UNIX vs. MPE Administration

e3000 Solutions Symposium 2002

Migration Track: Session #032

Chris Wong

Cerius Technology Group, Inc.

cwong@cerius.com

http://newfdog.hpwebhost.com

Agenda

- Introduction
- “Why” instead of only “how”
- Based on your existing MPE knowledge
- Processes, Session
- Internet Daemon
- Login
- Variables
- File System
- File Types
- Jobs: Management
- Jobs: Standard List
- Role Based Unix Environment

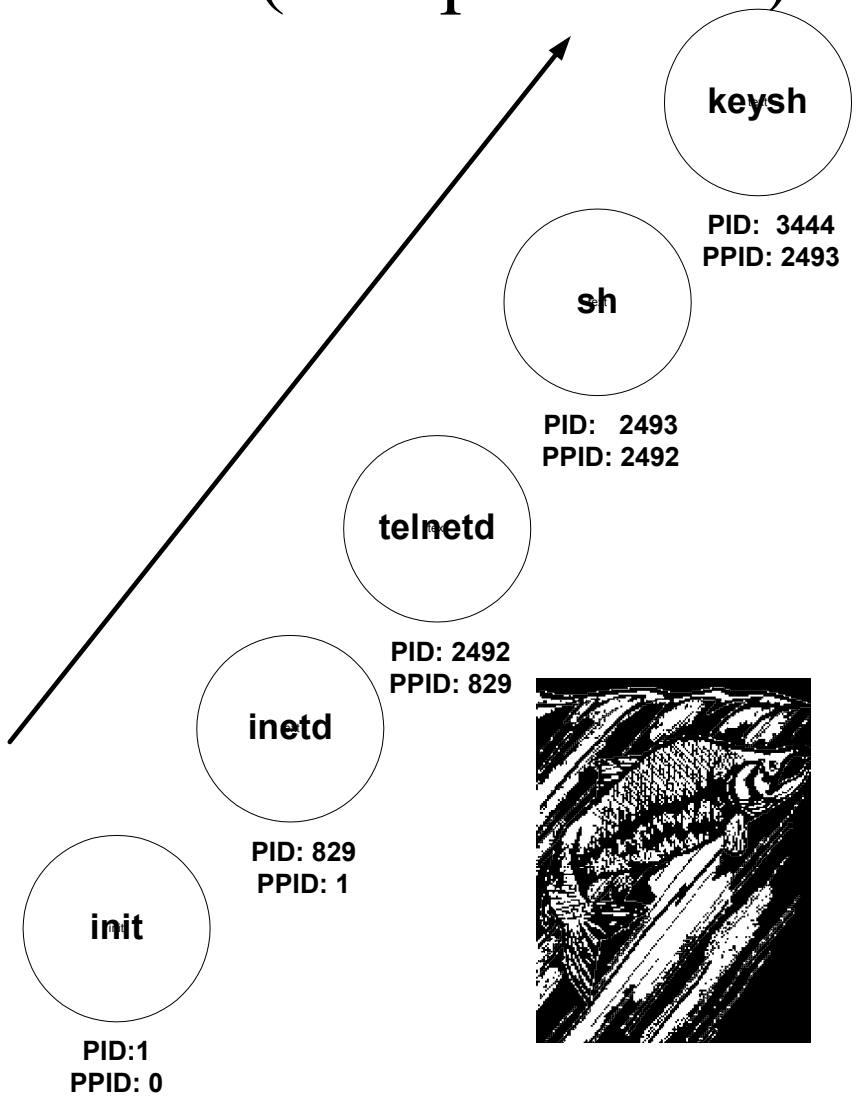
SHOWME

- **MPE/iX:**
- USER: #S266,MANAGER.SYS,SYSMGR (NOT IN BREAK)
- RELEASE: C.70.00 MPE/iX HP31900 C.39.06 USER VERSION: C.70.00
- CURRENT: WED, OCT 17, 2001, 10:57 AM
- LOGON: WED, OCT 17, 2001, 10:57 AM
- CPU SECONDS: 1 CONNECT MINUTES: 1
- $STDIN LDEV: 8 $STDLIST LDEV: 8
- **HP-UX:**
- **ps:** root 2493 *2492* 6 13:08:40 console 0:00 *-sh*
- **who -T**: root + console Oct 17 10:19 . 2493 system console
- **uname -a**: HP-UX ctg800 B.11.11 U 9000/811 2007963370 unlimited-user license

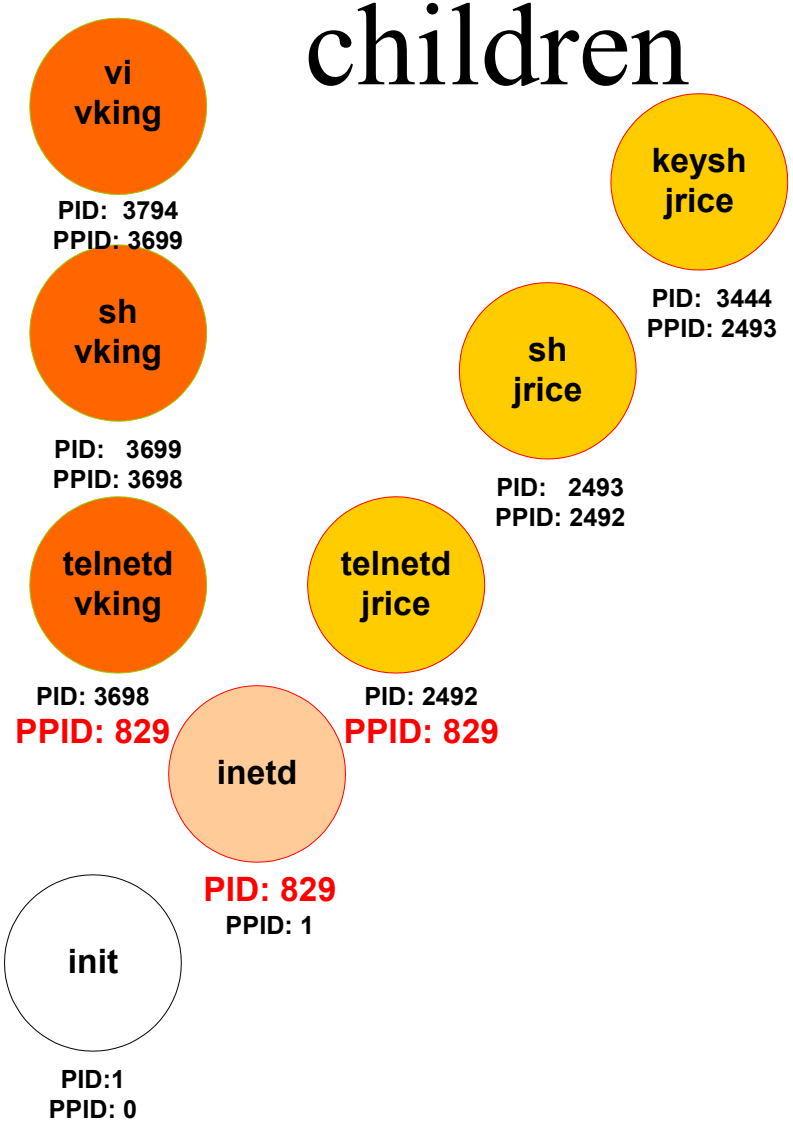
HP-UX Processes

- jrice ***2493 2492*** 6 13:08:40 pts/tc 0:00 -sh
- jrice starts another shell, the keysh
- jrice ***3444 2493*** 20 13:52:21 pts/tc 0:00 keysh
- Every process has its own process ID (PID)
- Every process has a parent process ID (PPID)
- Parents spawn children
- Parent/Child Relationships

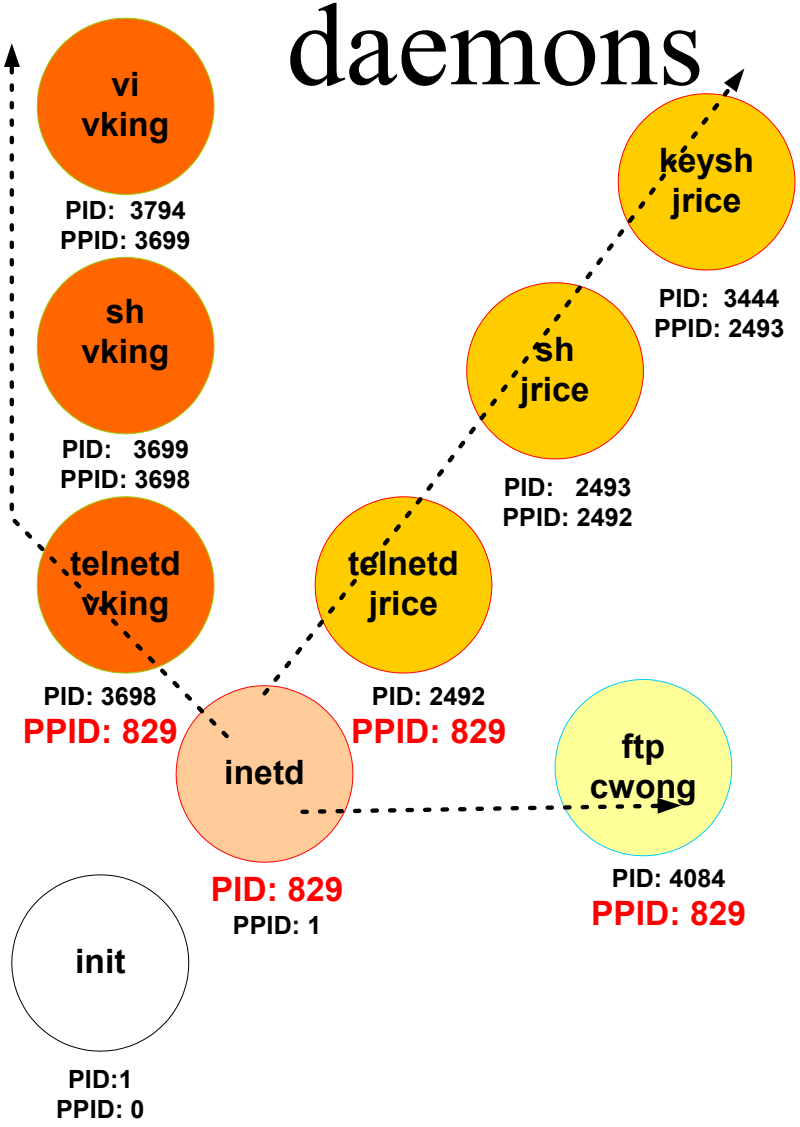
Every process is spawned from another (except for init)



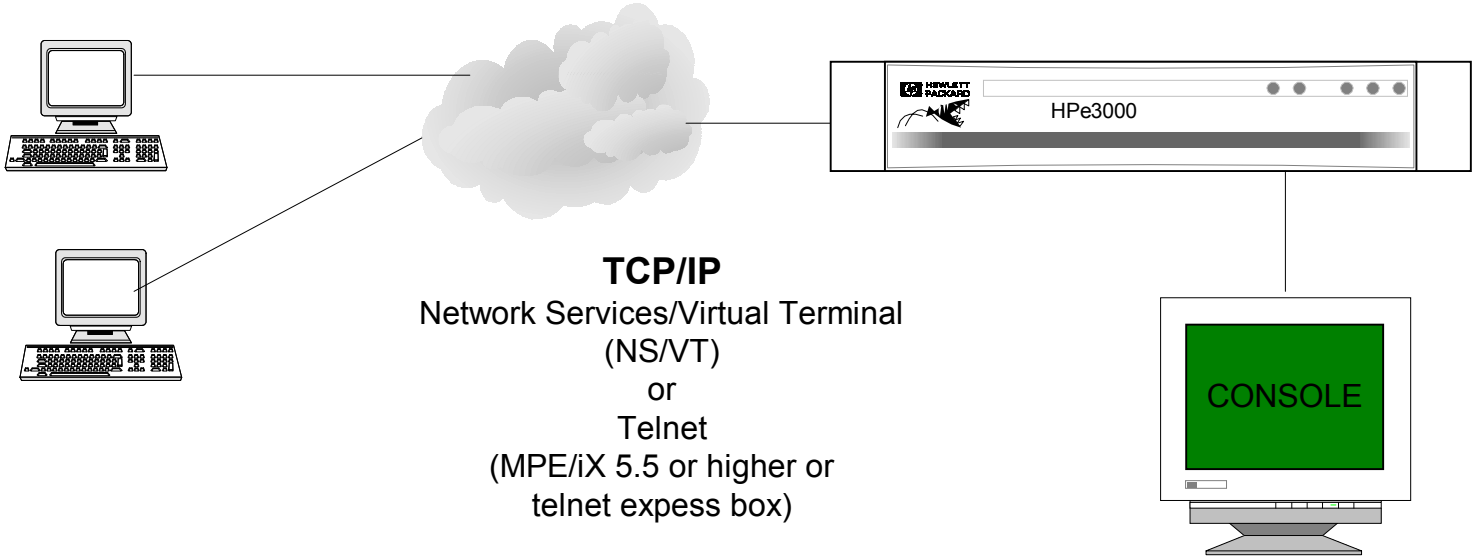
One parent can have multiple children



inetd can spawn many different daemons



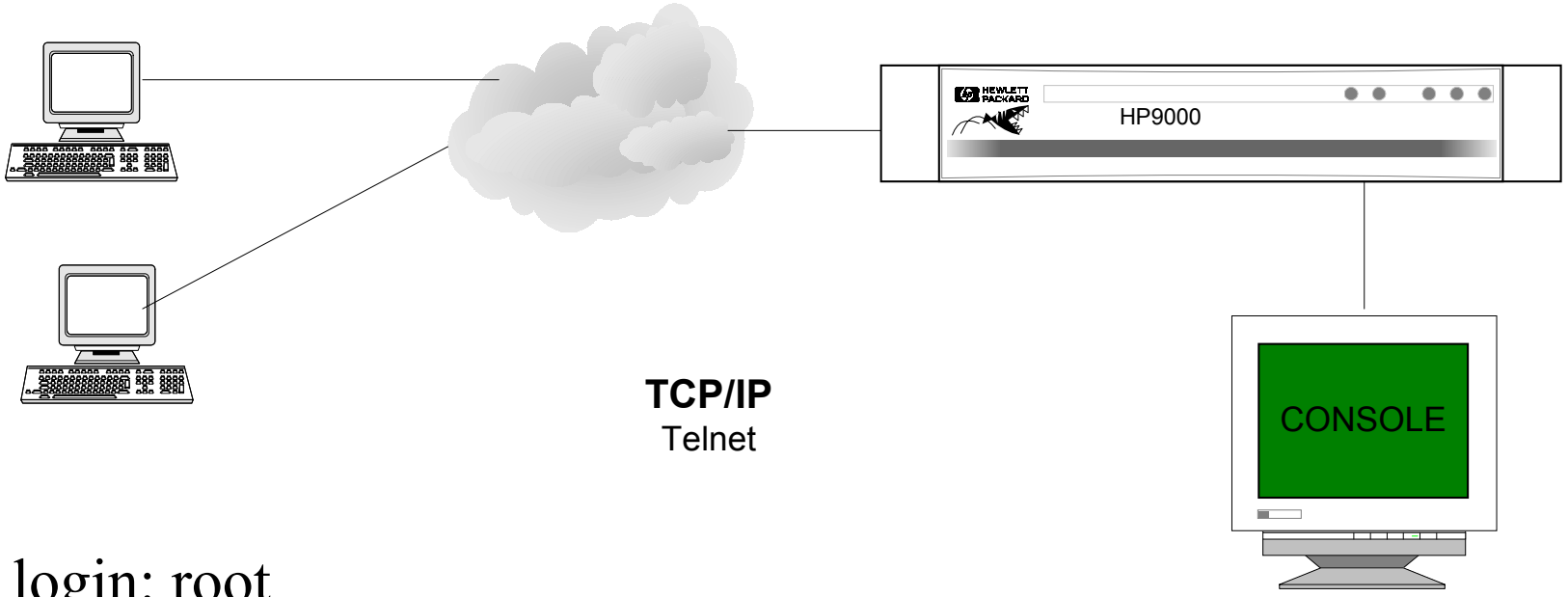
MPE/iX
User Starting a Session



TCP/IP
Network Services/Virtual Terminal
(NS/VT)
or
Telnet
(MPE/iX 5.5 or higher or
telnet express box)

MPE/iX: HELLO USER.ACCOUNT

HP-UX
User Starting a Session



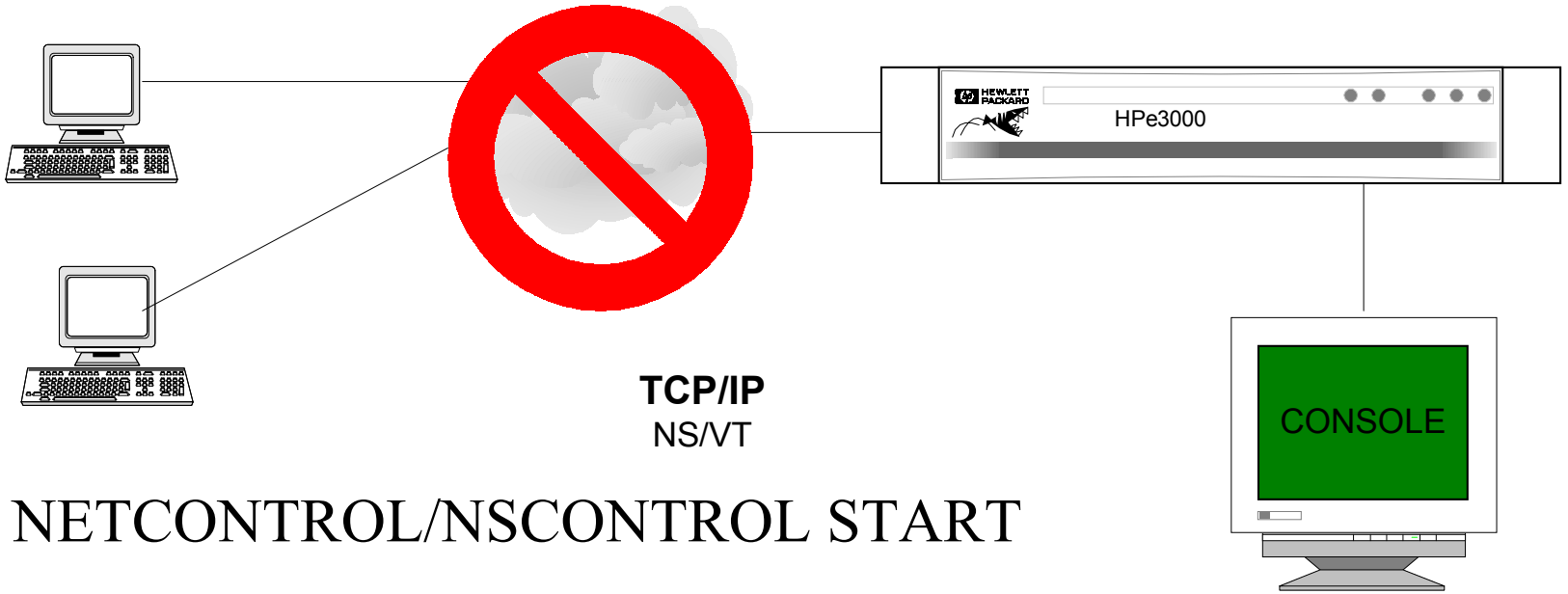
TCP/IP
Telnet

login: root

Starting a Session

- **MPE/iX**
  - TCP/IP
    - NS/VT or Telnet
  - Prompt: MPE/iX:
  - User name used with the “HELLO” command
    - USER.ACCOUNT
      - OPERATOR.SYS
    - SESSION,USER.ACCOUNT
- **HP-UX**
  - TCP/IP
    - Telnet
    - Secure replacements available
  - Prompt: login:
  - User name:
    - up to 8 characters/digits
      - bsmith

