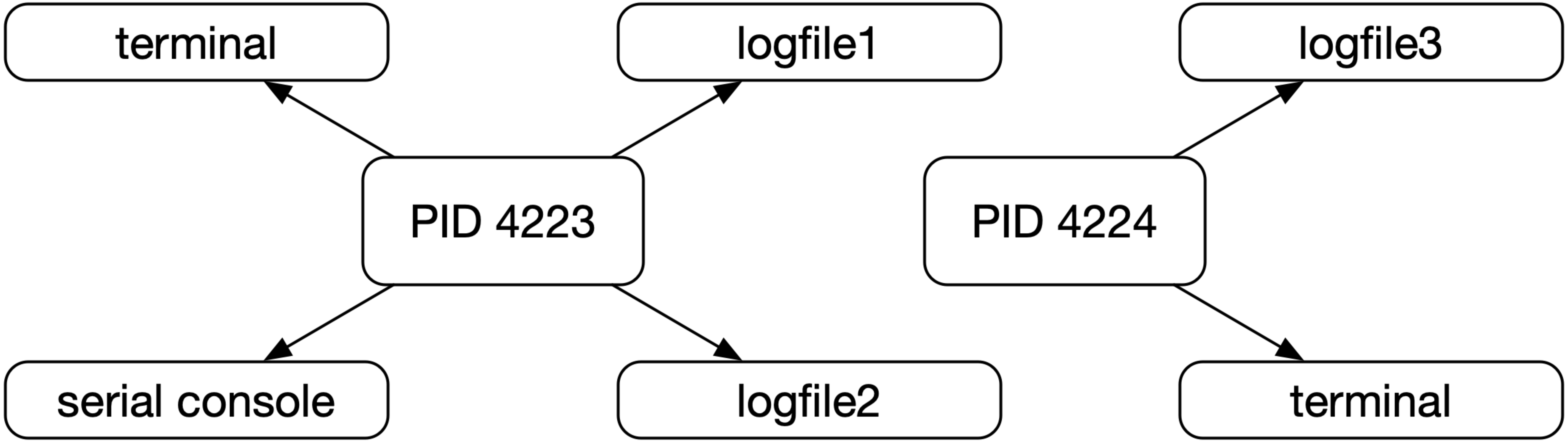
terminal

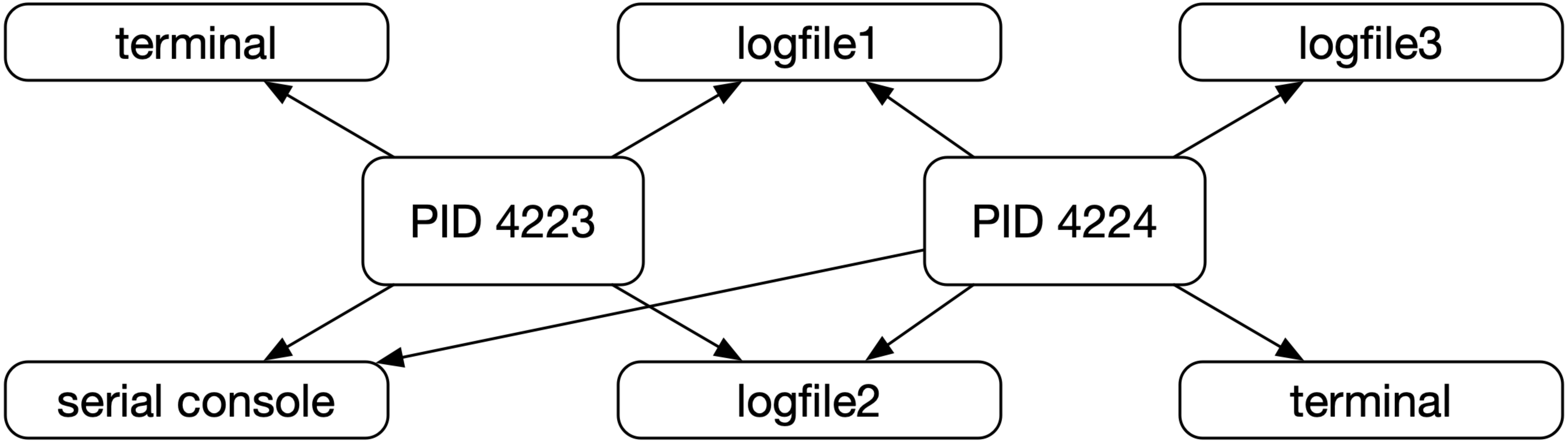
logfile1

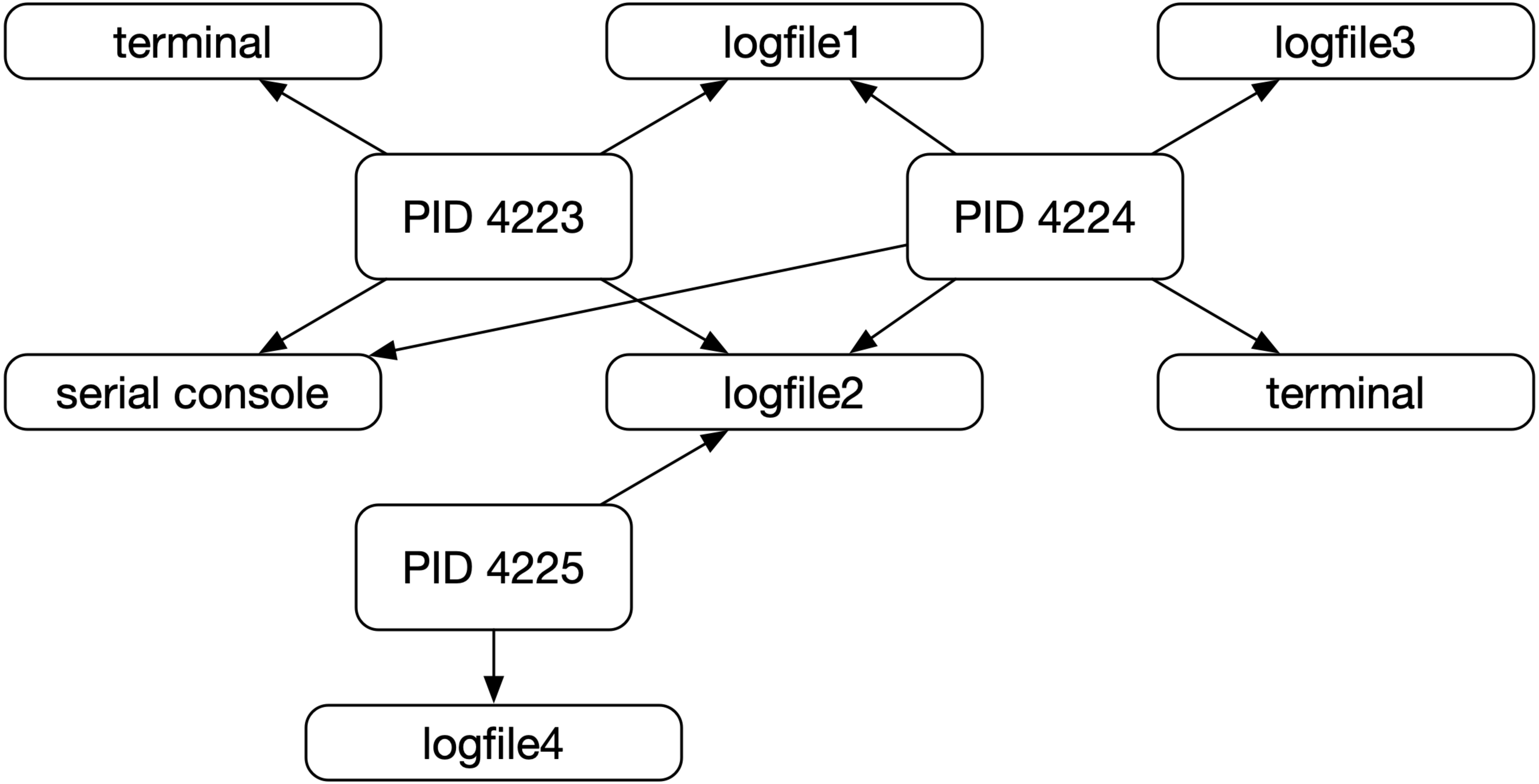
PID 4223

