A
Northern Illinois University
Academic Computing Services
Workshop

# UNIX Basics for Superusers

Michael G. Prais
Swen Parson 120
753-1057

The purpose of this workshop is to demonstrate to the owners of UNIX workstations what is available to control a typical system and where to find it. This workshop examines UNIX objects or structures in three areas.

Information Access -- Files and Directories
System Access -- Processes and Environments
External Access -- Communications and Printing

The level at which the material is presented assumes familiarity and facility with the material presented in *UNIX Basics for the Mere-Mortal User* (and knowledge of the difference between a UNIX system administrator and a *superuser* [see below]). This workshop does not provide experience in reconfiguring any of the subsystems examined as all participants are working on a single system. However, the examination of the components of these subsystems is expected to give the participant the knowledge and confidence to appropriately reconfigure their own workstation. This workshop also is limited in that it does not address the reconfiguration of the UNIX kernel nor the installation of a new hardware.

There are several good books on UNIX system administration in addition to the System and Network Administration manual that comes with your system. These include:

Mark G. Sobell, A Practical Guide to the UNIX System, second edition, Benjamin/Cummings (Redwood City, NJ), 1989.

Evi Nemeth, Grath Snyder, and Scott Seebass, UNIX System Administration Handbook, Prentice Hall (Englewood Cliffs, NJ), 1989.

Aeleen Frisch, Essential System Administration, O'Reilly & Associates (Sebastopol, CA), 1991.

David Fiedler and Bruce H. Hunter, UNIX Systems Administration, Hayden (Hasbrouck Heights, NJ), 1986.

Rik Farrow, UNIX System Security, Addison Wesley (Reading, MA), 1991.

Simson Garfinkel and Gene Spafford, Practical Unix Security, O'Reilly & Associates (Sebastopol, CA), 1991.

Tim O'Reilly and Grace Todino, Managing UUCP and Usenet, O'Reilly & Associates (Sebastopol, CA), 1991.

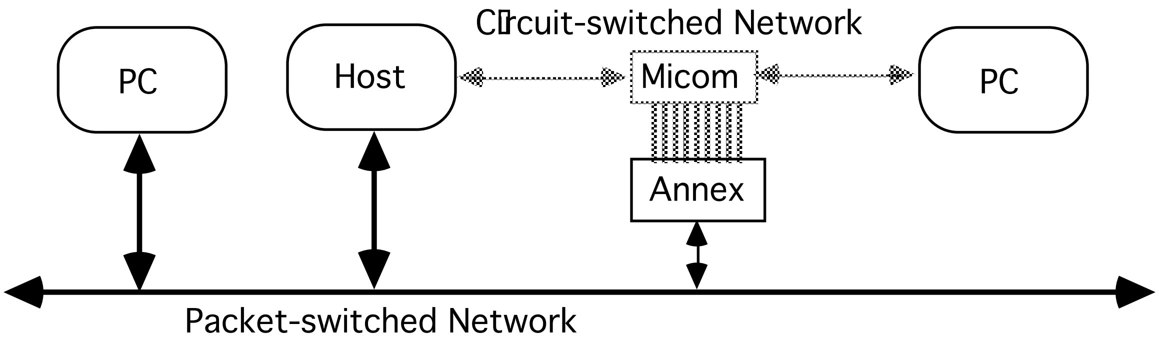
Gail Anderson and Paul Anderson, The UNIX C Shell Field Guide, Prentice Hall (Englewood Cliffs, New Jersey), 1986.

Valerie Quercia and Tim O'Reilly, X Windows System Volume 3: User's Guide, O'Reilly & Associates (Sebastopol, CA), 1990.

Craig Hunt, TCP/IP Network Administration, O'Reilly & Associates (Sebastopol, CA), 19XX.

UNIX is a common operating environment for workstations, minicomputers, and supercomputers. UNIX systems are multiuser systems that act as hosts for several users to simultaneously enter commands and receive responses. UNIX is available in several variants (BSD, SysV, and others), but most of the commands are universal. Any differences in the commands described in this workshop are illustrated by giving the syntax of both commands. Most differences appear in command options, program development, and in system administration.