Problems starting Session MPE/iX

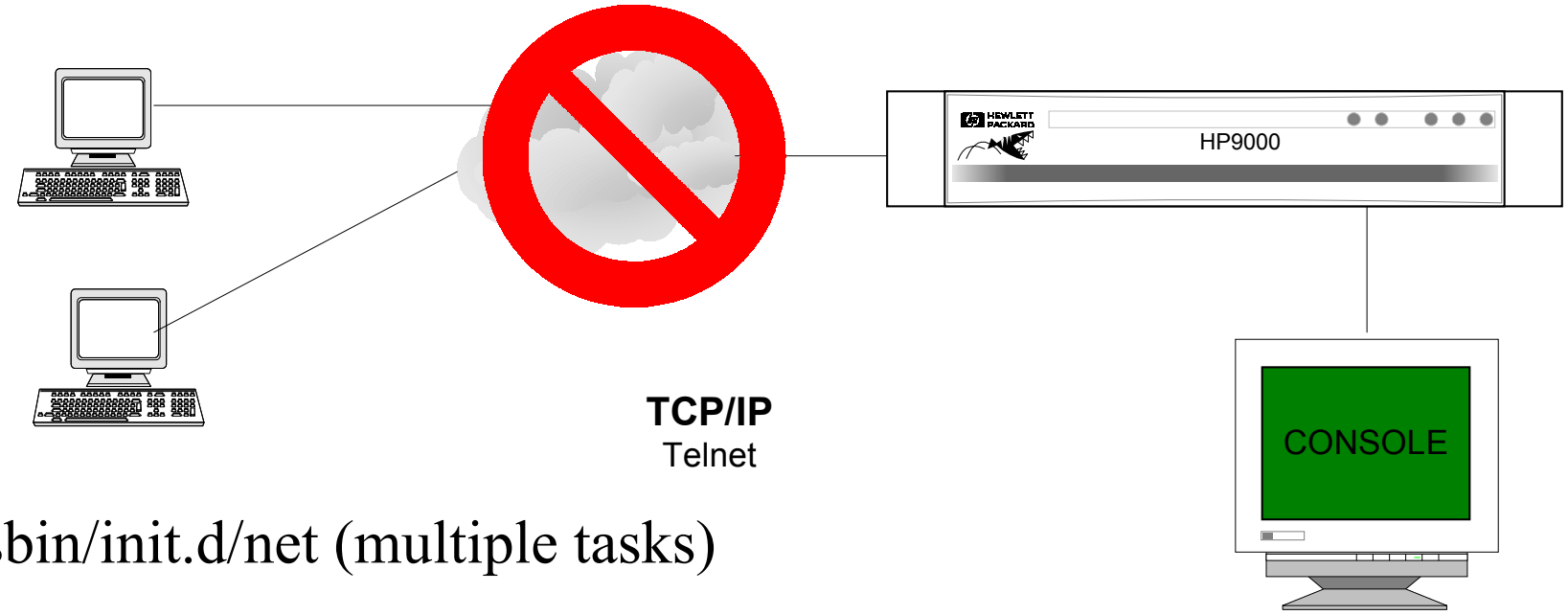


NETCONTROL/NSCONTROL START

INPRI is equal or less than JOBFENCE

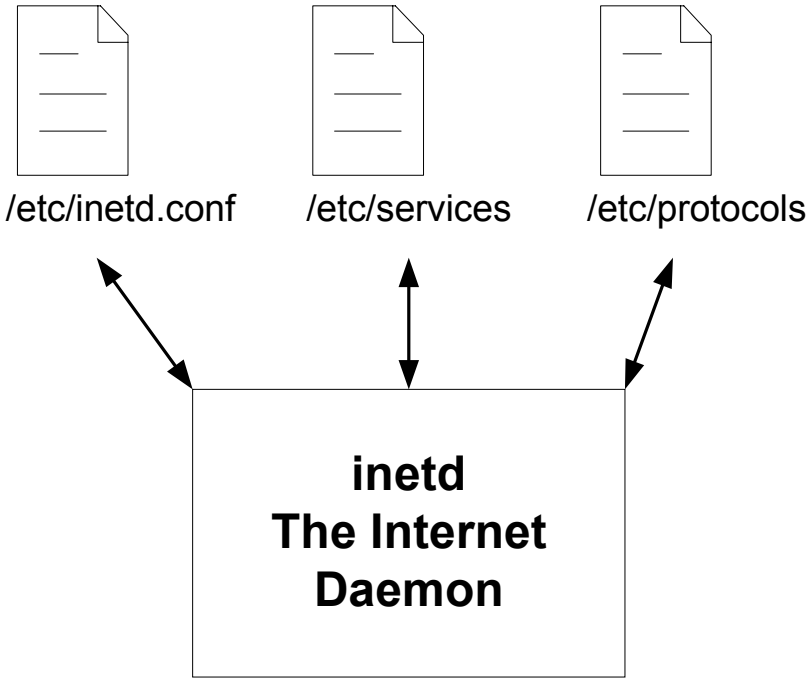
Session LIMIT exceeded

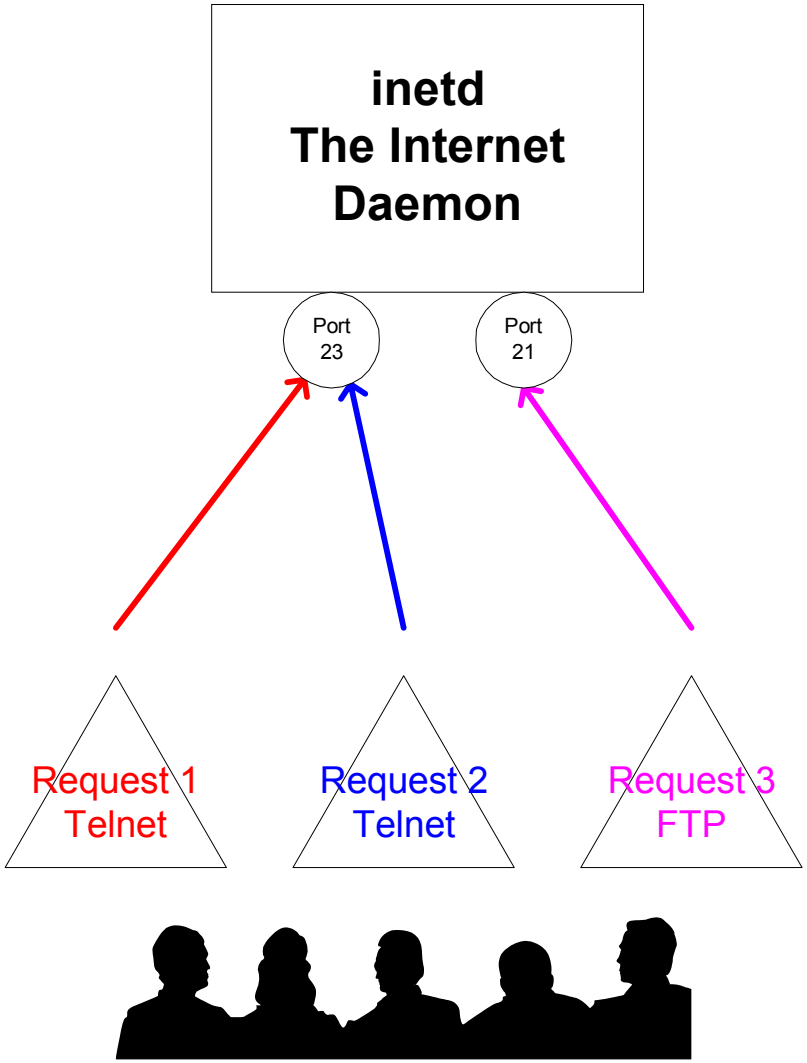
Problem starting Session
HP-UX



/sbin/init.d/net (multiple tasks)

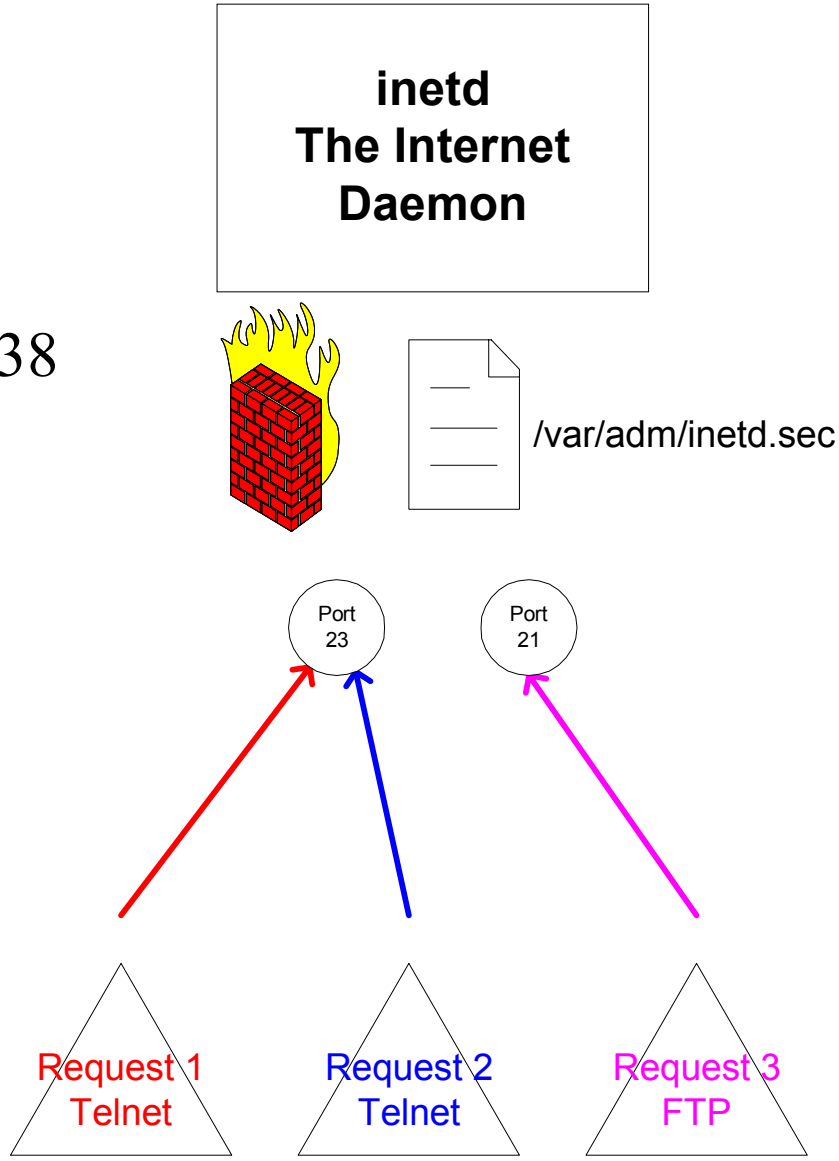
The Internet Daemon

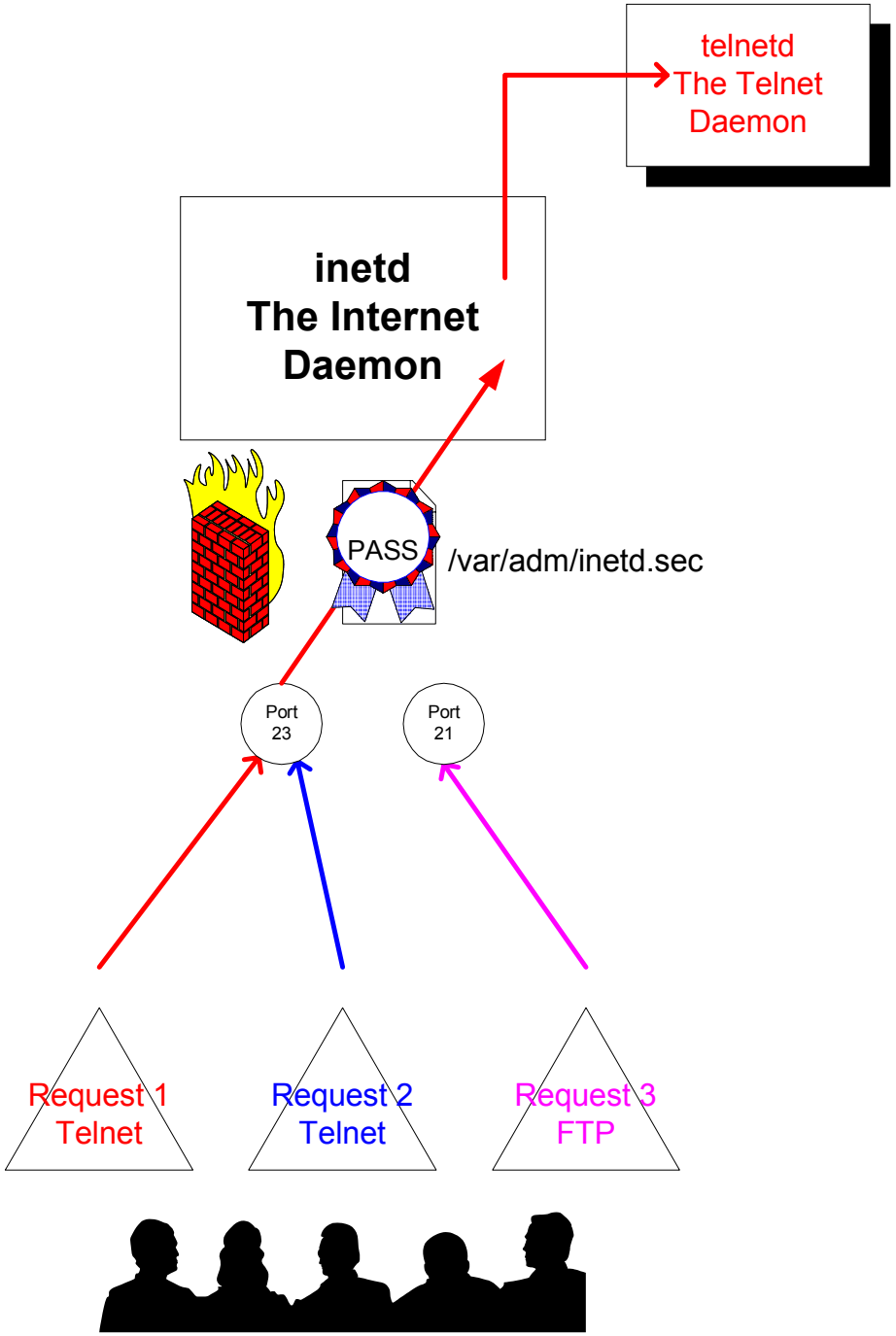


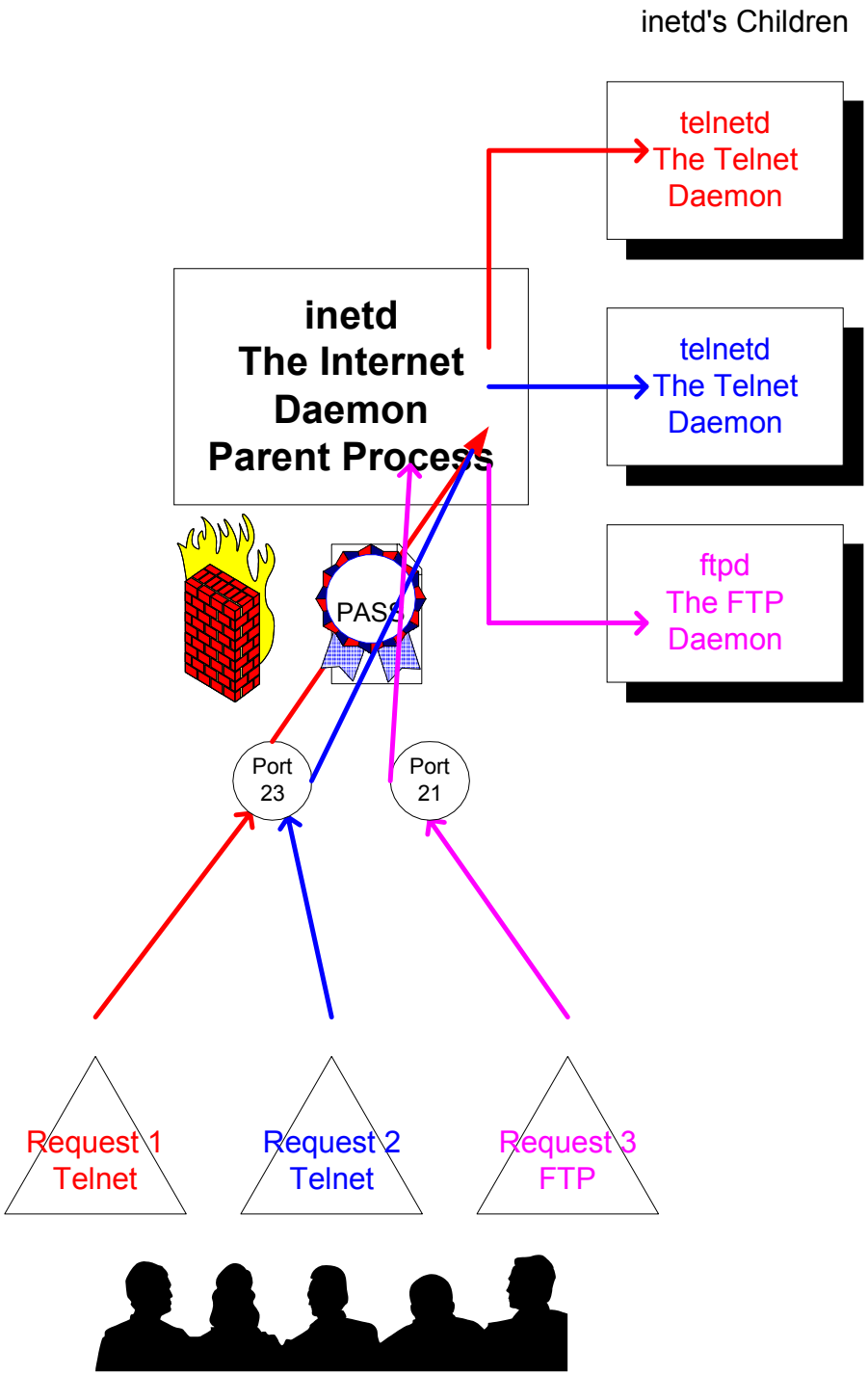

inetd
The Internet
Daemon
Port
23
Port
21
Request 1
Telnet
Request 2
Telnet
Request 3
FTP

