Unix系統導論

資訊系 郭雅貞
教學 717
email: kyj@cycu.edu.tw
電話: 2652913

課程簡介

- What is Unix
- Introduction to Unix
- Unix file system
- utilities
- Account management
- File system management
- Startup & Shutdown
- TCP/IP network management

課程簡介

- Patch
- Install & configure service
- NFS
- Cron
- System log
- Backup & restore
- Performance monitoring
- Shell script

計分方式

- 平常測驗　20%
- 作業　20%
- 期中上機測驗　15% (課程第9週週六下午考試)
- 期末上機測驗　25% (課程第17週週六下午考試)
- 線上互動　20%
- 額外加分

上課時間

非同步遠距(i-learning 上課)

原則上每星期五開放當週課程連結

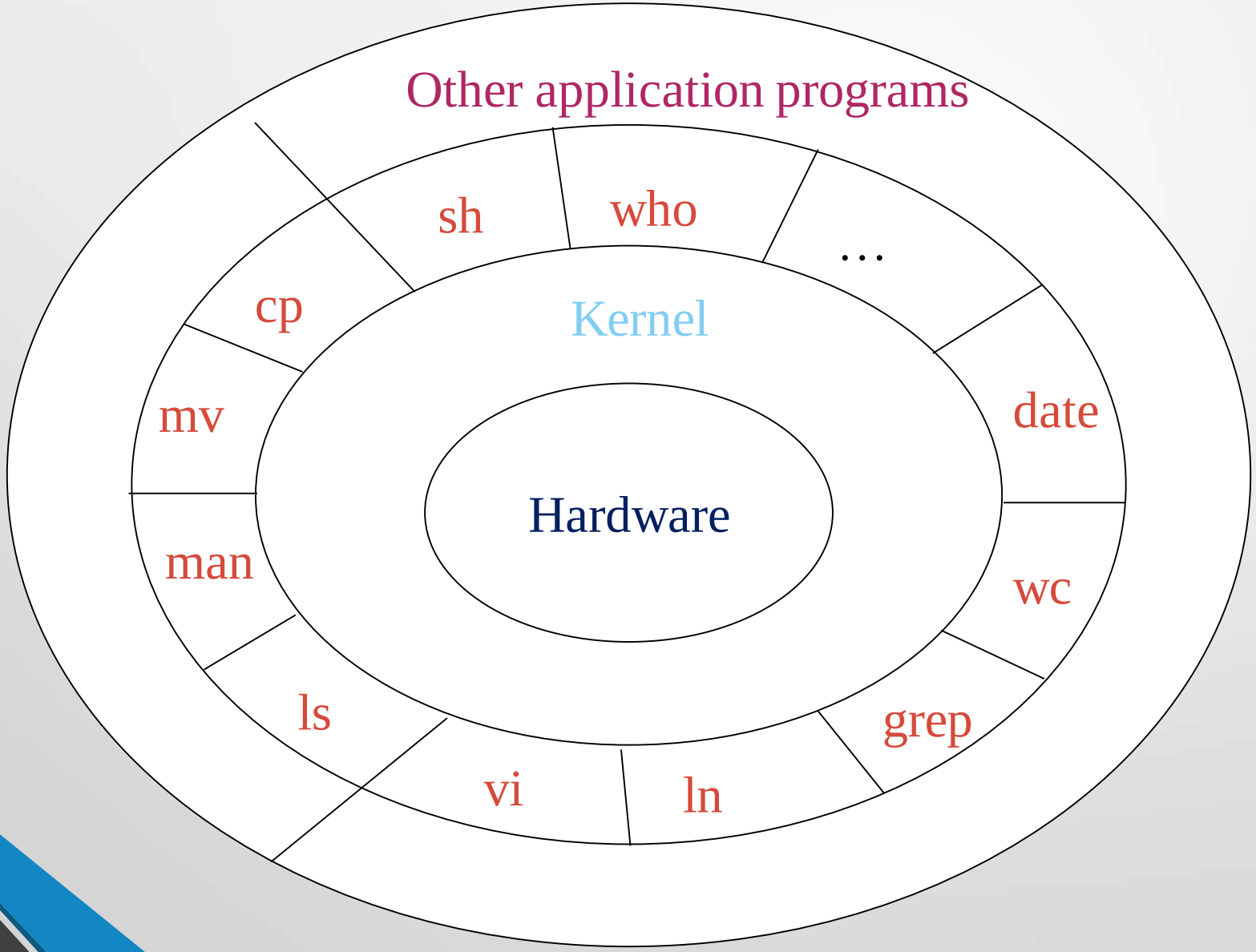

請遵守智慧財產權法規
不得非法影印

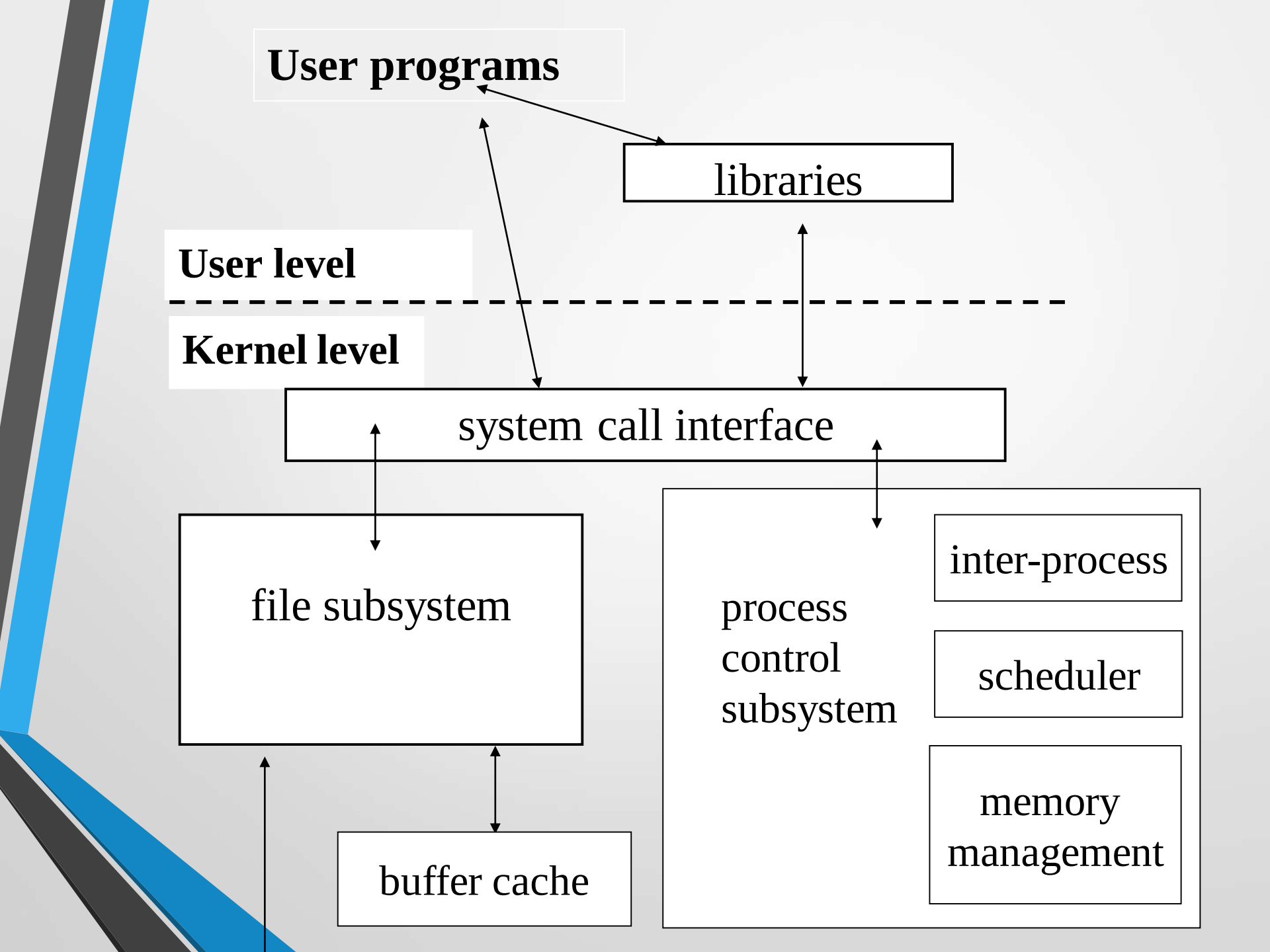