UNIX systems on campus are generally on the NIU packet-switched network *NIUnet*. They can be reached by other workstations on this network or by other workstations directly connected to or dialing-in to the Micom RS232C circuit switch.



## Network Access to a UNIX System

A UNIX System on the NIU packet-switched network can be accessed as
a remote system from any personal computer that is also on the network and
that uses the TCP/IP suite of communications software.
ACS has a Sun SPARCstation that is on the network.
The PCs in SP10A use a variant of the TCP/IP *telnet* command
which provides remote access as a DEC vt220 terminal on the network.

| | |
|---|---|
| tnvt220 nirvana | Accesses the ACS Sun SPARCStation. |

The hostname *nirvana* is translated through a table on the PCs
to the network of the ACS host system.

## Micom Access to a UNIX System

The UNIX systems on the packet-switched network can also be reached by first
going through the Micom circuit switch to get to the Annex terminal switch
(*umax*) which is on the packet-switched network.
The Annex allows terminals and PCs acting as terminals
on the circuit-switched network access to the packet-switched network.

The following steps describe how to reach the ACS Sun SPARCstation through
the Micom from the Stevens Lab.

| | |
|---|---|
| BREAK BREAK BREAK ENTER | Requests the Micom menu<br>over a Data-Over-Voice (DOV) line.<br>Another procedure is required for dial-in. |

| | |
|---|---|
| umax | Requests an Annex network connection. |
| ENTER ENTER | Requests the *annex:* prompt. |
| telnet nirvana.acs | Accesses the ACS Sun SPARCStation. |

Because ACS is on a different subnet than the Annex,
you must use the hostname and subnet of the ACS host system.

Most UNIX systems present a *login:* prompt to check account access.
Enter your account username and press Enter to identify yourself.
A *password:* prompt is displayed.
Enter the account password and press Enter to verify your identity.
The password is not displayed as a security measure,
but if you know that you typed it wrong,
you can use Backspace to erase erroneous characters,
and then retype the correct characters.
Successfully accessing a system through the *login:* and *password:* prompts
is often called *logging in*.

If the login/password combination does not match with the system values,
UNIX will respond with *login incorrect*, and redisplay the *login:* prompt.
Some systems may redisplay the *login:* prompt a limited number of times.

When the login/password combination is recognized by the system,
it displays several messages and finally a command line prompt.
If the system prompts for a terminal type, enter *vt220* and press Enter.

| | |
|---|---|
| ENTER | Scrolls the screen<br>and displays another prompt. |
| logout ENTER | Terminates your session. |

Follow the previous instructions and re-access the system.

The username for the system administrator or *superuser* account is *root*.
It is called *root* because it owns the root of the filesystem tree.
The typical prompt for the system administrator (*superuser* or *root*)

username is the octothorpe, pound sign, or hash mark (#).
You are not using the superuser account during this workshop,
but you should see this prompt when you access your workstation as *root* .
**Do not enter any commands that start with a octothorpe (#)**
unless you are prepared to reconfigure this (your) system and
you are using a superuser account.
You normally do not have the permissions to use these commands,
but there is a chance that you could adversely affect the system.

To make it easier edit the command line and files displayed on screen,
you must identify to a UNIX system
the terminal type that you are using or emulating.
The following commands set known control keys and the terminal type.
The most common *terminal type*
emulated by personal computer communication software is the *vt100*.
The *terminal type* for the telnet software on the personal computers
in Swen Parson 10 is *vt220*.

```
set noglob
eval `tset -e ^h -k ^u -i ^c -sr terminal_type`
unset noglob
stty all
setenv PATH /etc:/usr/etc:/usr/lib:$PATH
setenv
set ignoreeof
set noclobber
set
```

## Becoming the Superuser

It is a dangerous practice to use
the system administrator (*superuser* or *root*) account
as the environment for non-administrative tasks.
Like Superman, the superuser has the ability to do almost anything,
however, unlike Superman,
the superuser has few protections and should expect to suffer
the wrath of other users (if not your own personal inconvenience)
when presented with an inoperable system.