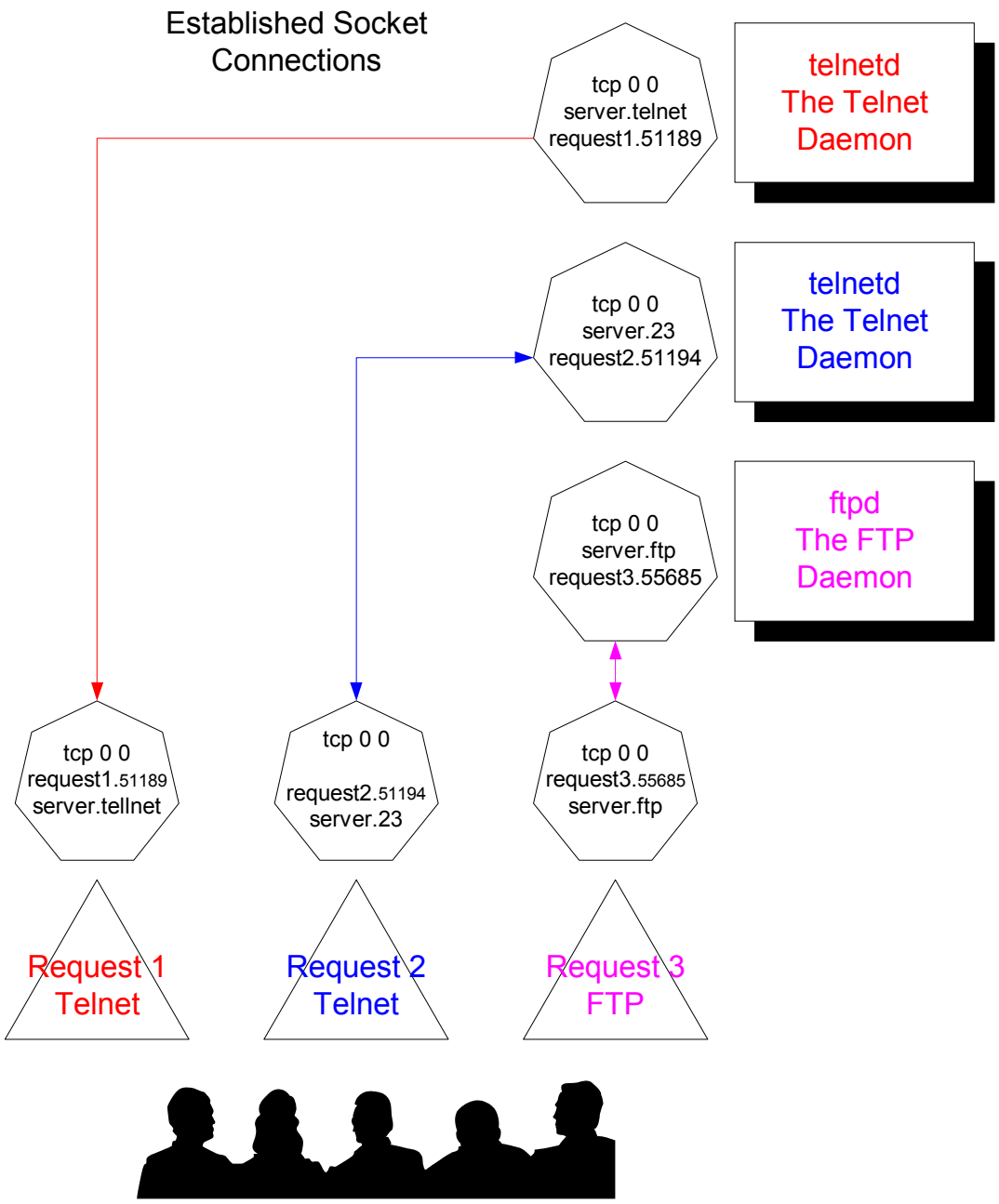
telnet allow
192.168.1.100-138

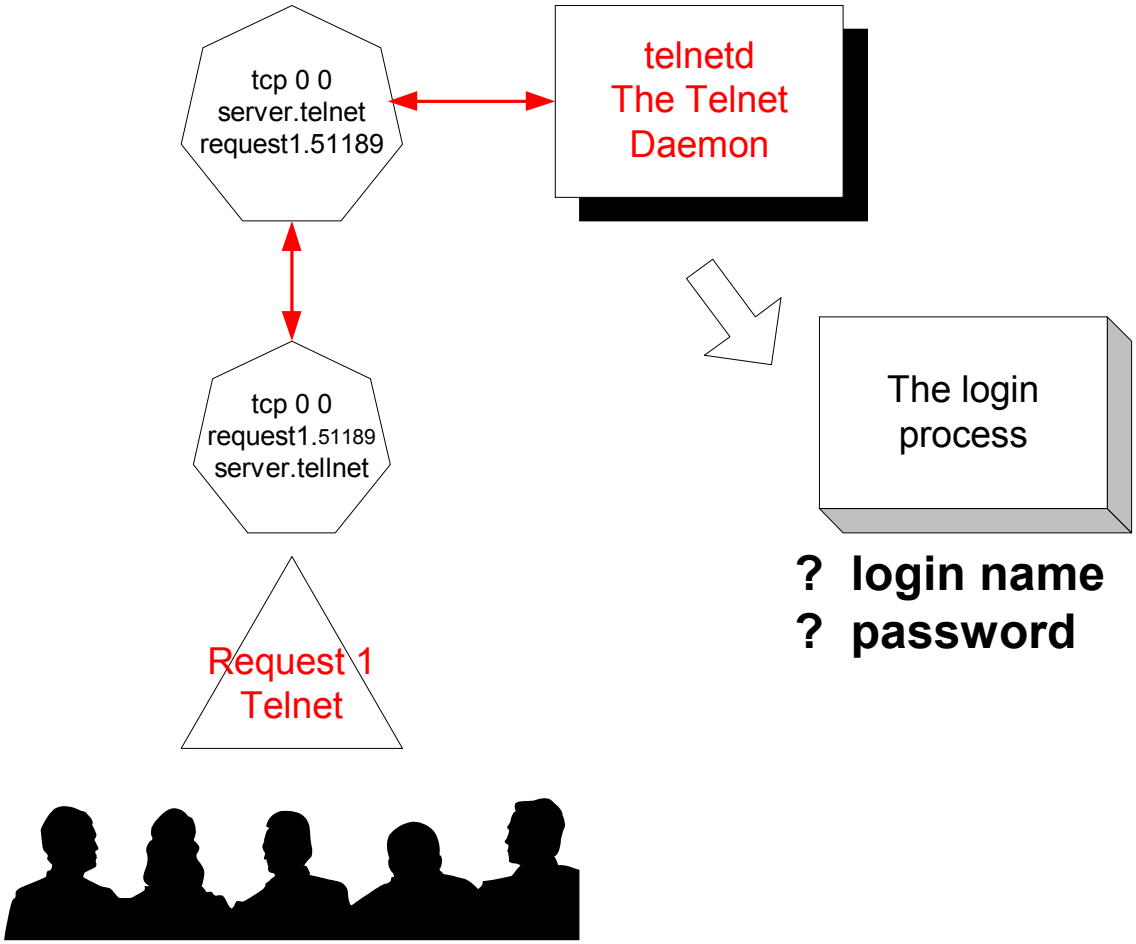
ftp deny host123



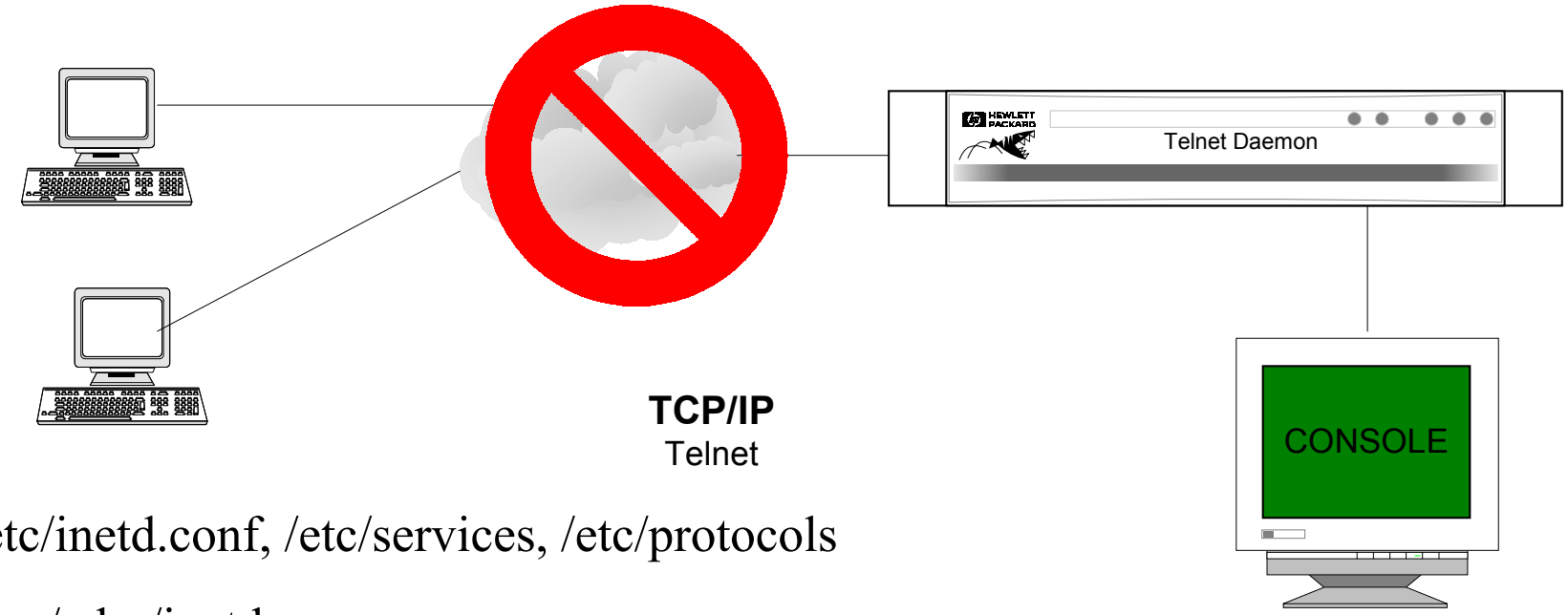

telnetd
The Telnet
Daemon
inetd
The Internet
Daemon
PASS
/var/adm/inetd.sec
Port
23
Port
21
Request 1
Telnet
Request 2
Telnet
Request 3
FTP


inetd's Children
telnetd
The Telnet
Daemon
inetd
The Internet
Daemon
Parent Process
telnetd
The Telnet
Daemon
ftpd
The FTP
Daemon
PASS
Port
23
Port
21
Request 1
Telnet
Request 2
Telnet
Request 3
FTP


Established Socket Connections
tcp 0 0
server.telnet
request1.51189
telnetd
The Telnet
Daemon
tcp 0 0
server.23
request2.51194
telnetd
The Telnet
Daemon
tcp 0 0
server.ftp
request3.55685
ftpd
The FTP
Daemon
tcp 0 0
request1.51189
server.tellnet
tcp 0 0
request2.51194
server.23
tcp 0 0
request3.55685
server.ftp
Request 1
Telnet
Request 2
Telnet
Request 3
FTP


tcp 0 0
server.telnet
request1.51189
telnetd
The Telnet
Daemon
The login
process
? login name
? password
tcp 0 0
request1.51189
server.tellnet
Request 1
Telnet

Problem starting Session Telnet



/etc/inetd.conf, /etc/services, /etc/protocols

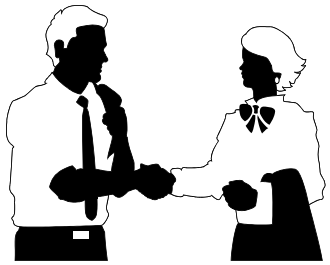
/var/adm/inetd.sec

inetd not running, no available terminals

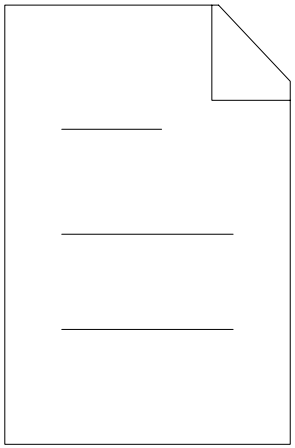
tcpwrapper, IPSec, IPFilter

Verifying the user

The login process



2 credentials:
User name
Password



/etc/passwd

- User name
- Password
- UID (User ID)
- GID (Group ID)
- GECOS (+4 fields)
- Home Directory
- Program to start or the default shell

The login process

- **MPE/iX**
  - Checks login name
  - Checks password(s)
  - Displays welcome msg
  - Runs logon UDC(s)
- **HP-UX**
  - Checks login name
  - Checks password(s)
  - Checks for activation status, terminal, time of day,nologin, aging
  - Auto exec files based on shell

Auto Executable File at login

- **ksh (rksh) and sh (rsh) (both POSIX and Bourne)**
  - /etc/profile
  - $HOME/.profile
- **csh**
  - /etc/csh.login
  - $HOME/.cshrc and $HOME/.login
- **keysh**
  - /etc/profile
  - $HOME/.profile
  - $HOME/.keyshrc

The profile files

- **/etc/profile**
  - Default PATH, MANPATH, TIMEZN
  - TERM, ERASE
  - DISPLAY CONTENTS OF: COPYRIGHT, MOTD
  - NOTIFY OF: MAIL, NEWS
- **$HOME/.profile**
  - TERM
  - PATH (added to)
  - EDITOR

Environment Variables
MPE/iX vs. HP-UX

- **MPE/iX**

- HPJOBNAME = BOBBY
- HPUSER = MANAGER
- HPACCOUNT = SYS
- HPHGROUP = SYSMGR
- HPCWD = /SYS/SYSMGR
- TZ = PST8PDT

- **HP-UX**

- LOGNAME=root
- HOME=/root
- PWD=/root
- TZ=PST8PDT
- *SHELL=/sbin/sh*

Environment Variables
MPE/iX Posix vs. HP-UX

- **MPE/iX Posix Shell**

- LOGNAME=MANAGER.SYS
- HOME=/SYS/SYSMGR
- HPCWD = /SYS/SYSMGR
- TZ = PST8PDT

- **HP-UX**

- LOGNAME=root
- HOME=/root
- PWD=/root
- TZ=PST8PDT
- *SHELL=/sbin/sh*

PATH Environment Variable

- **MPE/iX:** HPPATH = !HPGROUP,PUB,PUB.SYS,ARPA.SYS
- **MPE/iX Posix**: PATH=/usr/local/bin:/bin
- **HP-UX:**

  PATH=/usr/sbin:/usr/bin:/usr/ccs/bin:/usr/contrib/bin:/opt/mpi/bin:/opt/hparray/bin:/opt/nettladm/bin:/opt/upgrade/bin:/opt/fcms/bin:/usr/bin/X11:/usr/contrib/bin/X11:/opt/pd/bin:/opt/resmon/bin:/opt/ignite/bin:/opt/scr/bin:/opt/graphics/phigs/bin:/usr/sbin/stm/uut/bin/progs://opt/perl/bin:/opt/mx/bin:/opt/perf/bin:/opt/OV/bin/OpC:/sbin:/home/root
- Source another variable: MPE/iX: ! HP-UX: $
- Separate entries: MPE/iX: , HP-UX: :
- In general: POSIX = HP-UX

Source a variable

- In HP-UX the “$” sign is used with the variable name.
- For example, to add an entry to the PATH variable that is already set, instead of typing the entire PATH data over again, use the existing data and add to it.
- PATH=$PATH:/new/path