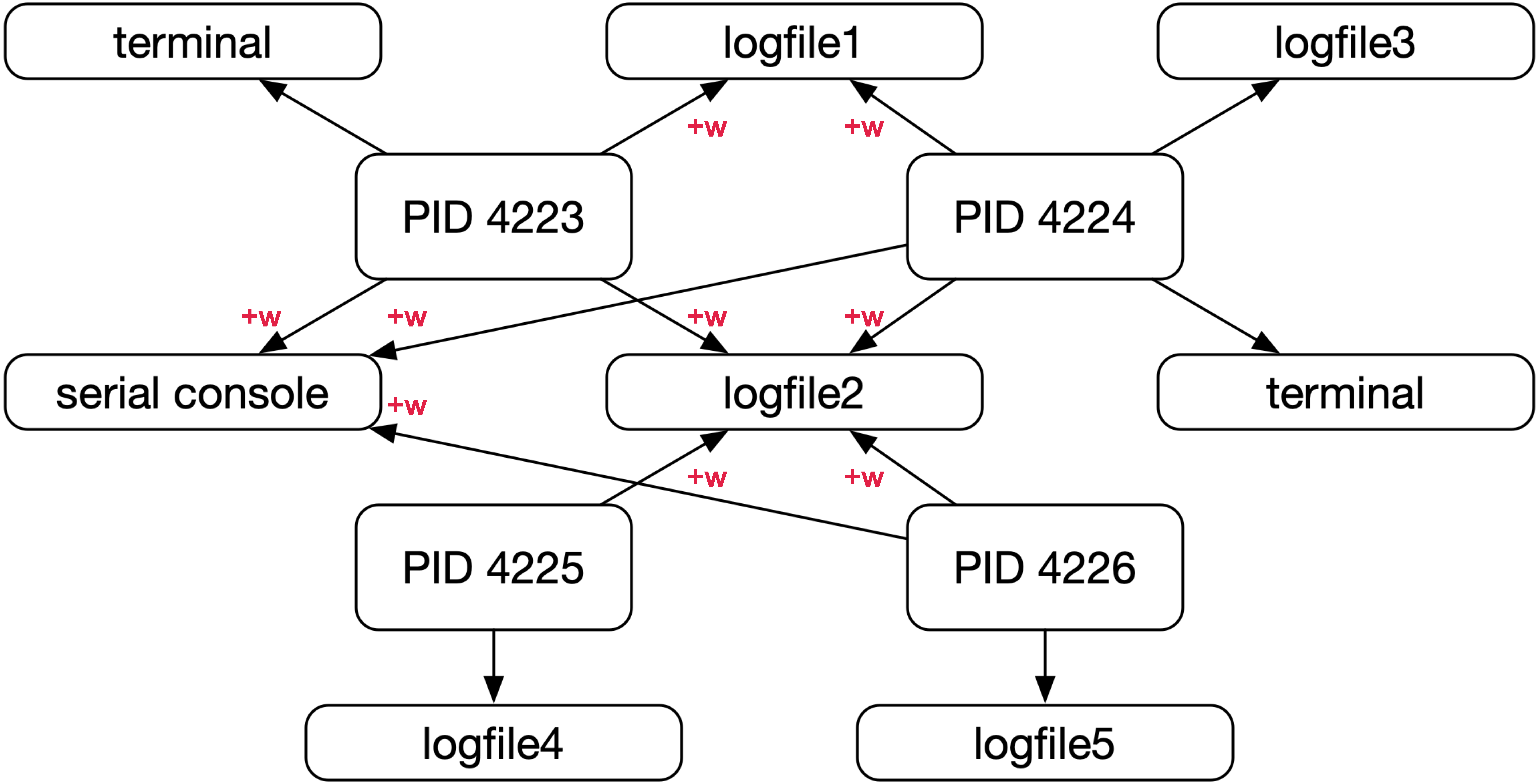
serial console

logfile2

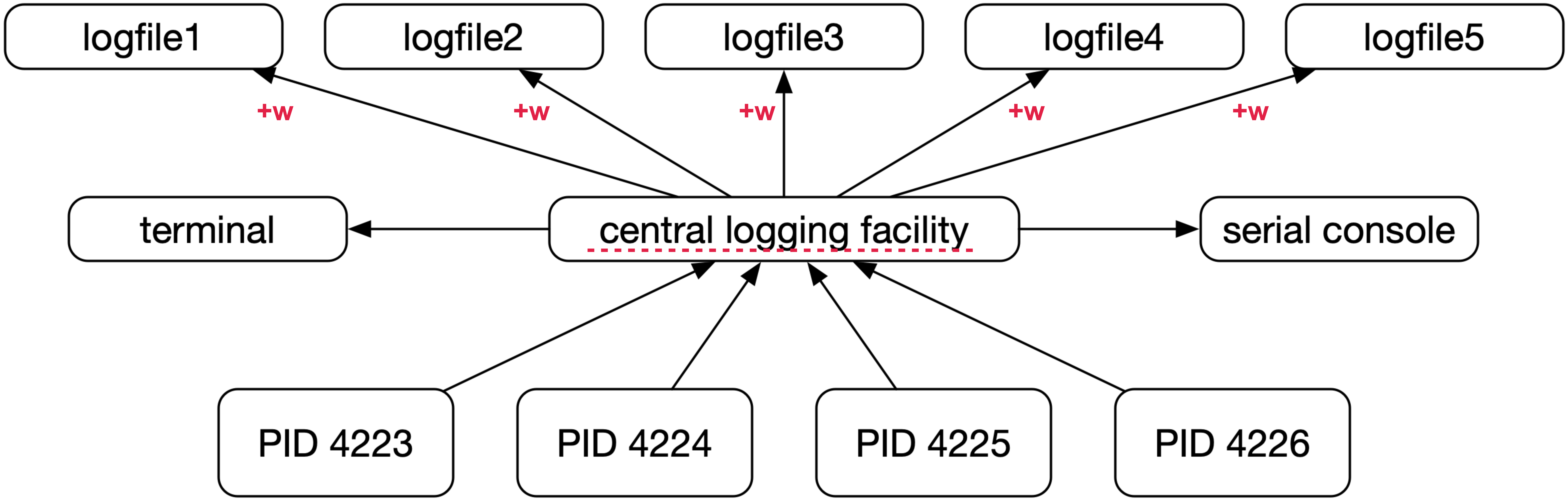

terminal
logfile1
logfile3
PID 4223
PID 4224
serial console
logfile2
terminal


terminal
logfile1
logfile3
PID 4223
PID 4224
serial console
logfile2
terminal


terminal
logfile1
logfile3
PID 4223
PID 4224
serial console
logfile2
terminal
PID 4225
logfile4



terminal
logfile1
logfile3
+w
+w
PID 4223
PID 4224
+w
+w
+w
+w
serial console
logfile2
terminal
+w
+w
+w
PID 4225
PID 4226
logfile4
logfile5