A system in the superuser environment is more vulnerable
than a system in a non-administrative environment
because the features that protect the system from the typical user
are removed in the superuser environment.
The superuser can do almost anything on the system
including making it totally inoperable
for the superuser and all other users.
While this is not irreversible
with a complete duplicate (backup) of the filesystems,
a set of installation tapes for UNIX and your other applications,
and a current set of documentation,
restoring the system is not a relaxing way
to spend the next twenty-four hours.

As the system administrator there are several items of information
that you should readily have.

Model Number of the system
Serial Numbers of all parts of the system
Processor Memory (eeprom memsize)
Swap Space (pstat -s)
Disk Memory (df)
Screen Size (eeprom scrsize)
UNIX Version Number (uname -a)
Host ID Number (hostid)    Hostname (hostname)
Internet Protocol Address (ifconfig le0)
Ethernet ID Number (dmesg)
Root Password

Most of these items are displayed at the console during the boot process.

dmesg    Displays system boot parameters.

more /var/adm/messages*    Displays the messages that appeared
on the system console in the last week.

eeprom    Displays hardware configuration information
for the Sun SPARCstation.

You can become the superuser (or any other user) from within any account with the *su* (set userid) command.
It is a security risk to use an *su* command without its full pathname.
It is also a security risk to run a user command while the superuser.
It is a major security risk to leave a superuser session unattended.

Use the next username in sequence to yours
as the argument to this command for this workshop
in the place of *nothing_for_superuser*.

| | |
|---|---|
| /bin/su *nothing_for_superuser* | Displays a *password:* prompt for another username. |
| *password* | Authenticates the new user and displays a command prompt for the other username. |
| whoami | Displays your new username. |

The *su* command does not normally change the current directory.

| | |
|---|---|
| pwd | Displays the directory of the original user. |

The USER, HOME, and SHELL environment variables are also maintained.

| | |
|---|---|
| setenv | Illustrates that you have the same environment as you had from your username. |
| suspend | Suspends your superuser session. |
| whoami | Displays your original username. |
| jobs | Displays the background processes. |
| fg | Returns the superuser (most recently suspended) session to the foreground. |
| whoami | Displays your new username. |

exit
Terminates your superuser session
and returns to your original session.

whoami
Displays your original username.

You can also become another user with the same environment
as the user has when he or she logs in.

/bin/su - *nothing_for_superuser*
Displays a *password:* prompt
for another username.

*password*
Authenticates the new user and
displays a command prompt
for the other username.

whoami
Displays your new username.

pwd
Displays the directory of the new user.

setenv
Illustrates that you have the environment
that you get when you login as another user
(the superuser) and the startup files
in the user's home directory (/) are executed.

Check the PATH variable in the environment.
It is a security risk to have the current directory
precede the system directories in the PATH.
The current directory can appear explicitly as a dot (.),
or as a pair of adjacent colons (::),
or as a single colon at the start of the PATH.
It is also a security risk to have the current directory
any place in the PATH of the superuser.
It is too easy to forget to check who has been able to write
bogus executables to the current directory.
Use *./filename* when you need to run a file in the current directory.

Th *su* - command does not work on the Encore:
do not issue the following *exit* command
unless you want to terminate your session completely.

| | |
|---|---|
| exit | Terminates your superuser session and returns to your original session. |

It is not necessary to start up and wait for a full session as another user to run a single command.

| | |
|---|---|
| su *nothing_for_superuser* -c “whoami” | Displays a prompt for the password of another user. |
| *password* | Authenticates the new user and and executes a single command as the other user. |

It is a compromise of security when more than one user can access the system with the same username.
The system keeps track of who knows how to get to other usernames, including the superuser username, in the /var/adm/sulog file.

| | |
|---|---|
| more /var/adm/sulog | Displays when the *su* command has been used. |

This file should be owned by the superuser and unreadable by others (700).

It is a loss of security when superuser access becomes available to an unknown users.
This is possible through poorly chosen passwords, an unsecured console, an unguarded station with a superuser session, or system directories that can be changed by unwarranted users.
Always exit superuser sessions before moving arms length from a station.