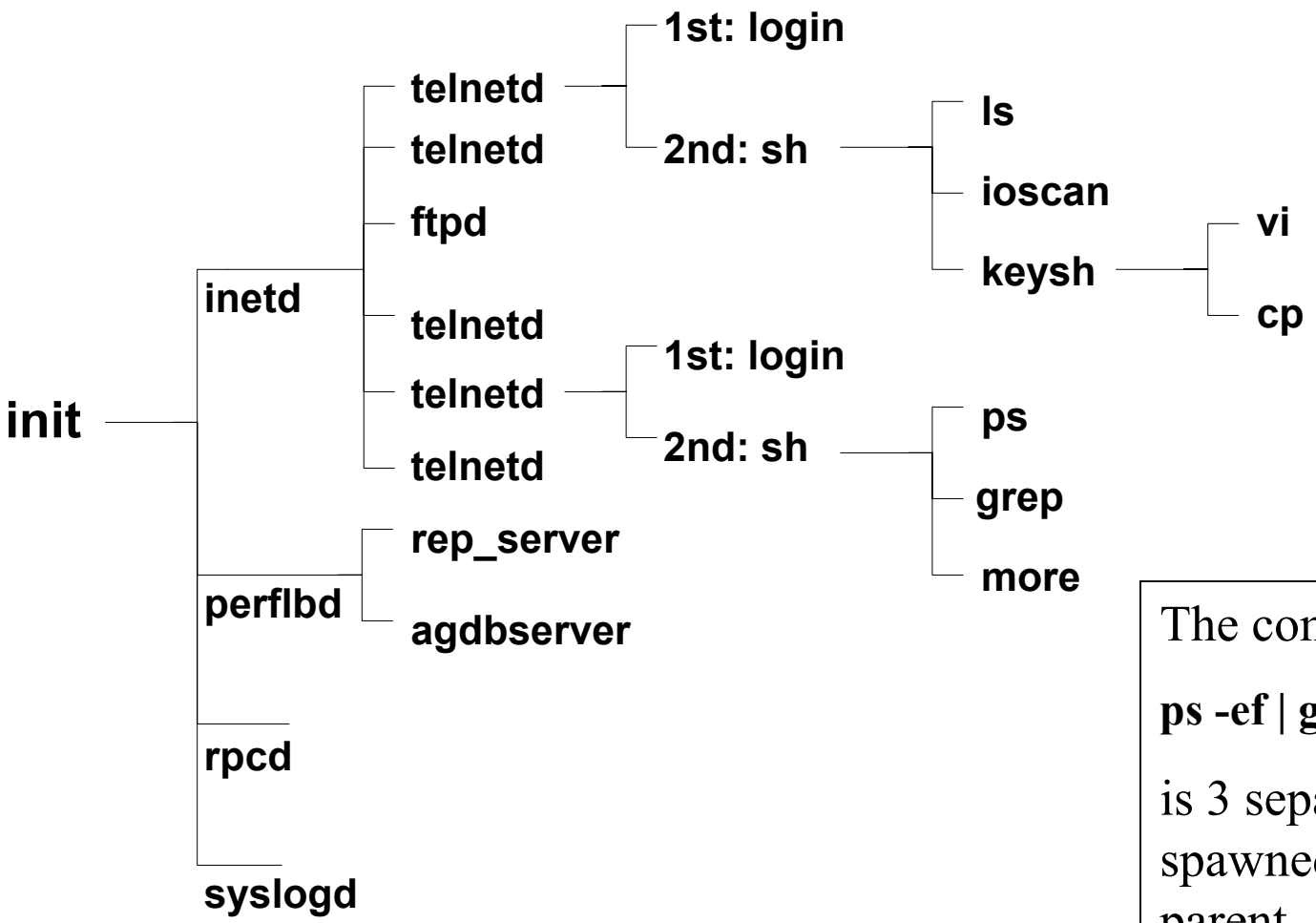
HP-UX Environment Variables

- Greatly used
- Most commonly used variables:
  - TERM, DISPLAY, ***HOME***, COLUMNS, EDITOR, SHELL, ERASE, ***PATH*** and ***MANPATH***
- Scripts depend on variables
  - Scripts start applications
  - $ORACLE_HOME
  - $DB2_HOME

Recalling Commands

- MPE/iX: listredo
- HP-UX:
  - Most common way is to use:
    - the {ESC} key with the {k} key.
  - Required environmental variables:
    - export EDITOR=vi
    - export HISTFILE=$HOME/.sh_history
    - export HISTSIZE=128 (default)
  - fc is also available

Process Tree



The command:

ps -ef | grep jrice | more

is 3 separate processes spawned from the same parent

Processes

- root 937 1 0 Feb 25 ? 0:11 /usr/sbin/inetd
- root 14179 937 0 15:03:19 pts/ta 0:00 telnetd -b /etc/banner.telnet
- jrice 14180 14179 0 15:03:19 pts/ta 0:00 -sh
- jrice 14211 14180 1 15:04:45 pts/ta 0:00 ps -fu jrice

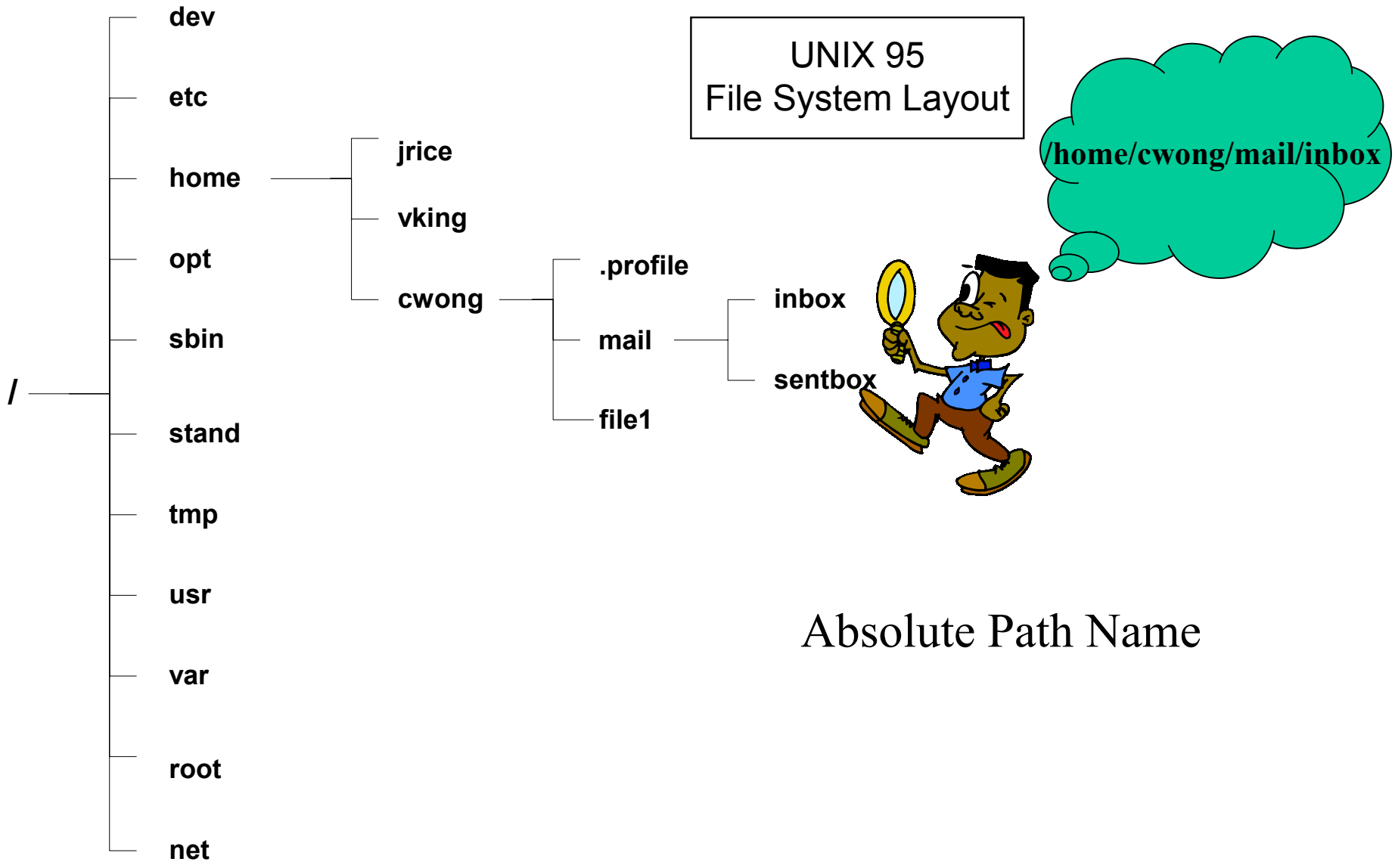
The login process

MPE

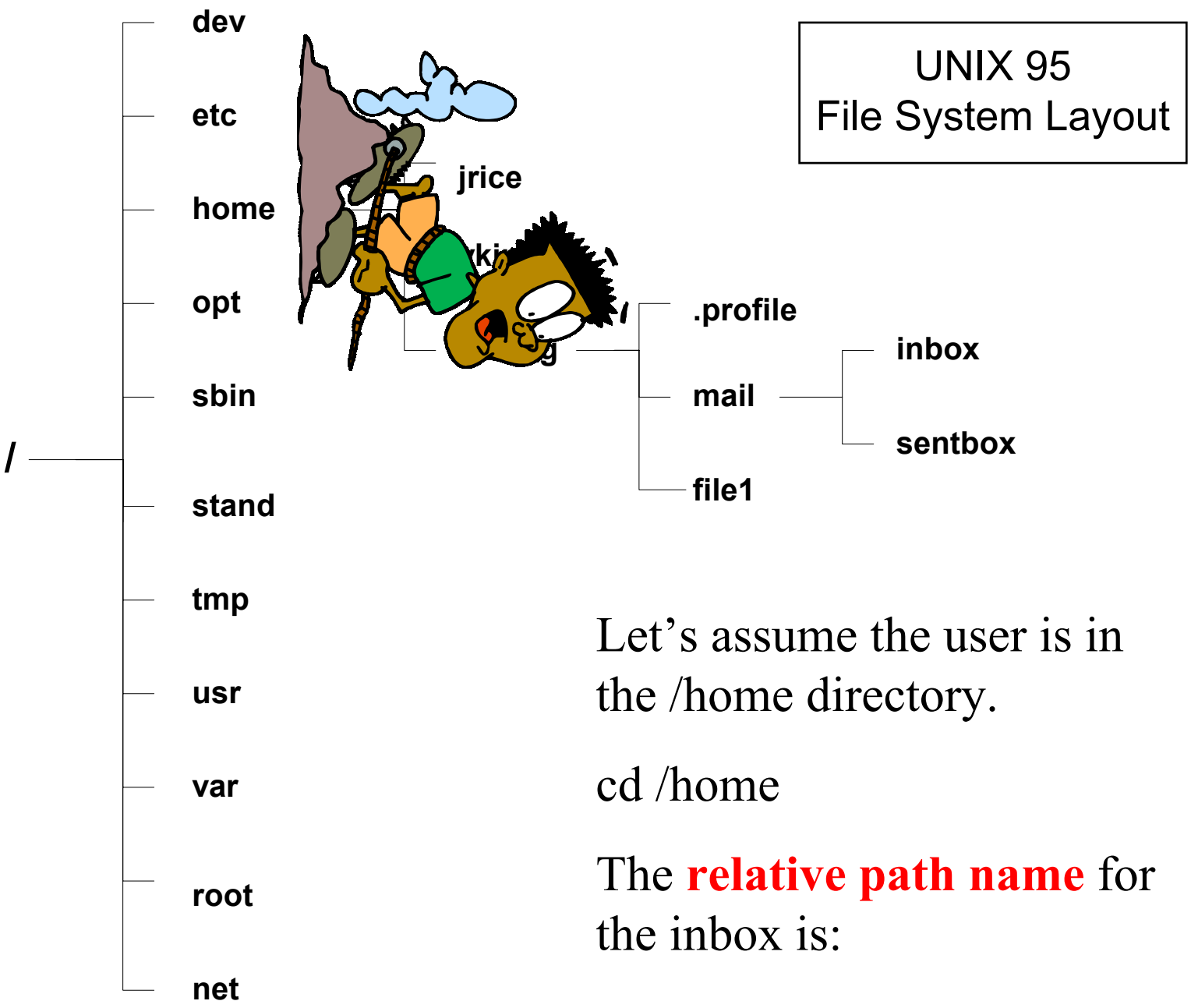
- Connect using telnet or NS/VT
- Checks the logon name
- Checks password(s)
- Checks the session limit
- Displays welcome message
- Runs logon UDC(s)
- Sets variables
- Sets JCWs
- Sets File equates
- Third party security
- Starts application or menu

UNIX

- Connect using telnet if Internet Daemon security is passed
- Displays the telnet banner
- Checks the login name and password
- Checks for trusted system security configurations
- Checks disk quotas
- Executes shell initialization scrips
- Sets variables
- Displays message of the day
- Displays copyright
- Checks for mail status
- Checks of news status
- Sets umask and mesg
- Starts application or menu



Absolute Path Name

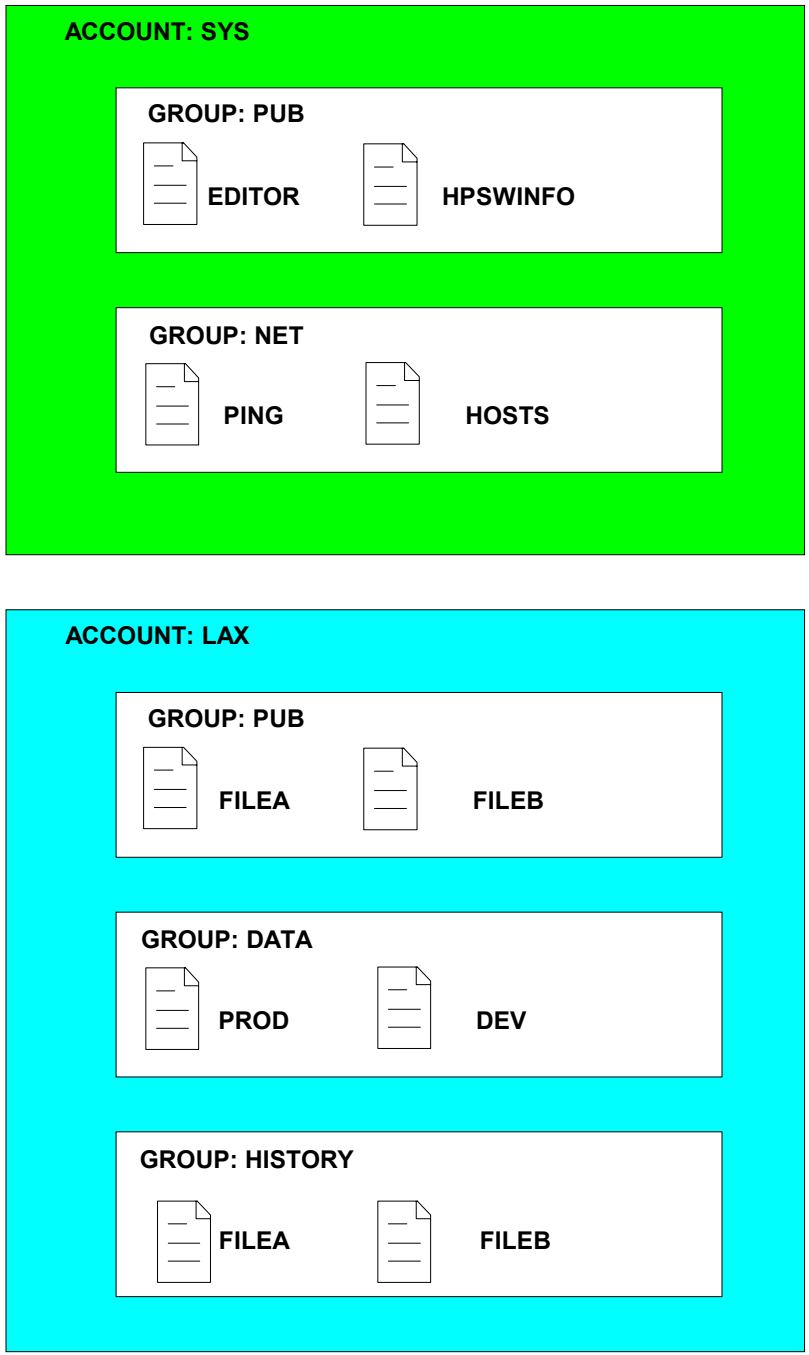


Let's assume the user is in the /home directory.

cd /home

The **relative path name** for the inbox is:

cwong/mail/inbox



The Original MPE File System (Prior to version 4.5)