Introduction to Unix

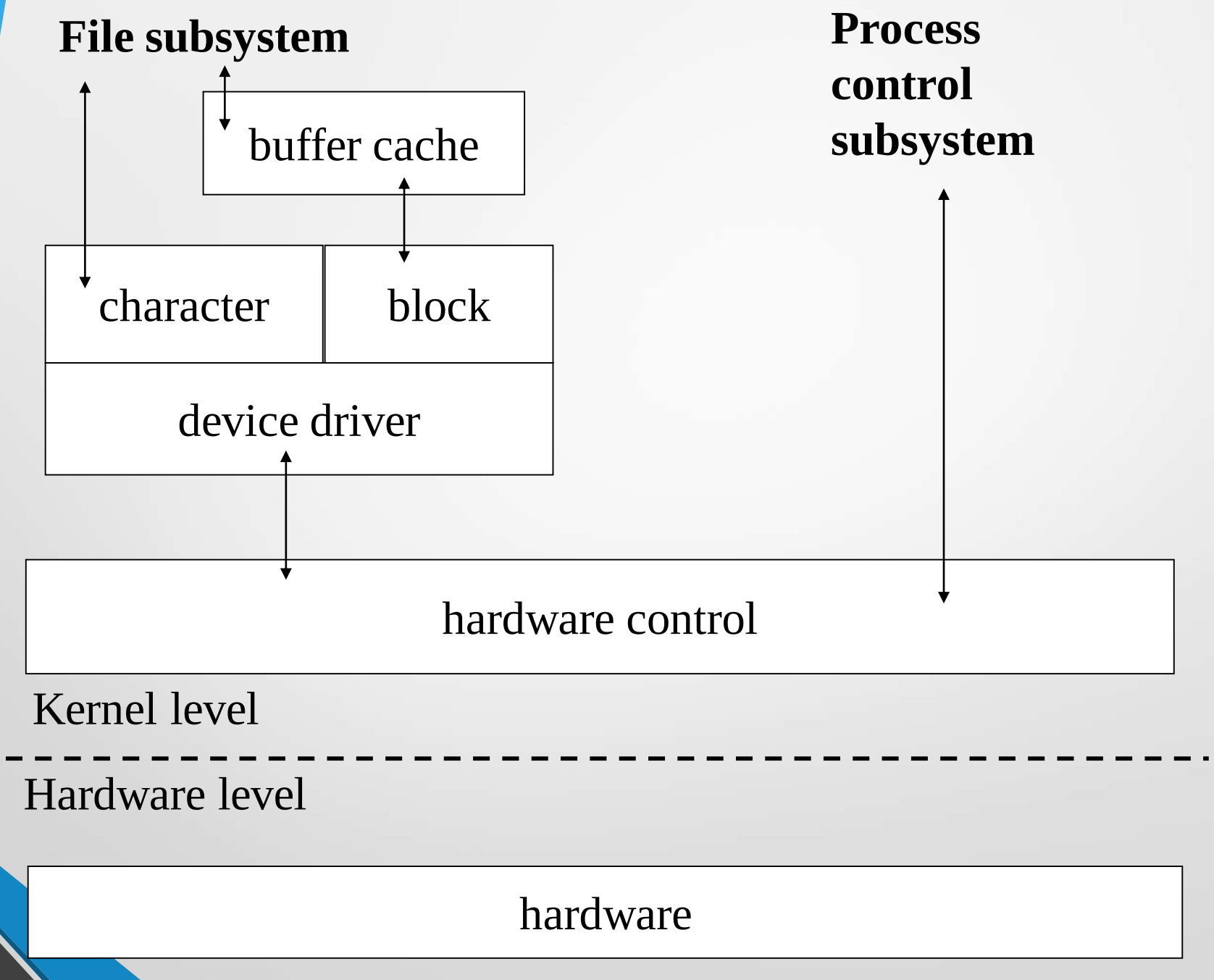
- 1960s AT&T Bell Lab. GE, MIT Multics
- 1970s Ken Thompson DEC PDP-7 Unix(Assembly)
- 1970s Dennis Ritchie Interdata 8/32 Unix(C)
- 1980s AT&T System V
  Berkeley BSD
  SCO Xenix
- 1990s AT&T USL Novell
  Berkeley BSD Release 4.4

What is Unix?