logfile1

logfile2

logfile3

logfile4

logfile5

+w

+w

+w

+w

+w

terminal

central logging facility

serial console

PID 4223

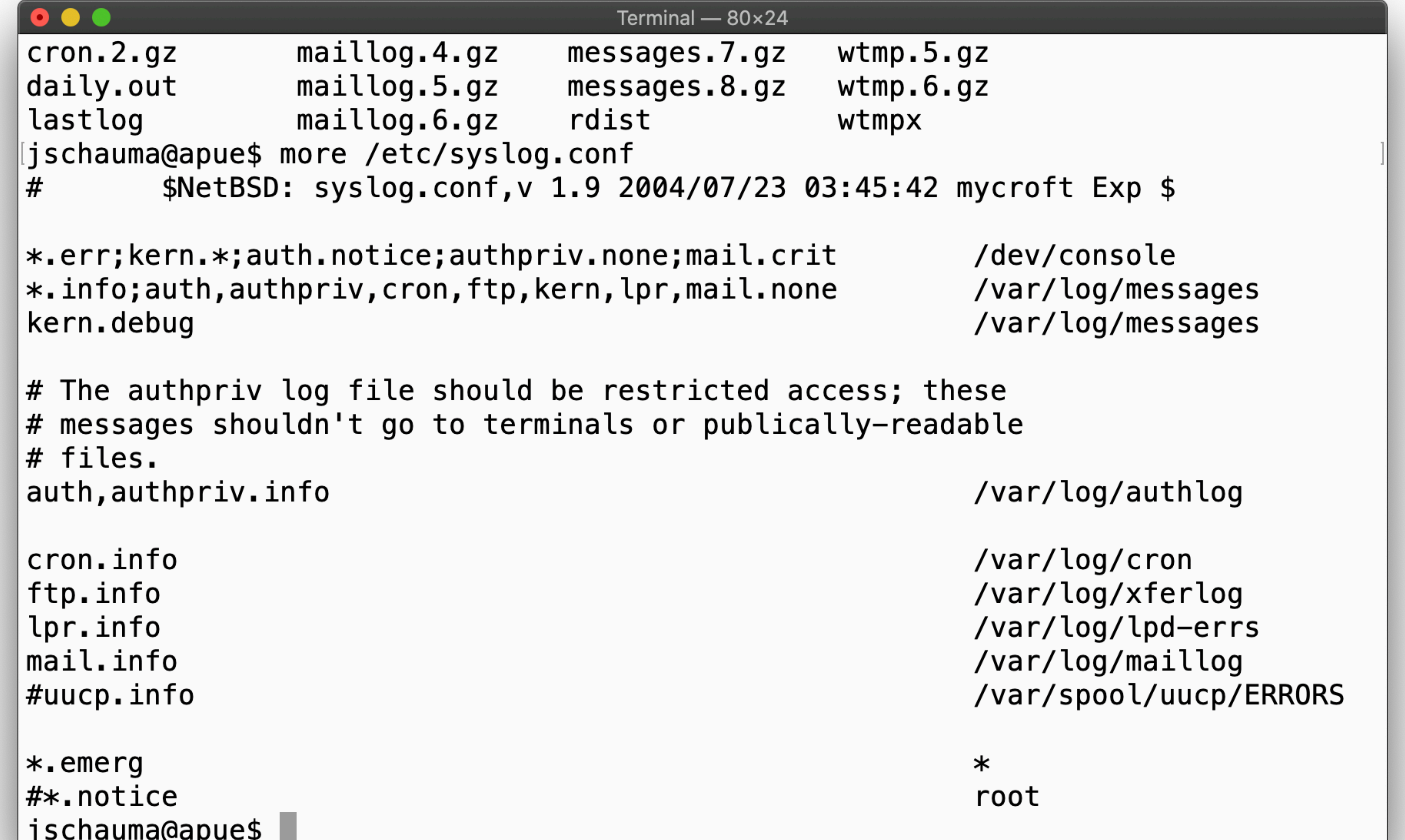
PID 4224

PID 4225

PID 4226

Jan Schaumann @jschauma · 21h

syslogd(8) be like

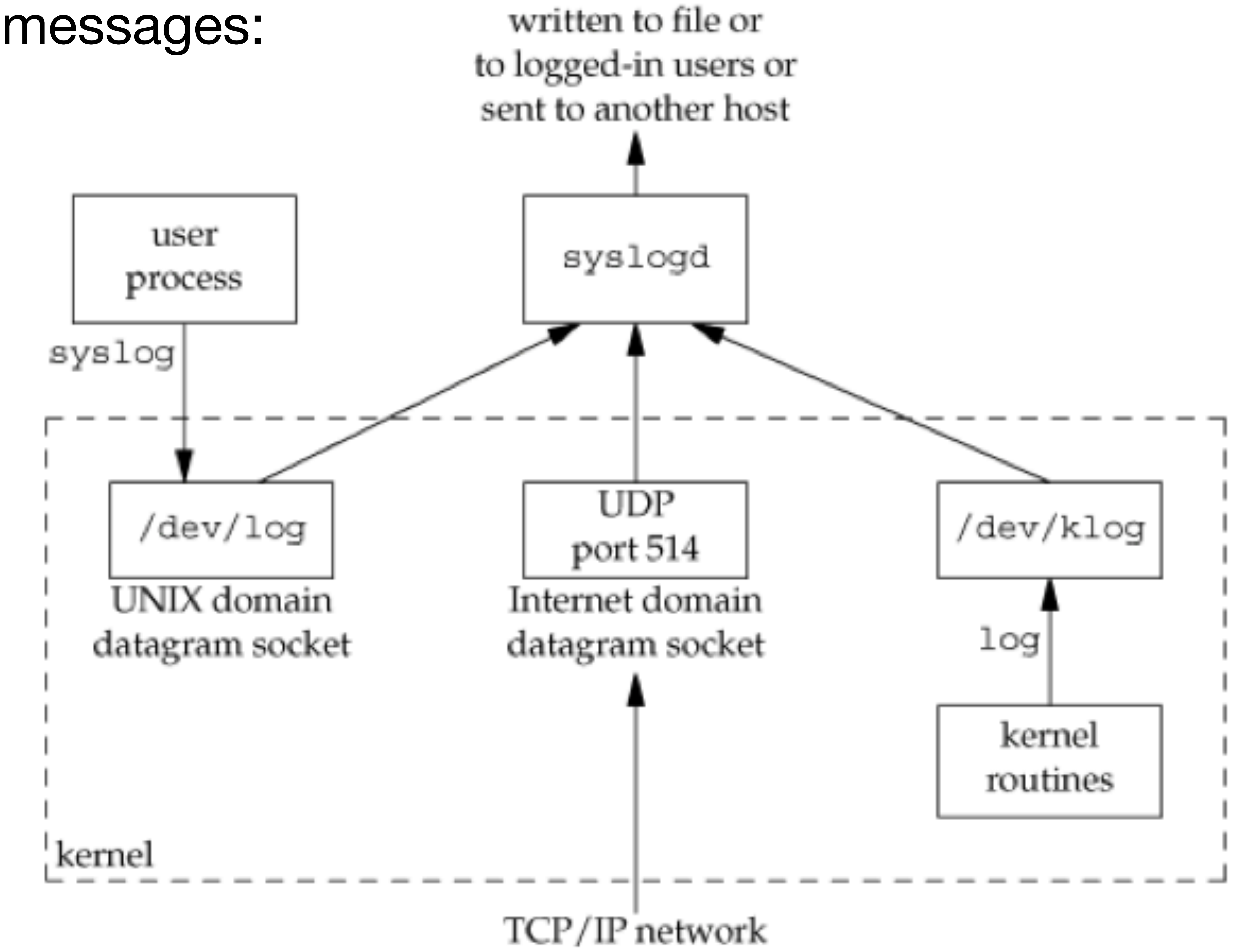


```
cron.2.gz       maillog.4.gz    messages.7.gz   wtmp.5.gz
daily.out       maillog.5.gz    messages.8.gz   wtmp.6.gz
lastlog         maillog.6.gz    rdist           wtmpx
jschauma@apue$ more /etc/syslog.conf
#       $NetBSD: syslog.conf,v 1.9 2004/07/23 03:45:42 mycroft Exp $

*.err;kern.*;auth.notice;authpriv.none;mail.crit        /dev/console
*.info;auth,authpriv,cron,ftp,kern,lpr,mail.none        /var/log/messages
kern.debug                                              /var/log/messages

# The authpriv log file should be restricted access; these
# messages shouldn't go to terminals or publically-readable
# files.
auth,authpriv.info                                      /var/log/authlog

cron.info                                               /var/log/cron
ftp.info                                                /var/log/xferlog
lpr.info                                                /var/log/lpd-errs
mail.info                                               /var/log/maillog
#uucp.info                                              /var/spool/uucp/ERRORS

*.emerg                                                 *
#*.notice                                               root
jschauma@apue$
```

syslogd(8)