Fully Qualified File Name

FILE.GROUP.ACCOUNT

EDITOR.PUB.SYS

HPSWINFO.PUB.SYS

PING.NET.SYS

HOSTS.NET.SYS

FILEA.PUB.LAX

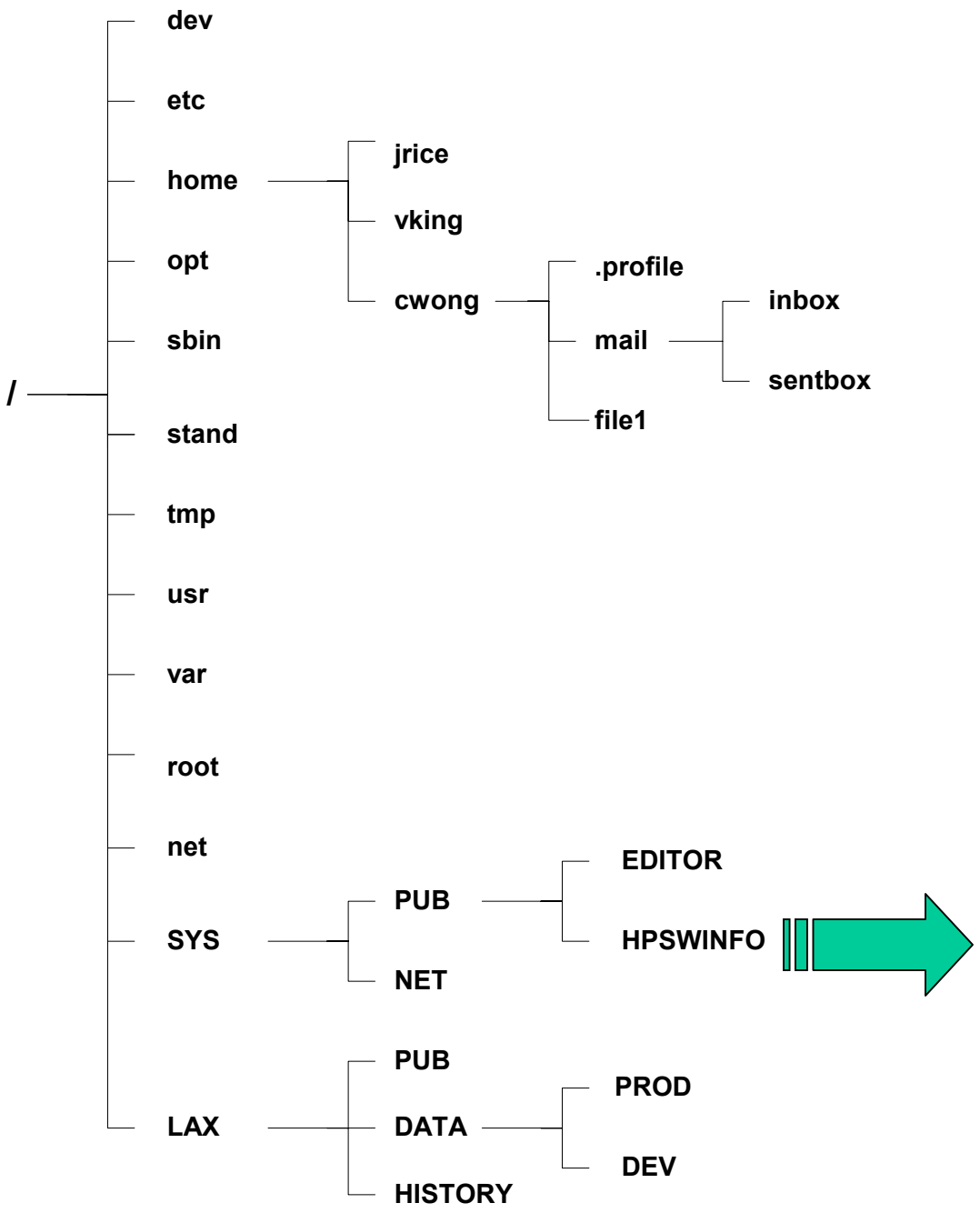
FILEB.PUB.LAX

PROD.DATA.LAX

DEV.DATA.LAX

FILEA.HISTORY.LAX

FILEB.HISTORY.LAX



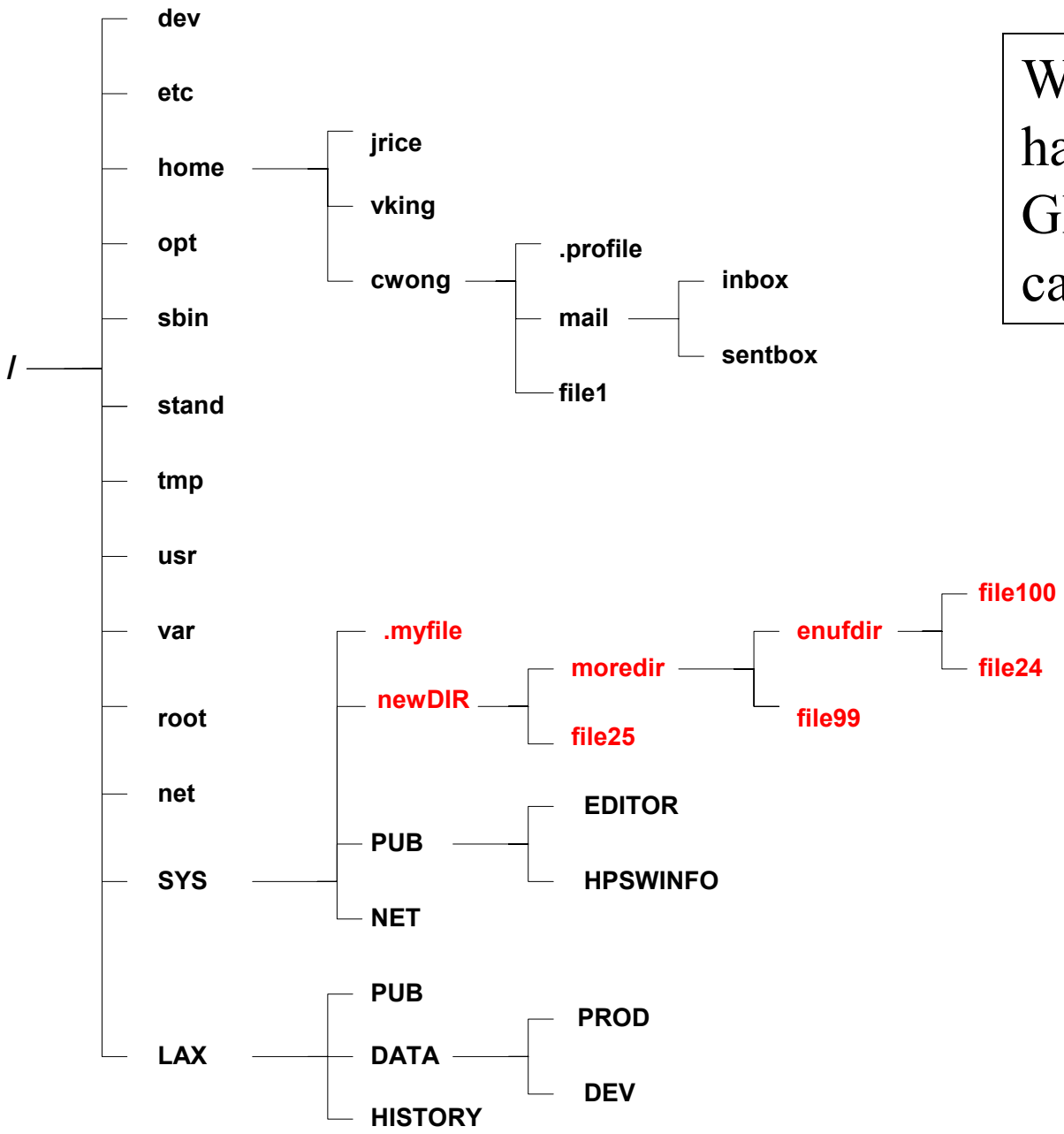
The MPE/iX Hierarchical File System (HFS)

The MPE Fully Qualified File:

HPSWINFO.PUB.SYS

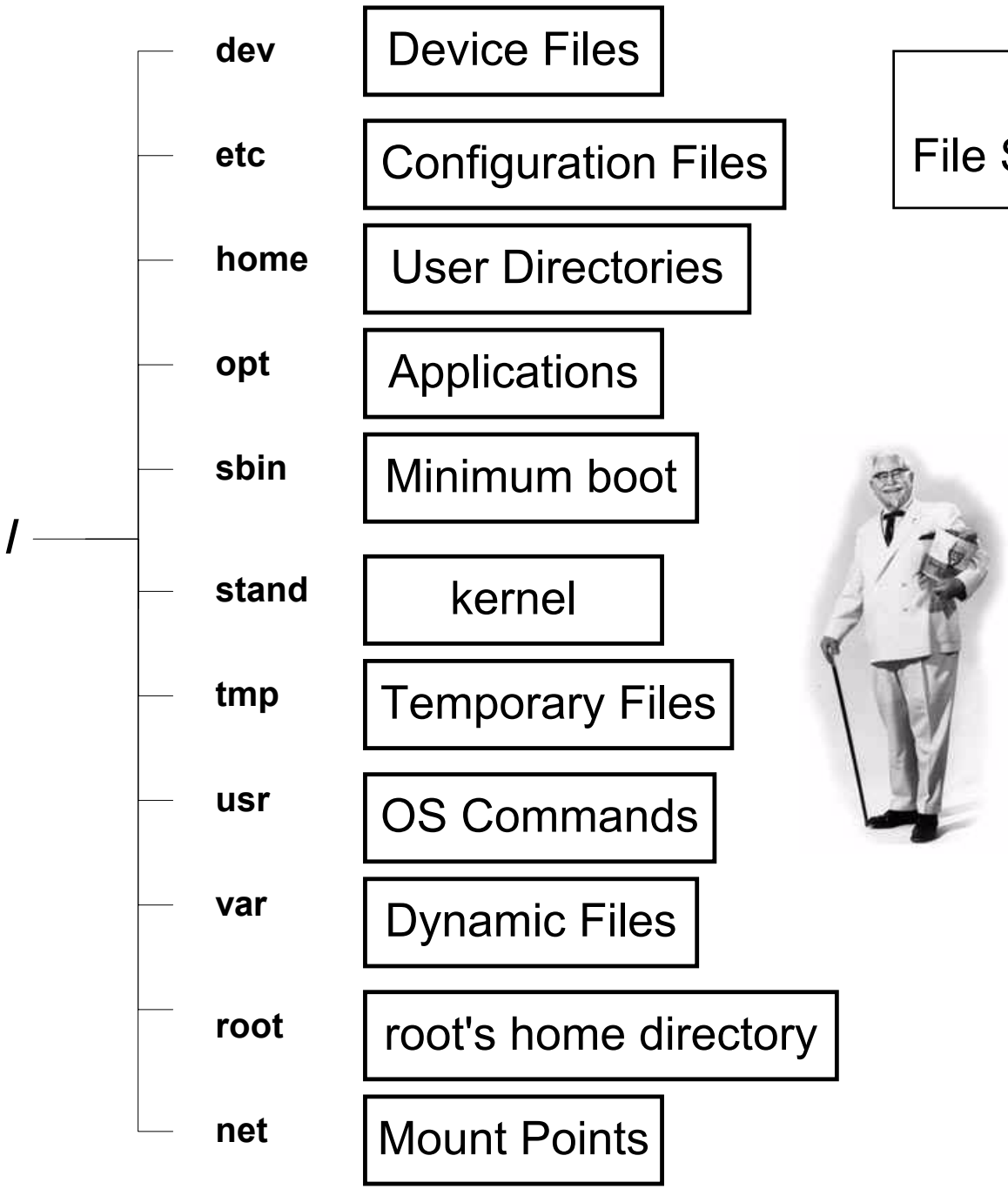
equates to the POSIX Absolute Path Name:

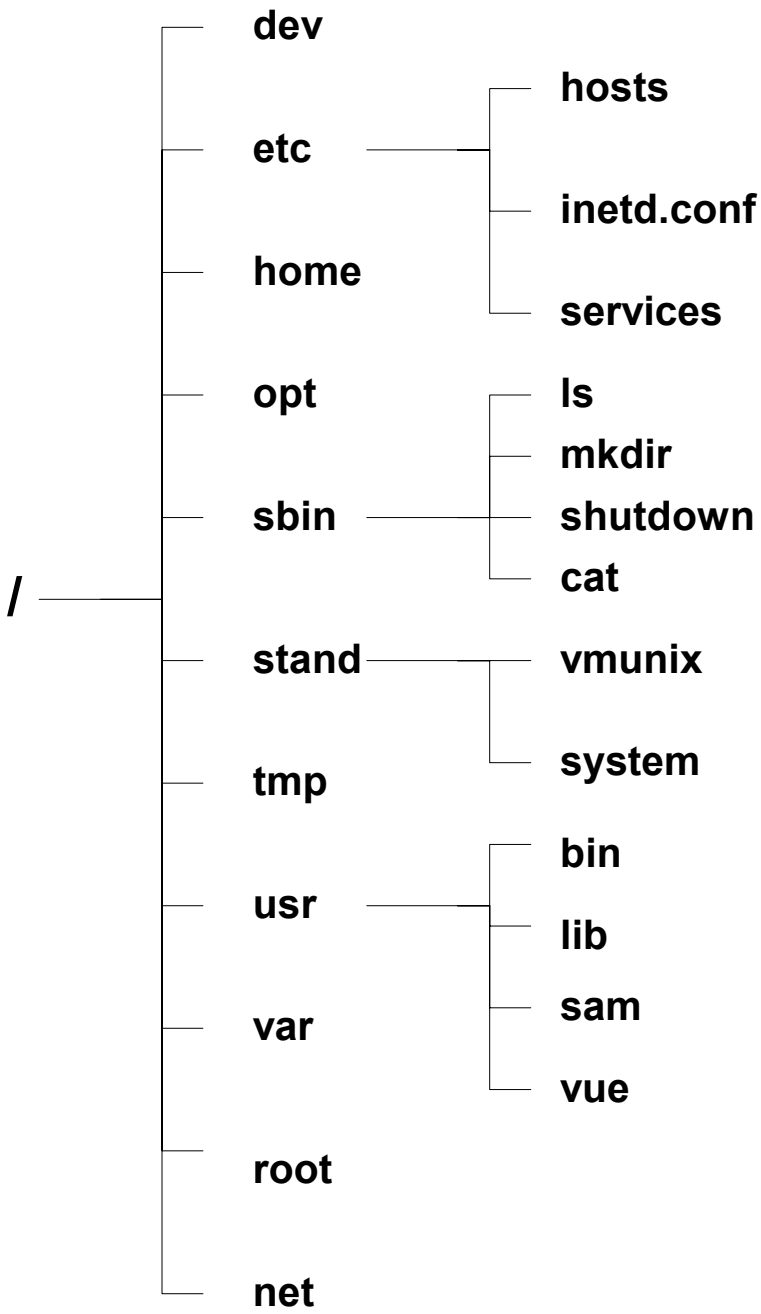
/SYS/PUB/HPSWINFO



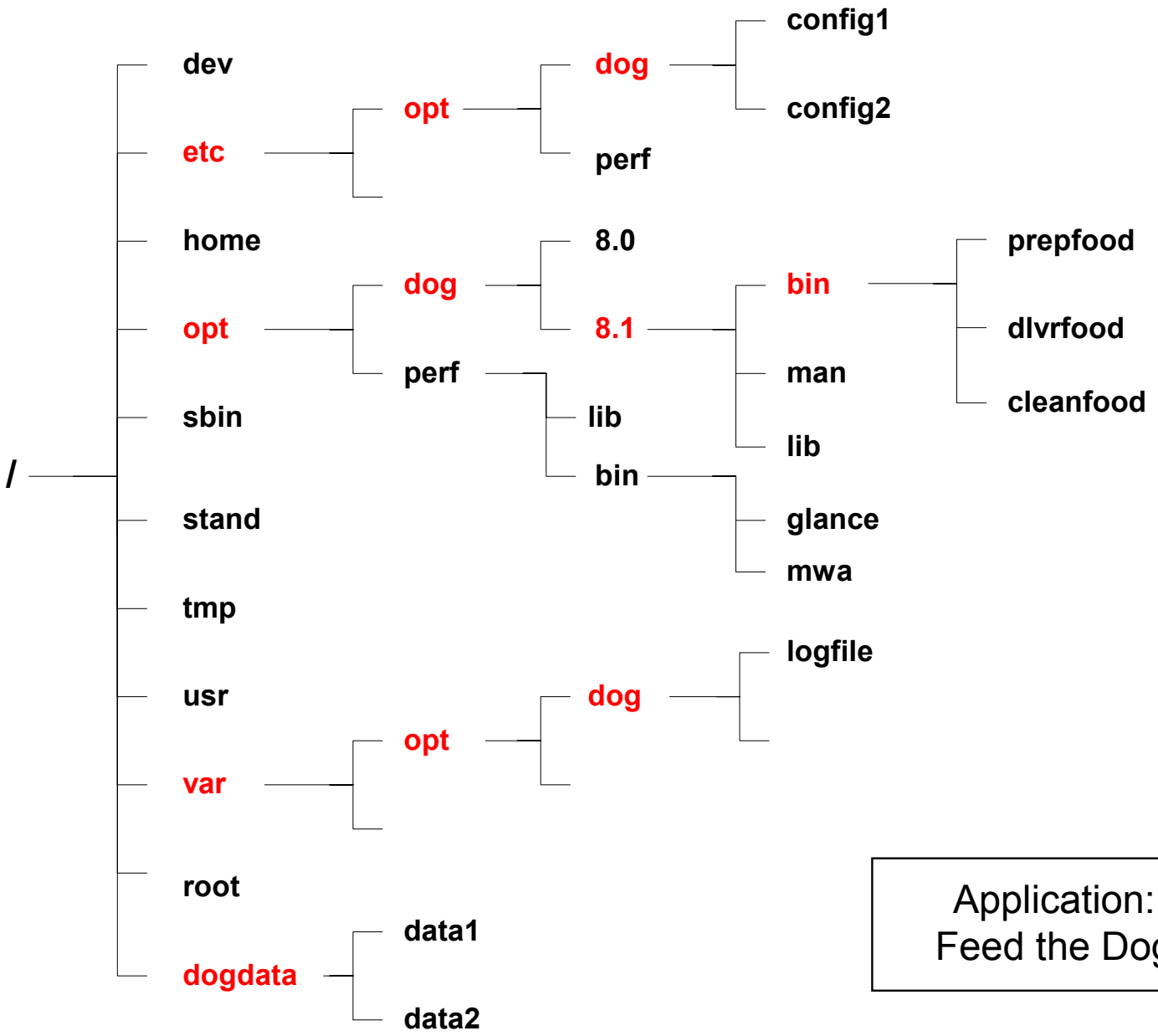
With HFS, Files do not have to belong in a GROUP and directories can be nested

UNIX 95
File System Layout





UNIX 95
File System Layout



Application:
Feed the Dog

Optional Applications

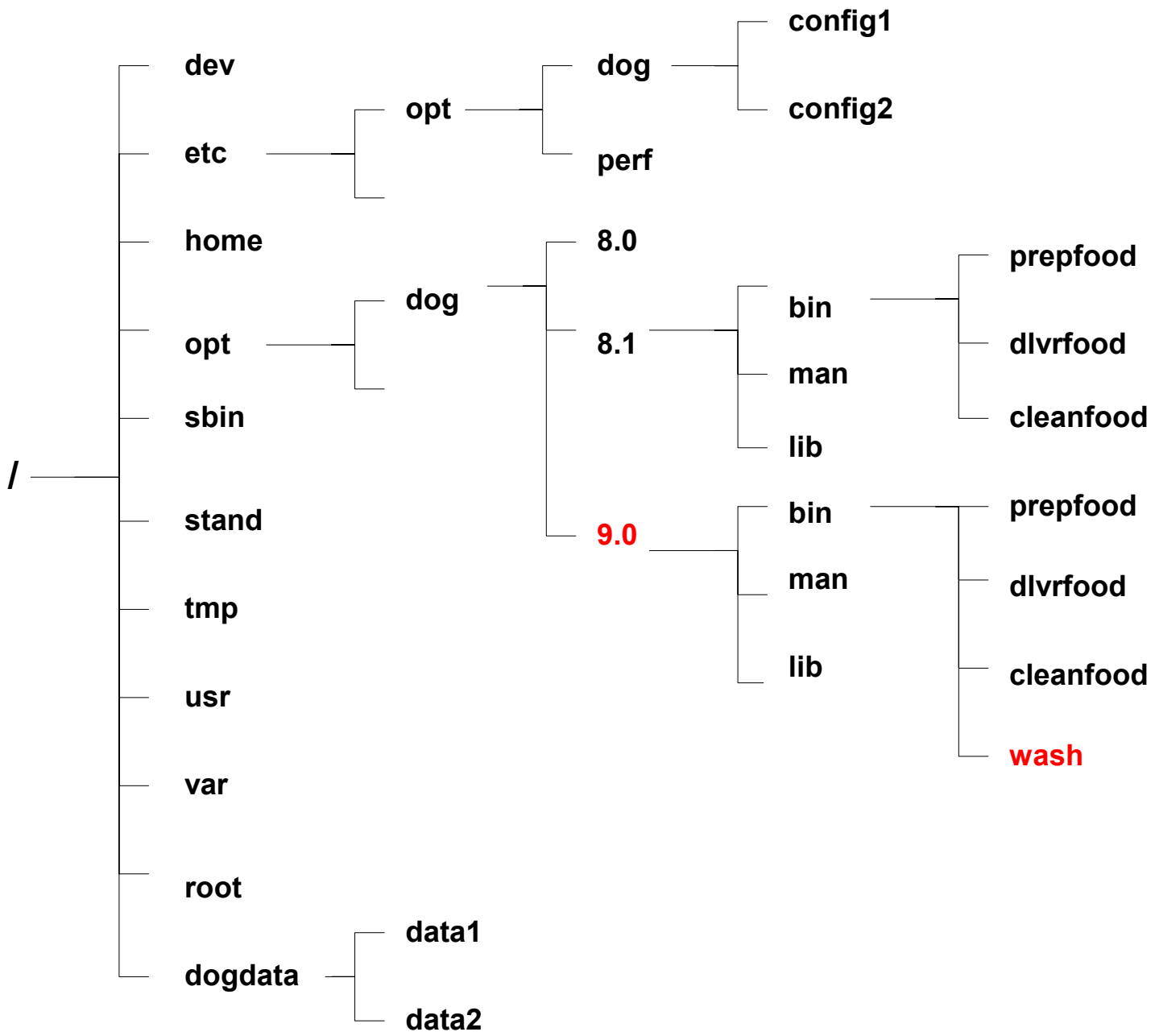
- /opt/dog/release/bin
  - Read-only. Programs, libraries, man pages
- /etc/opt/dog/config1
  - Files for system administrator to edit
- /var/opt/dog/logfile
  - Variable files, application writes to
- /dogdata (no standard for this, but may be for specific database in use)
  - Databases