- Operating system
  - to make efficient use of the hardware
  - acts as the primary interface to hardware
- characteristics
  - multitasking
  - multiuser


Other application programs
sh
who
...
cp
Kernel
mv
date
Hardware
man
wc
ls
grep
vi
ln


User programs
libraries
User level
Kernel level
system call interface
file subsystem
process
control
subsystem
inter-process
scheduler
memory
management
buffer cache


File subsystem
Process control subsystem
buffer cache
character
block
device driver
hardware control
Kernel level
Hardware level
hardware

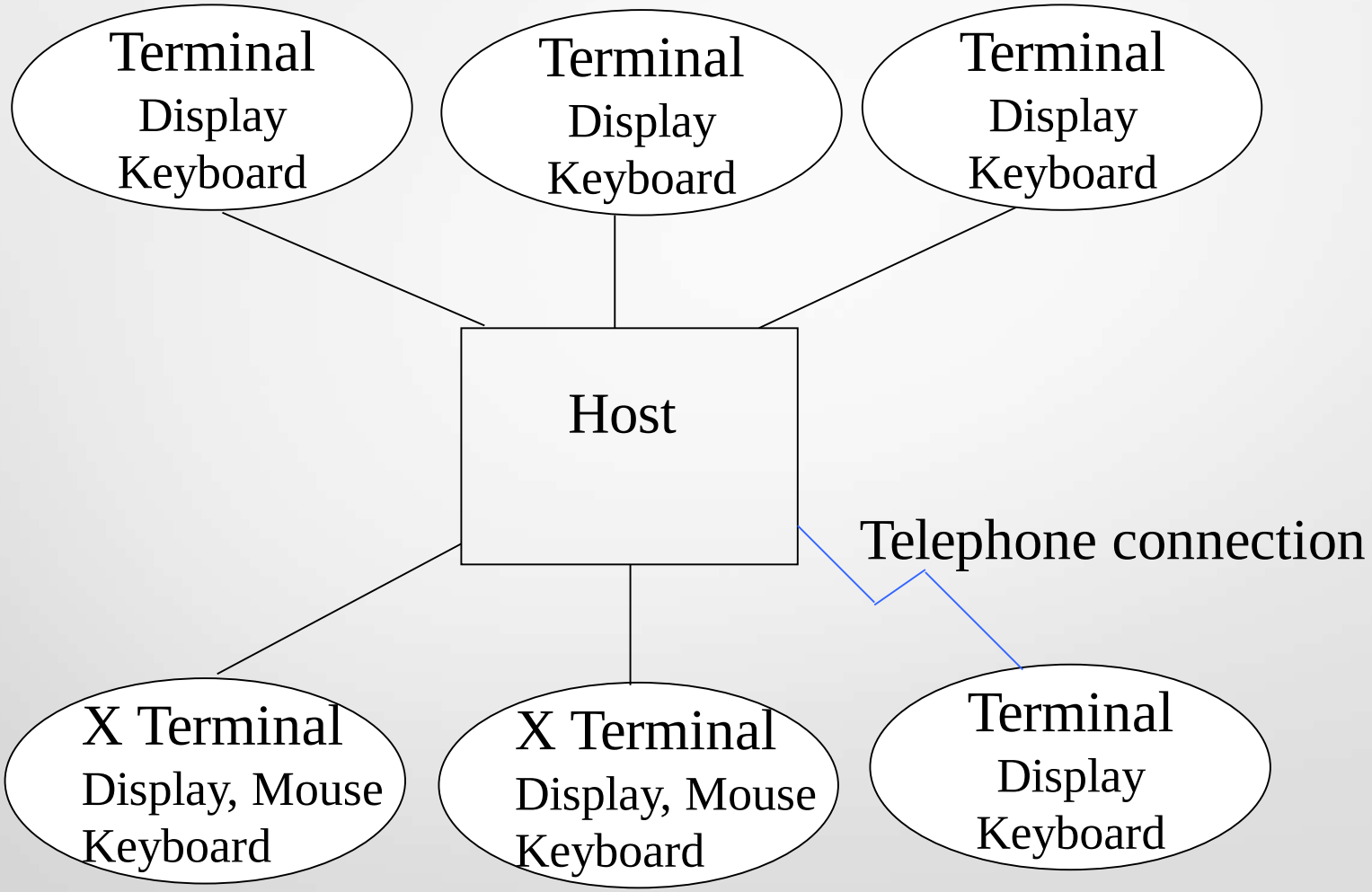
Major types of commercial Unix

Name of Unix	Company
AIX	IBM
HP-UX	Hewlett-Parckard(HP)
Solaris	Sun Microsystems
Irix	Silicon Graphics
Ultrix	Digital Equipment Corporation
SCO Unix	Santa Cruz Operation
Unixware	Novell