There are three ways to generate log messages:

- via the kernel routine log(9)
- via the userland routine syslog(3)
- via UDP messages to port 514



syslog(3)

```
#include <syslog.h>

void openlog(const char *ident, int logopt, int facility);

void syslog(int priority, const char *message, ...);
```

openlog(3) allows us to set specific options when logging:

- prepend *ident* to each message
- specify logging options (such as LOG_CONS | LOG_PERROR | LOG_PID)
- specify a *facility* (such as LOG_DAEMON, LOG_MAIL etc.)

syslog(3) writes a message to the system message logger, tagged with *priority*. A *priority* is a combination of a *facility* (as above) and a level (such as LOG_DEBUG, LOG_WARNING or LOG_EMERG).

syslog(3)

Terminal — 159×24

```
           logger -p local0.notice -t HOSTIDM -f /dev/idmc

SEE ALSO
     syslog(3), syslogd(8)

STANDARDS
     The logger utility conforms to IEEE Std 1003.2-1992 ("POSIX.2").

NetBSD 9.0                     April 26, 2012                     NetBSD 9.0
jschauma@apue$ logger -p local0.info "A logging logger logs local logs."
jschauma@apue$ logger -p user.info "A logging logger logs local logs."
jschauma@apue$ logger -p user.notice "A logging logger logs local logs."
jschauma@apue$ logger -p user.debug "Debug messages are discarded, just like in
fo messages."
jschauma@apue$ logger -p user.warning "Warning: this will get logged."
jschauma@apue$ logger -p daemon.emerg "This is a test of the emergency broadcas
t system."

Message from syslogd@apue at Nov 19 19:59:21 ...
Nov 19 19:59:21 apue jschauma: This is a test of the emergency broadcast system
.
jschauma@apue$
  3 sh
```

```
Nov 19 19:54:27 apue slogdemo[2635]: SIGUSR
Nov 19 19:56:25 apue syslogd[1962]: last message repeated 3 times
Nov 19 19:56:48 apue slogdemo[1957]: somebody sent us SIGQUIT
Nov 19 19:58:24 apue jschauma: A logging logger logs local logs.
Nov 19 19:59:03 apue jschauma: Warning: this will get logged.

Message from syslogd@apue at Nov 19 19:59:21 ...
Nov 19 19:59:21 apue jschauma: This is a test of the emergency broadcast system
.
^C
jschauma@apue$ tail messages
Nov 19 19:54:27 apue slogdemo[2635]: SIGUSR
Nov 19 19:54:33 apue slogdemo[2635]: received SIGINFO
Nov 19 19:54:51 apue slogdemo[2635]: SIGUSR
Nov 19 19:55:25 apue syslogd[1962]: last message repeated 2 times
Nov 19 19:56:41 apue slogdemo[1957]: received SIGINFO
Nov 19 19:56:48 apue slogdemo[1957]: somebody sent us SIGQUIT
Nov 19 19:57:51 apue jschauma: A logging logger logs local logs.
Nov 19 19:58:25 apue syslogd[1962]: last message repeated 2 times
Nov 19 19:59:03 apue jschauma: Warning: this will get logged.
Nov 19 19:59:21 apue jschauma: This is a test of the emergency broadcast system
.
jschauma@apue$
  0 sh
```

syslog(3)

- De-facto standard for message logging on Unix systems since the 1980s.
- Documented in RFC3164, now standardized in RFC5424.
- On the network, defaults to UDP port 514.
- Various newer versions with many new features (TCP, TLS, logging to a database or a filter, …) available, e.g., syslog-ng, rsyslog.
- Quickly leads to large-scale messaging systems including e.g., Elasticsearch, Solr, Flume, Fluentd, …

- See also: log(9), logger(1), syslog(3), syslog.conf(5), syslogd(8)