HP doesn’t always get it right

- /opt/perf/bin/glance /opt/perf/bin/mwa
  - Read-only. Programs, libraries, man pages
- /var/opt/perf/datafiles/logglob
- /var/opt/perf/status.scope
  - Variable files, application writes to
- /var/opt/perf/parm should be: /*etc*/opt/perf/parm, since it’s a config file

/opt/APPLICATION/Release

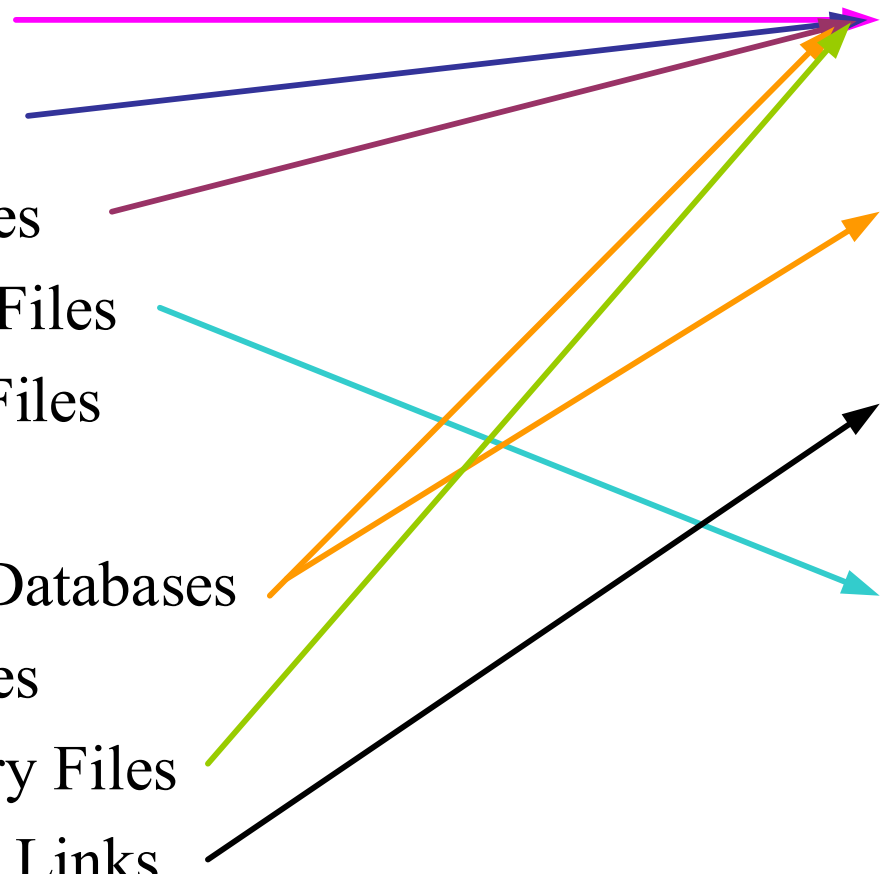
- dog=/opt/feed/8.1/bin
- PATH=$PATH:$dog
- The user enters: prepfood
  - /opt/dog/8.1/bin/prepfood is executed
- New release
  - Create new directory (/opt/dog/9.0)
  - Install new version
  - Change dog variable to: dog=/opt/dog/9.0/bin
  - Problems with new version?
    - Both old and new programs exist (8.1 and 9.0)
    - Quickly change back to old by changing the variable
  - Other benefits:
    - Testing, organization, rolling upgrades, and ease of management


/
dev
etc
home
opt
sbin
stand
tmp
usr
var
root
dogdata
data1
data2
opt
dog
perf
config1
config2
dog
8.0
8.1
9.0
bin
man
lib
bin
man
lib
prepfood
dlvrfood
cleanfood
prepfood
dlvrfood
cleanfood
wash

File Types

- **MPE/iX**
  - Binary
  - ASCII
  - Spool Files
  - Message Files
  - Circular Files
  - KSAM
  - IMAGE Databases
  - PRIV Files
  - Temporary Files
  - Symbolic Links
- **HP-UX**
  - Ordinary (-)
  - Block (b)
  - Character (c)
  - Directory (d)
  - Link (l)
  - Network (n)
  - Pipe (p)
  - Socket (s)

- **MPE/iX**
  - Binary
  - ASCII
  - Spool Files
  - Message Files
  - Circular Files
  - KSAM
  - IMAGE Databases
  - PRIV Files
  - Temporary Files
  - Symbolic Links



- **HP-UX**
  - Ordinary (-)
  - Block (b)
  - Character (c)
  - Directory (d)
  - Link (l)
  - Network (n)
  - Pipe (p)
  - Socket (s)

- KSAM: 3rd party products (Bitech, HP-Eloquence)
- Circular Files: None
- PRIV Files: Regular file/directory with special permissions

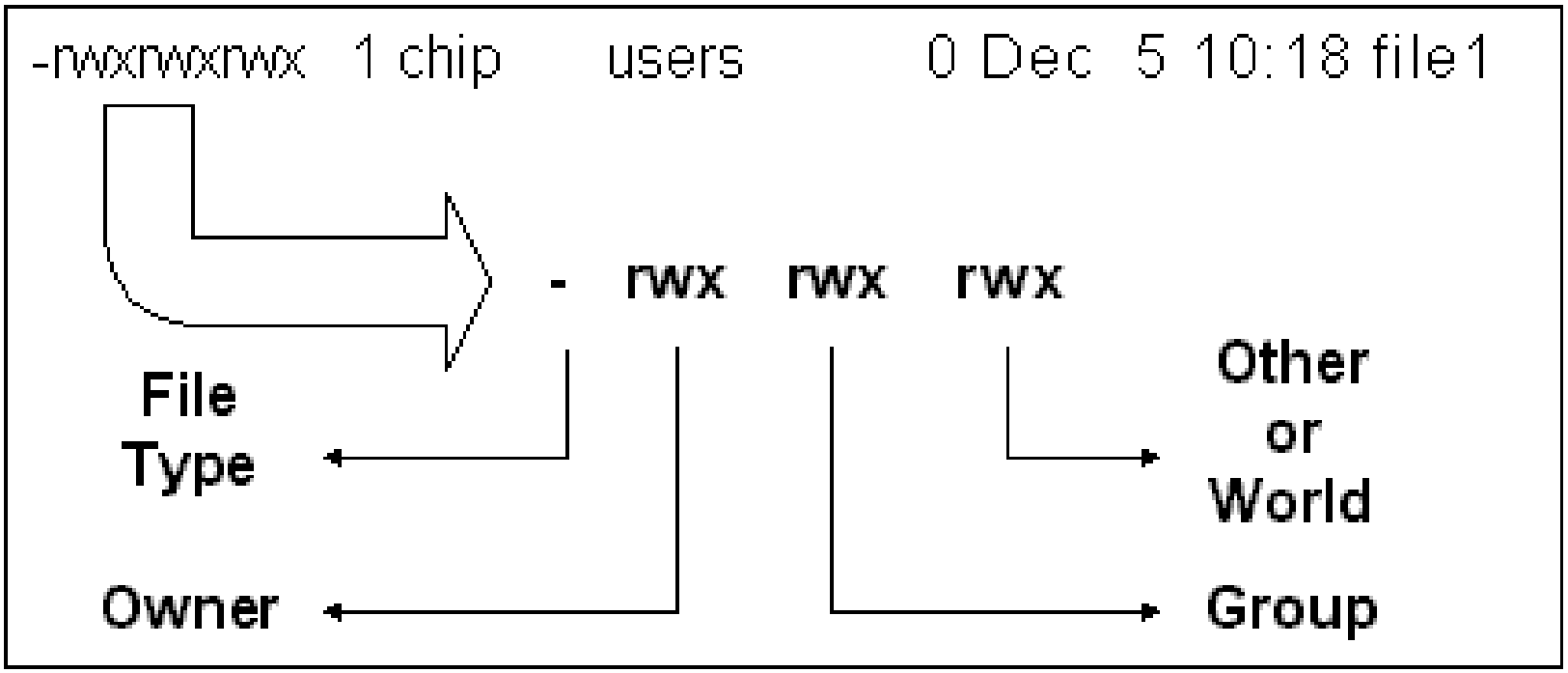
```
:listf editor.pub,-3
*********************
```

FILE: EDITOR.PUB.SYS

```
FILE CODE : 1029                FOPTIONS: BINARY,FIXED,NOCCTL,STD
BLK FACTOR: 1                   CREATOR : MANAGER.SYS
REC SIZE: 256(BYTES)            LOCKWORD:
BLK SIZE: 256(BYTES)            SECURITY--READ    : ANY
EXT SIZE: 324(SECT)              WRITE   : ANY
NUM REC: 323                     APPEND  : ANY
NUM SEC: 336                     LOCK    : ANY
NUM EXT: 1                       EXECUTE : ANY
MAX REC: 323                    **SECURITY IS ON
MAX EXT: 1                      FLAGS   : NO ACCESSORS
NUM LABELS: 0                   CREATED : SUN, MAR 18, 2001,  9:38 AM
MAX LABELS: 0                   MODIFIED: SUN, MAR 18, 2001,  9:38 AM
DISC DEV #: 14                  ACCESSED: THU, OCT 18, 2001,  9:58 AM
SEC OFFSET: 0                   LABEL ADDR: $000000C8.$003C5420
VOLSET    : MPEXL_SYSTEM_VOLUME_SET
```

```
shell/iX> ls -l /SYS/PUB/EDITOR
*************************************
-rwxr-xr-x   1 MANAGER.SYS       SYS       82688 Mar 18  2001   /SYS/PUB/EDITOR
```

UNIX File

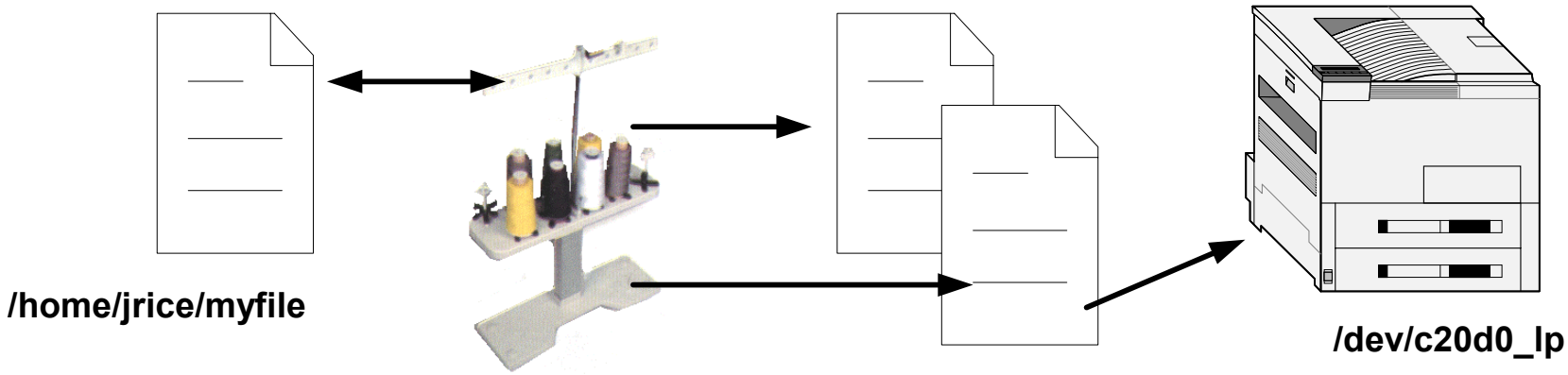


UNIX Directory: drwxr-xr-x

W on directory: contents can be deleted or added

HP-UX: Everything is a file

- -r-sr-xr-x root bin 40960 Nov 14 2000 /usr/bin/lp
- -rwx------ jrice users 713 Oct 12 08:18 /home/jrice/myfile
- crw-r--r-- lp bin 216 0x020002 Oct 18 15:18 /dev/c20d0_lp
- -rw-r----- lp lp 104 Oct 18 16:16 /var/spool/lp/request/dj/cA0000ctg800
- rw-r----- lp lp 713 Oct 18 16:16 /var/spool/lp/request/dj/dA0000ctg800



JOBS: Management

- Management of jobs
  - MPE: START (defaults to START RECOVERY)
    - SCHED Jobs will be rescheduled
    - Incomplete Jobs will restart (if streamed with the ;restart option)
  - HP-UX: Scheduled cron jobs will be rescheduled
    - Incomplete jobs: 3rd party software, built-in to apps

JOBS: Standard List

- JOB --> 10 (streams device) --> $STDLST (LP)
- What do you use the standard list for?

Term: Standard Input

Definition: Unix commands receive information from standard input.

AKA: stdin, input stream, standard input

Examples:

```
$ rm -i file1
remove file1? y
```

The reply (y) is the standard input. It was entered at the keyboard. Keyboard is the default standard input.

```
$ sendmail user@yourcompany.com < /etc/hosts
```

The standard input is the file named /etc/hosts.

```
$ ll | grep *.rc
```

The standard input for the grep command is the output from the ll command.

Term: Standard Output

Definition: Unix commands send information to standard output.

AKA: stdout, output stream, standard output stream, standard list

Examples:

```
$ more myfile1
Line one of my file!
Line two of my file.
```

Standard output sent to the display. The default standard out is the display (screen or terminal).

```
$ more myfile1 > myfile2
```

In this example, the standard output is being redirected from the display to a file (myfile2).

```
$ ll | grep *.rc
```

The standard output of the ll command is used as the standard input to the grep command.

Term: Standard Error

Definition: Unix commands send information regarding errors to standard error.

AKA: stderr

Examples:

```
$ more myfle1
myfle1: No such file or directory
```

Standard error is sent to the display. The default standard error is the display (screen or terminal).

```
$ more myfle1 2> myfile2
```

In this example, the standard error is being redirected from the display to a file (myfile2).

Input/Output/Error Redirection Summary

Example	Description
cmd < file	Read stdin from a file.
cmd > file	Redirect stdout to a file.
cmd >> file	Append stdout to a file.
cmd < inputfile > outputfile	Redirect stdin and stdout simultaneously.
cmd1 | cmd2	Piping stdout from one command to stdin of another.
cmd **2**> file	Redirect stderr to a file.

STANDARD LIST

So, what's the problem?

Only <u>output</u> that arises from the normal operating of a Unix command is sent to standard output.


```
#  This is my job #1
#
touch file1
cp file1 file2
rm file1
ID=`whoami`
if [ "${ID}" = "jrice" ] ; then
 /usr/lib/sendmail cwong@cerius.com < file2 ; else
 echo "***** WRONG USER RUNNING JOB *****"
fi
```

```
ctg500: ./job1

ctg500:
```

```
ctg500: touch file1

ctg500:
```

```
#  This is my job #1
#
#
echo "*******************************" >> logfile1
echo "      This is my job #1        " >> logfile1
echo "*******************************" >> logfile1
echo "" >> logfile1
echo "Job executed by: `who -T` " >> logfile1
echo "On machine: `uname -a` " >> logfile1
echo "Date started: `date` " >> logfile1
touch file1
cp file1 file2
rm file1
ID=`whoami`
if [ "${ID}" = "jrice" ] ; then
 /usr/lib/sendmail cwong@cerius.com < file2 ; else
 echo "***** WRONG USER RUNNING JOB *****"
fi
```

Contents of logfile1

****
This is my job #1
****

Job executed by: jrice - pts/ta Mar 8 15:03 . 14180 ctg800
On machine: HP-UX ctg500g B.11.00 U 9000/800 1568700558 unlimited-user license
Date started: Fri Mar 8 20:54:38 PST 2002

```
#  This is my job #1
#
#
echo "**********************************" >> logfile1
echo "      This is my job #1         " >> logfile1
echo "**********************************" >> logfile1
echo "" >> logfile1
echo "Job executed by: `who -T` " >> logfile1
echo "On machine: `uname -a` " >> logfile1
echo "Date started: `date` " >> logfile1
set -x
touch file1
cp file1 file2
rm file1
ID=`whoami`
if [ "${ID}" = "jrice" ] ; then
 /usr/lib/sendmail cwong@cerius.com < file2 ; else
 echo "***** WRONG USER RUNNING JOB *****"
fi
```

ctg500: ./job1 2>> logfile1

```
*******************************
     This is my job #1
*******************************

Job executed by: jrice    - pts/ta       Mar  8 15:03    .    14180  ctg800
On machine: HP-UX ctg500g B.11.00 U 9000/800 1568700558 unlimited-user license
Date started: Fri Mar  8 21:02:46 PST 2002
+ touch file1
+ cp file1 file2
+ rm file1
+ + whoami
ID=jrice
+ [ jrice = jrice ]
+ /usr/lib/sendmail cwong@cerius.com
+ 0< file2
```

```
#  This is my job #1
#
#
echo "**********************************" >> /var/opt/app1/logfile1
echo "      This is my job #1         " >> /var/opt/app1/logfile1
echo "**********************************" >> /var/opt/app1/logfile1
echo "" >> /var/opt/app1/logfile1
echo "Job executed by: `who -T` " >> /var/opt/app1/logfile1
echo "On machine: `uname -a` " >> /var/opt/app1/logfile1
echo "Date started: `date` " >> /var/opt/app1/logfile1
set -x
touch file1
cp file1 file2
rm file1
ID=`whoami`
if [ "${ID}" = "jrice" ] ; then
 /usr/lib/sendmail cwong@cerius.com < file2 ; else
 echo "***** WRONG USER RUNNING JOB *****"
fi
```

```
*******************************
      This is my job #1
*******************************

Job executed by: jrice    - pts/ta       Mar  8 15:03    .    14180  ctg800
On machine: HP-UX ctg500g B.11.00 U 9000/800 1568700558 unlimited-user license
Date started: Fri Mar  8 21:10:56 PST 2002
+ touch file1
touch: file1 cannot create
+ cp file1 file2
cp: cannot access file1: No such file or directory
+ rm file1
rm: file1 non-existent
+ + whoami
ID=jrice
+ [ jrice = jrice ]
+ /usr/lib/sendmail cwong@cerius.com
+ ../job1[17]: file2: Cannot find or open the file.
```

Creating a Standard List on HP-UX

- Send “output” to a log file:
  - 1). One logfile for each application (/var/opt/app/logfile)
  - 2). One logfile for each job (/var/opt/app/logfile “unique value”)
  - 3). One logfile for everything (/var/adm/syslog/syslog.log)

Problem

- Need to add a new user to the PAYROLL application.
- Solution on MPE: user with correct capabilities for the PAYROLL account can create the new user. MANAGER.SYS does not have to do this.
- Solution on UNIX: only UID 0 can add new users.

Creating a role based environment

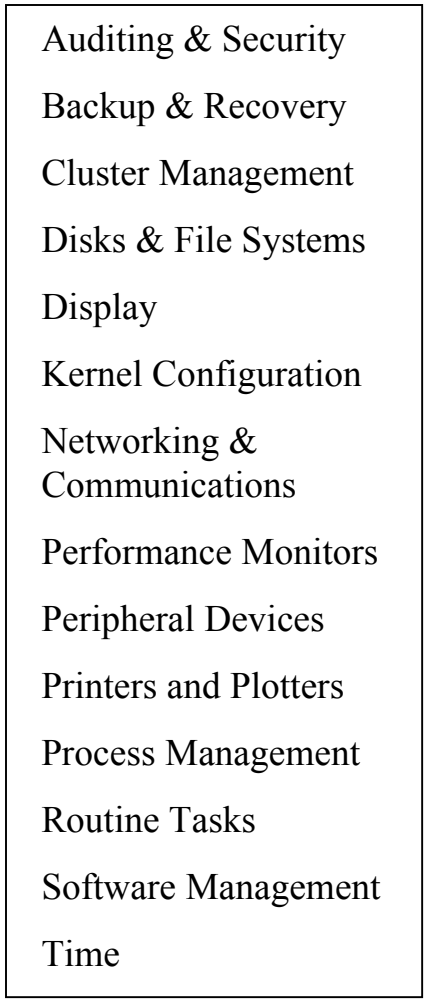
- Give non-System Admins the root password
- Create SUID/SGID scripts
- “sudo”
- Restricted SAM
- ServiceControl Manager
- ALL ARE FREE!!

SUID Scripts/Programs

- What is it?
- File with certain permissions:
- -r-sr-xr-x 1 root bin /sbin/passwd

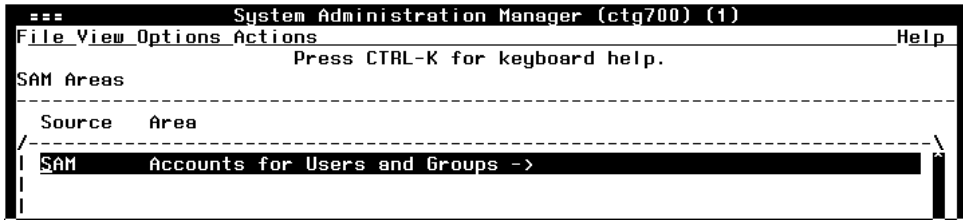
Restricted SAM Builder

- sam -r
- Includes all SAM areas
  - Disabled, Enabled or Partial
- Save Privileges
- Select user(s)
- /etc/sam/custom/”user”.cf



Testing & Using Restricted SAM

- sam -f login
  - sam -f jrice



- User only sees areas that are enabled for that user
- SAM is not in the user's PATH variable:
  - Add /usr/sbin to the user's PATH
  - Create an alias called sam that executes /usr/sbin/sam
  - Have the user execute the full pathname (/usrs/bin/sam)

Added Benefit

- Auditing
- /var/sam/log/samlog
- User jrice (UID:4004) added user: bshaver

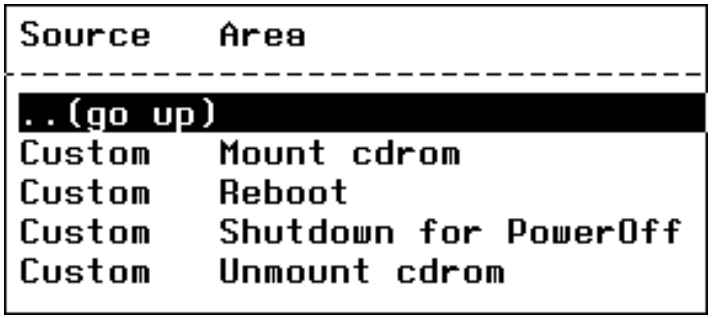
```
@!@1@958083415@4004
```
Adding user bshaver

Added Benefit

- Templates
  - Create templates that specify which tasks are to be enabled
    - User management
    - Backup/Restore
    - Add/Increase Logical Volumes & File Systems
    - Install Patches
- One template can be assigned to a user

Customize SAM

- Create a custom area/group
- Create a custom application
  - Execute using: “user”



Auditing & Security

Backup & Recovery

Cluster Management

Disks & File Systems

Display

Kernel Configuration

Networking & Communications

Performance Monitors

Peripheral Devices

Printers and Plotters

Process Management

Routine Tasks

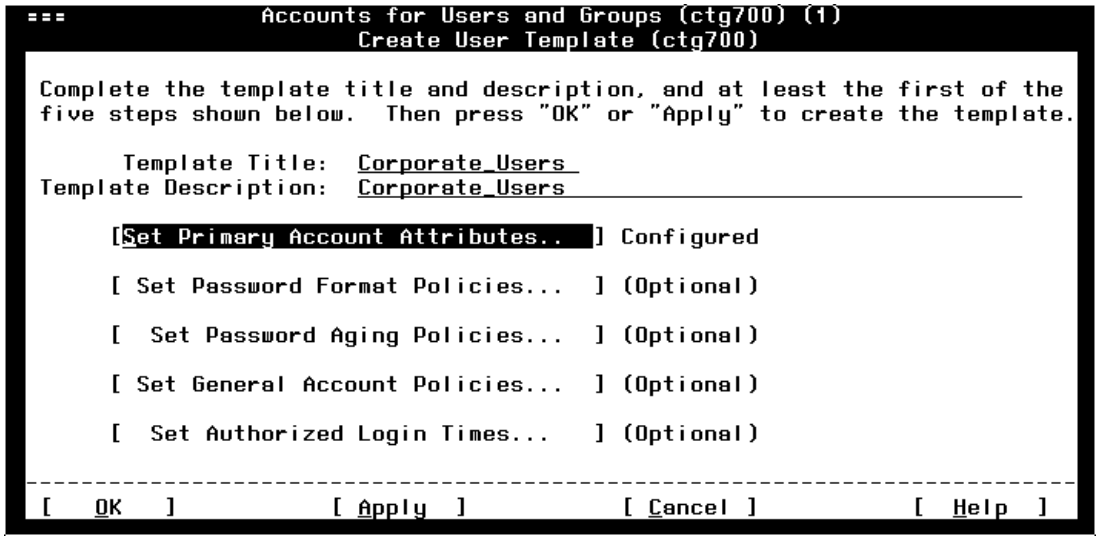
Software Management

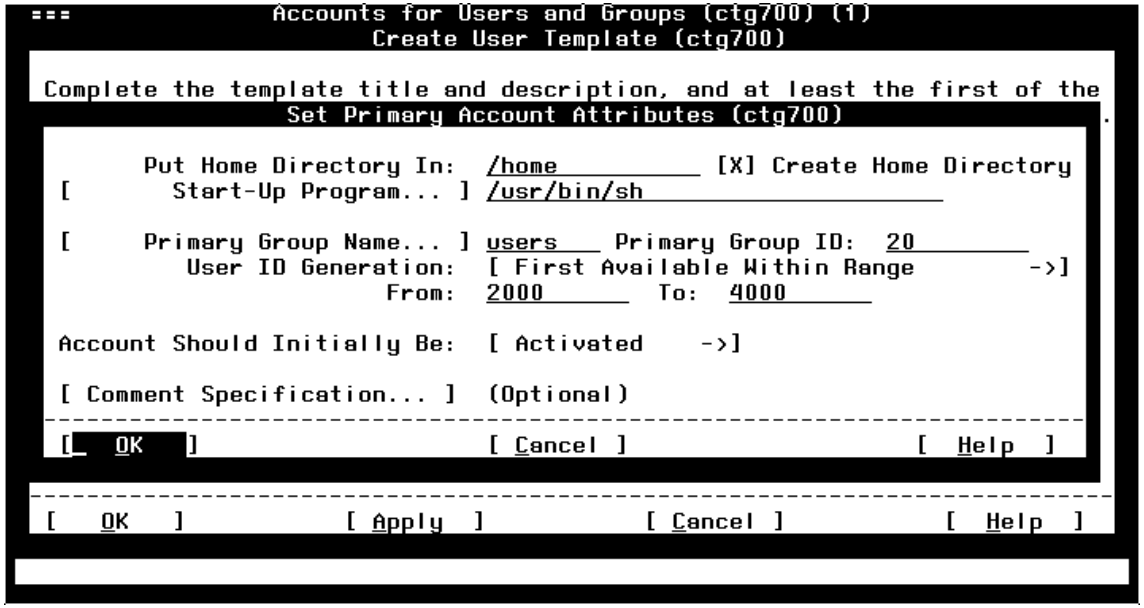
Time

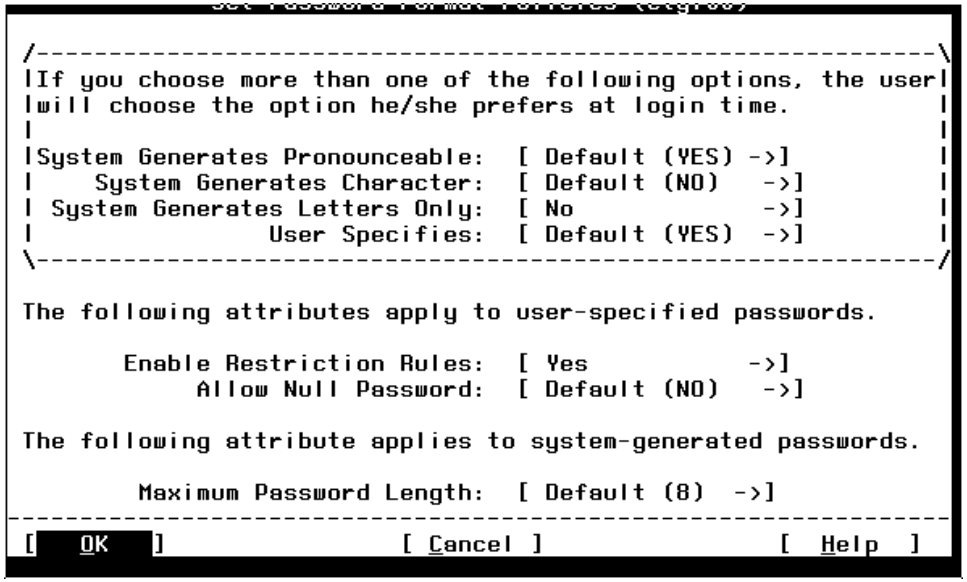
Your Area

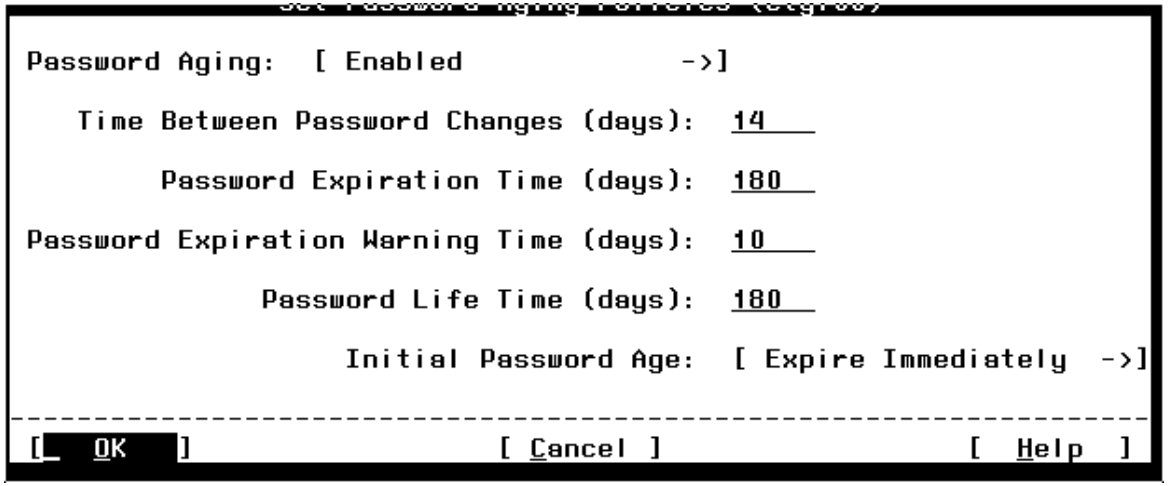
SAM Templates (predefined fields)

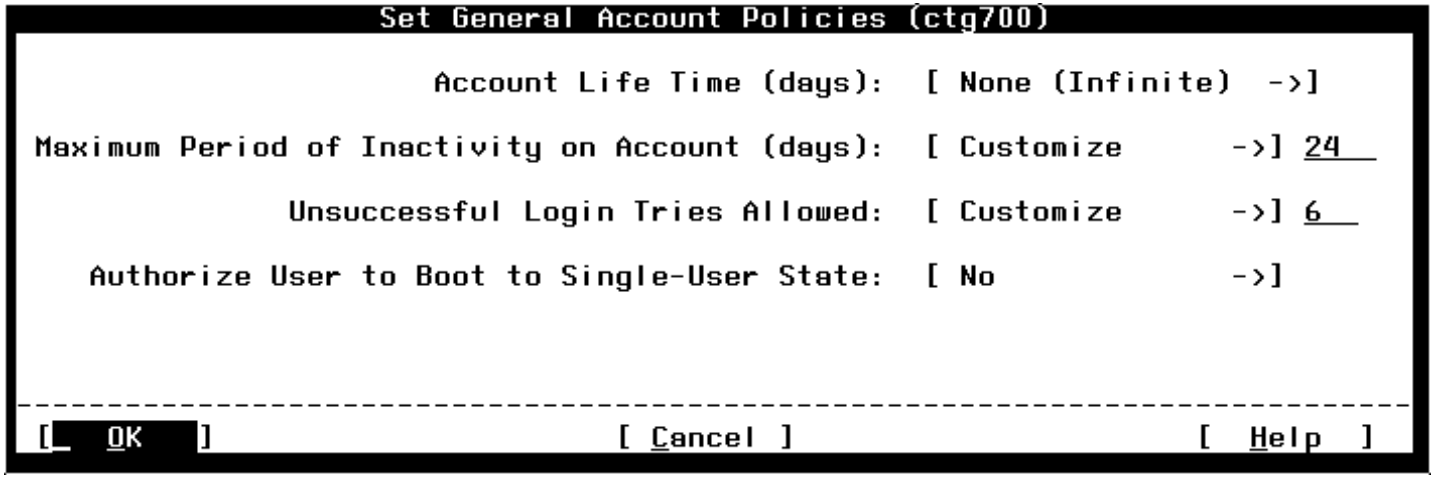
- Ease administration
- Create consistency
- Increase security

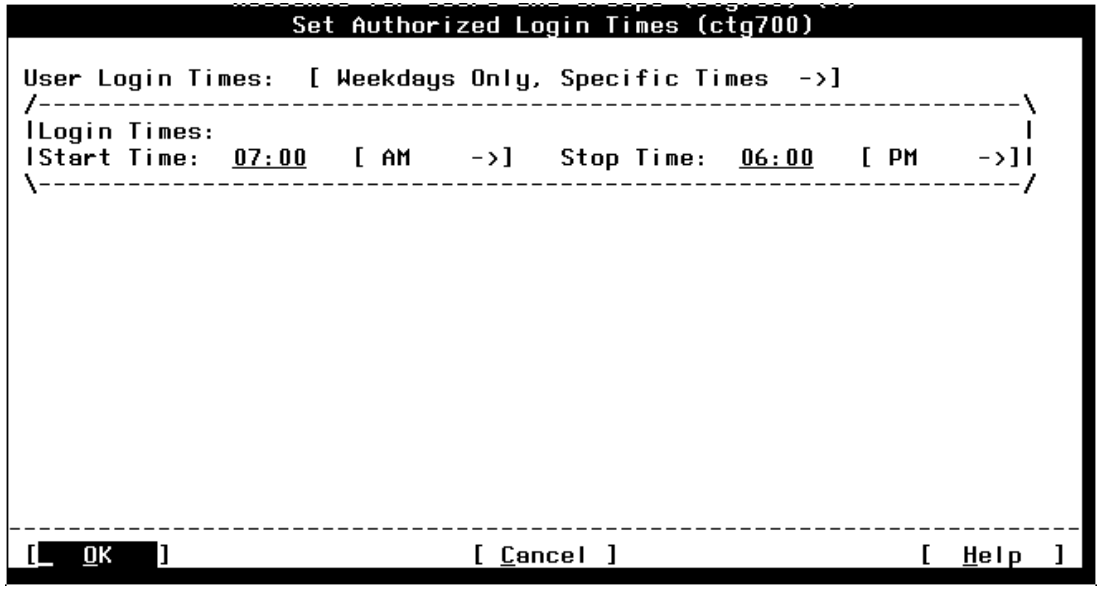

Accounts for Users and Groups (ctg700) (1)
Create User Template (ctg700)
Complete the template title and description, and at least the first of the five steps shown below. Then press "OK" or "Apply" to create the template.
Template Title: Corporate_Users
Template Description: Corporate_Users
[Set Primary Account Attributes..] Configured
[Set Password Format Policies...] (Optional)
[Set Password Aging Policies...] (Optional)
[Set General Account Policies...] (Optional)
[Set Authorized Login Times...] (Optional)
[OK] [Apply] [Cancel] [Help]

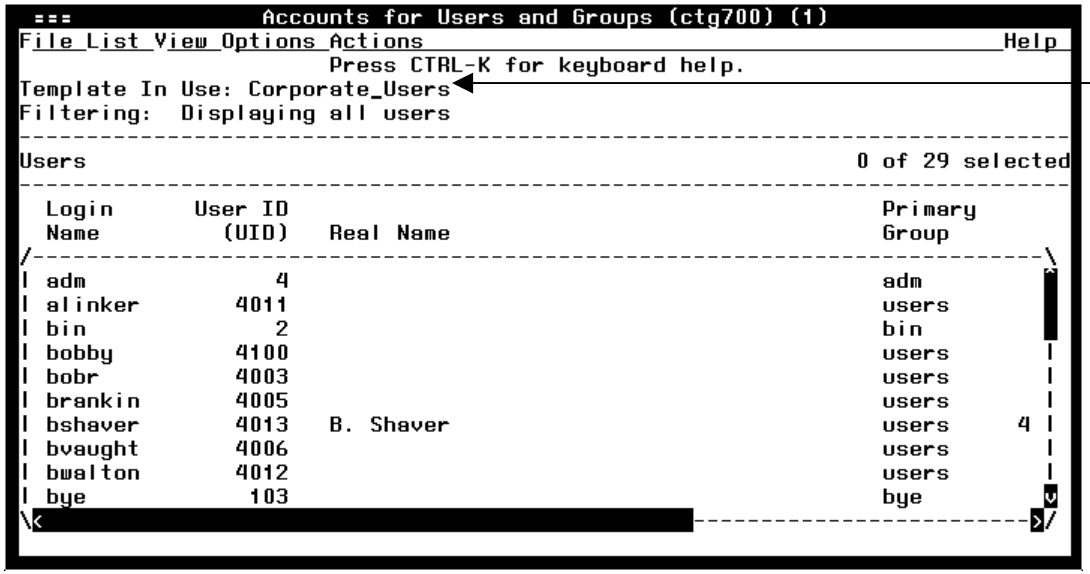

Accounts for Users and Groups (ctg700) (1)
Create User Template (ctg700)
Complete the template title and description, and at least the first of the
Set Primary Account Attributes (ctg700)
Put Home Directory In: /home [X] Create Home Directory
[Start-Up Program...] /usr/bin/sh
[Primary Group Name...] users Primary Group ID: 20
User ID Generation: [First Available Within Range ->]
From: 2000 To: 4000
Account Should Initially Be: [Activated ->]
[Comment Specification...] (Optional)
[OK] [Cancel] [Help]
[OK] [Apply] [Cancel] [Help]


If you choose more than one of the following options, the user will choose the option he/she prefers at login time.
System Generates Pronounceable: [Default (YES) ->]
System Generates Character: [Default (NO) ->]
System Generates Letters Only: [No ->]
User Specifies: [Default (YES) ->]
The following attributes apply to user-specified passwords.
Enable Restriction Rules: [Yes ->]
Allow Null Password: [Default (NO) ->]
The following attribute applies to system-generated passwords.
Maximum Password Length: [Default (8) ->]
[OK]
[Cancel]
[Help]

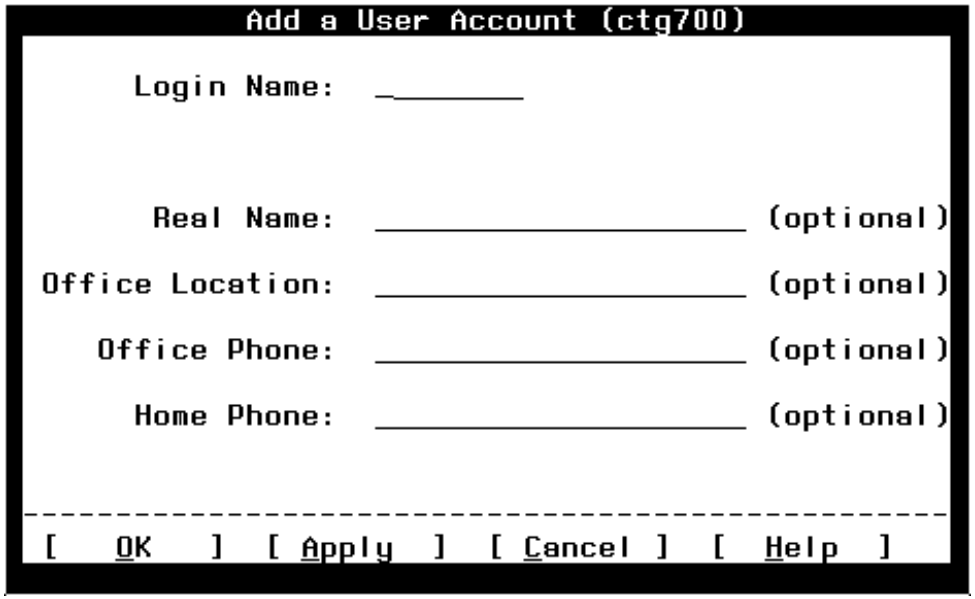

Password Aging: [Enabled ->]
Time Between Password Changes (days): 14
Password Expiration Time (days): 180
Password Expiration Warning Time (days): 10
Password Life Time (days): 180
Initial Password Age: [Expire Immediately ->]
[OK]
[Cancel]
[Help]


Set General Account Policies (ctg700)
Account Life Time (days): [None (Infinite) ->]
Maximum Period of Inactivity on Account (days): [Customize ->] 24
Unsuccessful Login Tries Allowed: [Customize ->] 6
Authorize User to Boot to Single-User State: [No ->]
[OK]
[Cancel]
[Help]


Set Authorized Login Times (ctg700)
User Login Times: [Weekdays Only, Specific Times ->]
Login Times:
Start Time: 07:00 [AM ->] Stop Time: 06:00 [PM ->]
[OK]
[Cancel]
[Help]



When the user runs SAM, they use the template. When adding a new user, the following window is displayed.



Wow! All the user has to enter is the login name!

sudo
superuser do

- Sudoers file
  - /opt/sudo/sbin/visudo to edit
  - Who can do what on which system(s).

```
# Host alias specification
Host_Alias PROD=ctg700,ctg800
Host_Alias DEV=ctg500
# User alias specification

# Cmnd alias specification
Cmnd_Alias MOUNT=/sbin/mount,/sbin/umount
Cmnd_Alias SHUTDOWN=/sbin/shutdown
# User privilege specification
#root   ALL=(ALL) ALL
jrice PROD=MOUNT
jrice ALL=SHUTDOWN
smokey DEV=MOUNT
~
```

How the user uses sudo

- Enter sudo followed by the command and options
- Command must be configured in the sudoers file for that user and system

```
$ whoami
jrice
$ /sbin/mount /dev/dsk/cdrom /cdrom
mount: must be root to use mount
$
$ /opt/sudo/bin/sudo /sbin/mount /dev/dsk/cdrom /cdrom
$ bdf | grep cdrom
/dev/dsk/cdrom     2457600 2457600       0  100% /cdrom
```

ServiceControl Manager

- Manage Multiple HP-UX servers from one central location
- Role assignments
- SCM is a wrapper, added functionality is wrapped around: commands, scripts, file-copy and applications
- HP Supported

SCM Integration

- Event Monitoring System (EMS)
- Online JFS
- Software Distributor/UX
- SAM
- Ignite/UX and Recovery
- System Configuration Repository (SCR)
- Security Patch Check Tool

- HP-UX Commands
- bdf
- ls
- rm
- cat
- cp
- ps
- mv
- find
- test

Parts of SCM

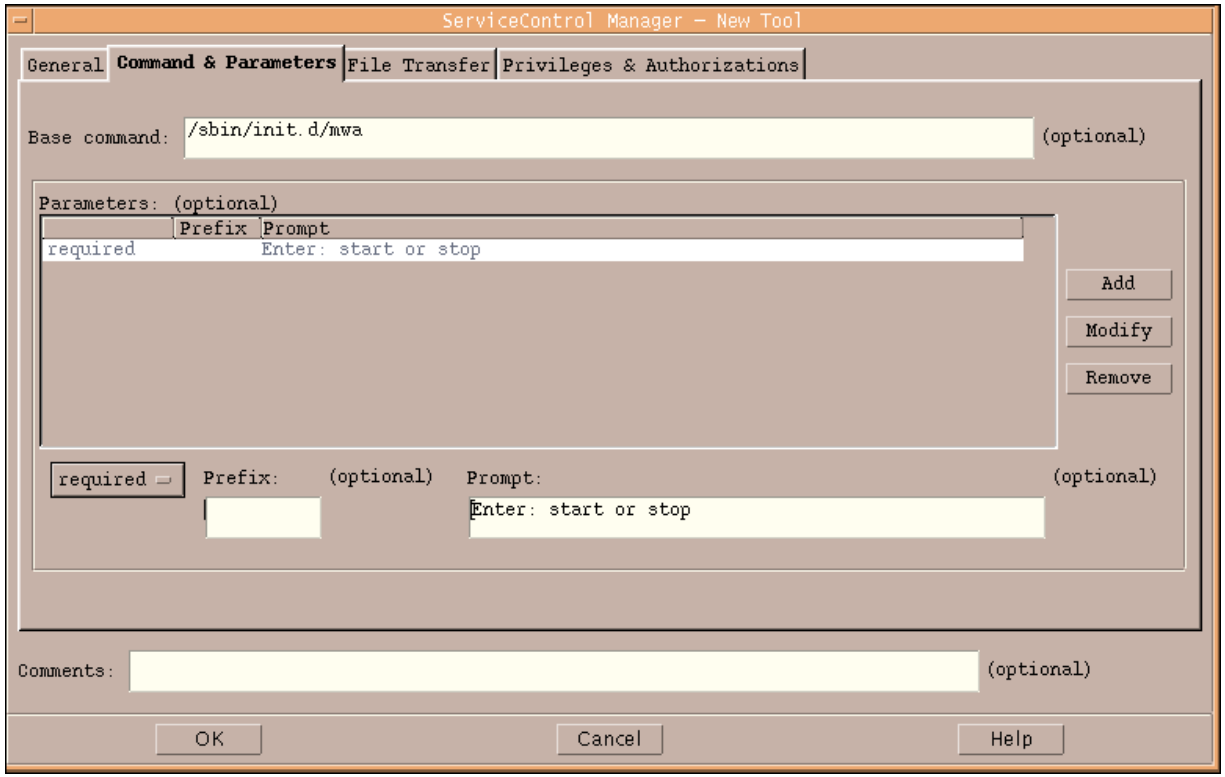
- Central Management Server (CMS)
  - Ignite/UX Server
- SCM Cluster
  - CMS and nodes
- Tools
  - SSA - Single System Aware
  - MSA - Multiple System Aware
- Users
- Roles

Tools

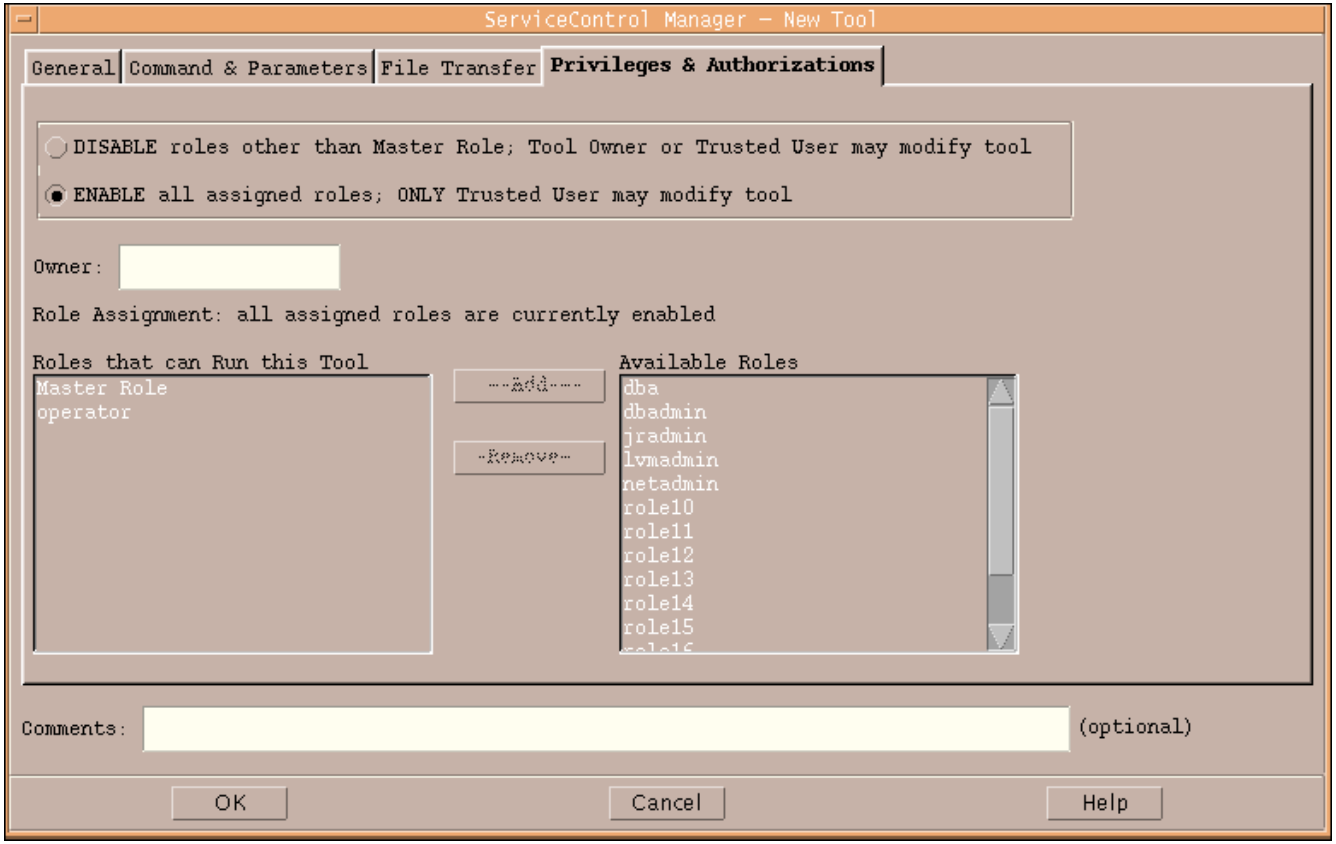
- Command
- Program
- Script
- File-copy
- Customized
- Defined in Tool Definition File (.tdef)

- **Tool Rules**
- Any SCM user can create a tool
- An SCM user may modify a tool they own, they can't modify the owner or role
- Only the Trusted User can authorize tools to be run on selected nodes by selected users
- The SCM admin can modify any tool, including its owner and role
- Only the SCM admin can delete tools

Add tool using GUI

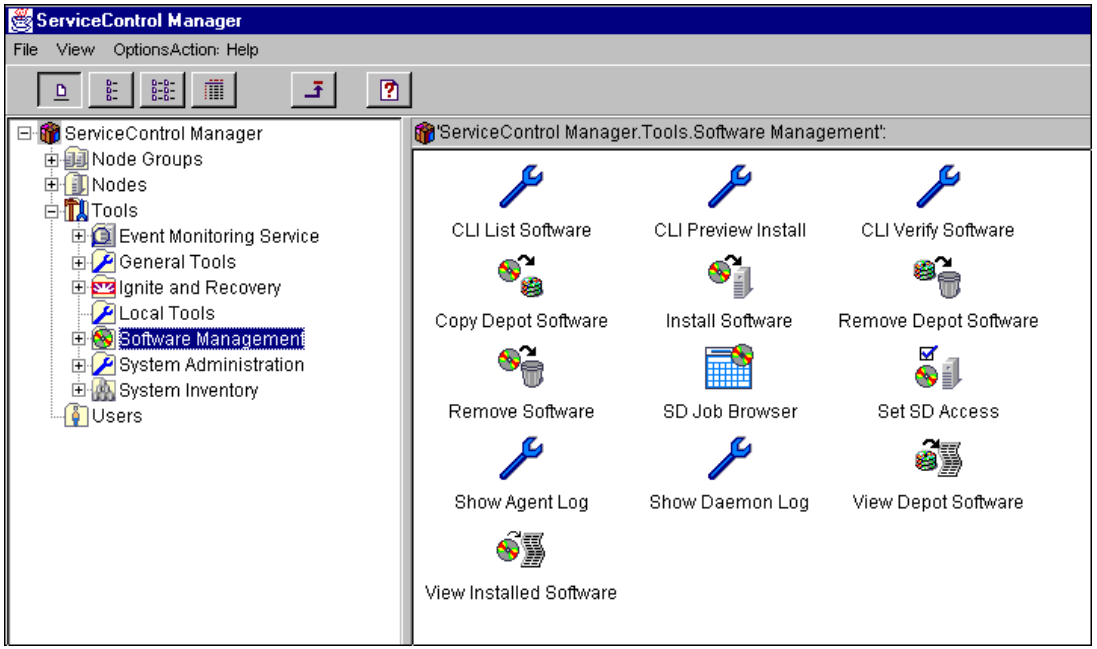


Assign Tool to Role



Using SCM

- Command Line
- GUI
- Web Interface->
  - mxexec -t mwa -A start -n ctg500



Validation

- HP-UX login process
- Trusted User? Any tool on any node.
- Not Trusted? Can only run tools assigned to their role(s) on specific node(s)
- An authorization can be added if using the startup/shutdown script technique: flag on the script configuration file

	SUID/SGID Scripts/Pgms	**sudo**	**Restricted SAM**	**Service Control Manager**
Supported by HP	No	No	Yes	Yes
Cost	Your time	Free	Free	Free
Integrated with HP Tools	No	No	Yes	Yes
Available Interfaces	Command Line	Command Line	GUI or CUI	Command Line, GUI or Web
Auditing	You write	Yes	Yes	Yes

Training on HP-UX for the MPE Administrator

- HP World 2002 - Los Angeles, Sept.
  - All day seminar
- 3 days hands-on at your site, in Maryland at http://www.techgroupMD.com or in Seattle area at http://www.cerius.com

HP-UX 11i Security

by Chris Wong
http://newfdog.hpwebhost.com/hpuxsecurity

Prentice Hall PTR

$39.99

450 pages

ISBN: 0130330620