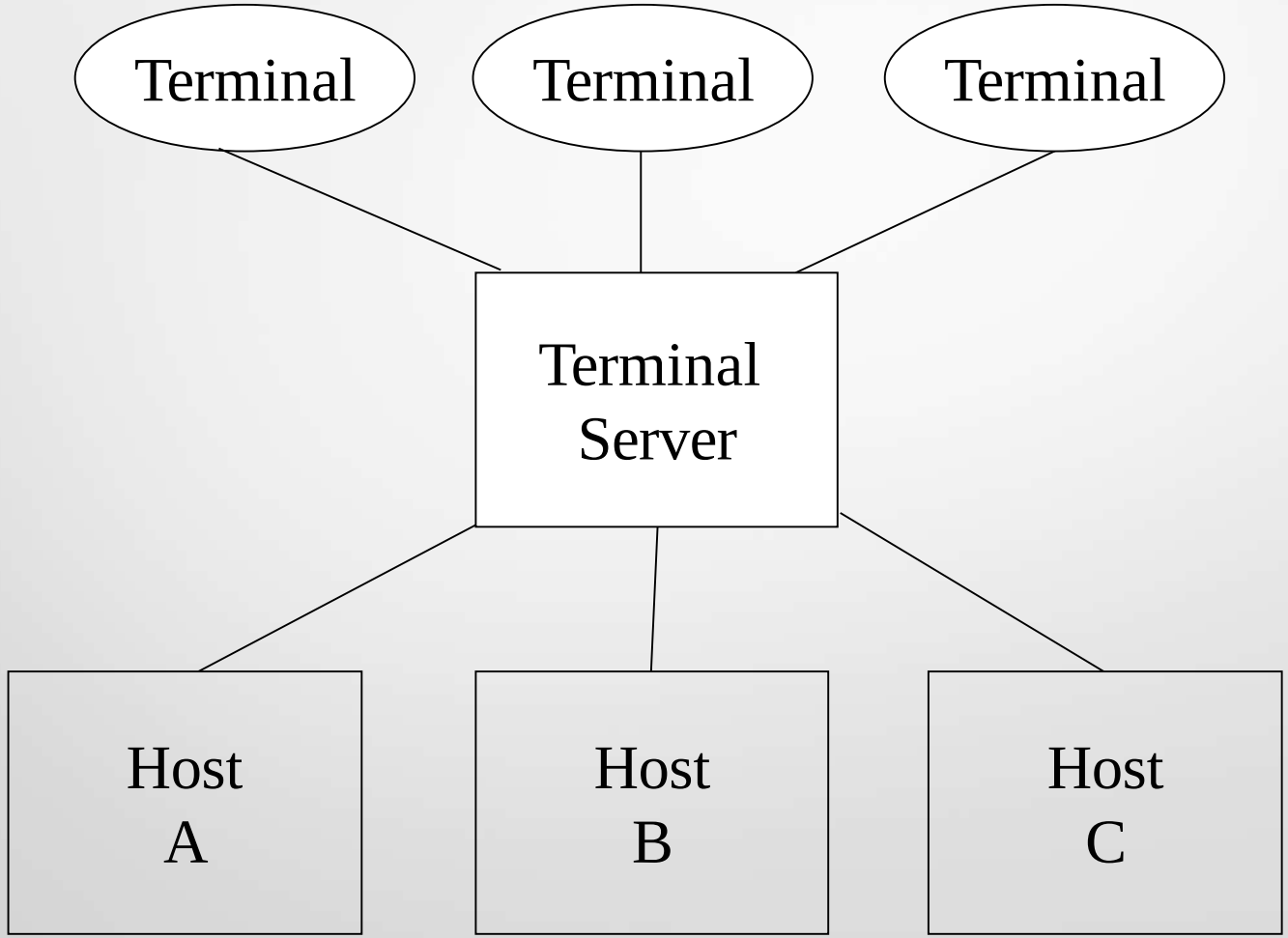
Major types of free Unix

- Linux
  - Redhat Linux
  - Debian Linux
  - SUSE Linux
  - Ubuntu Linux
  - …
- FreeBSD

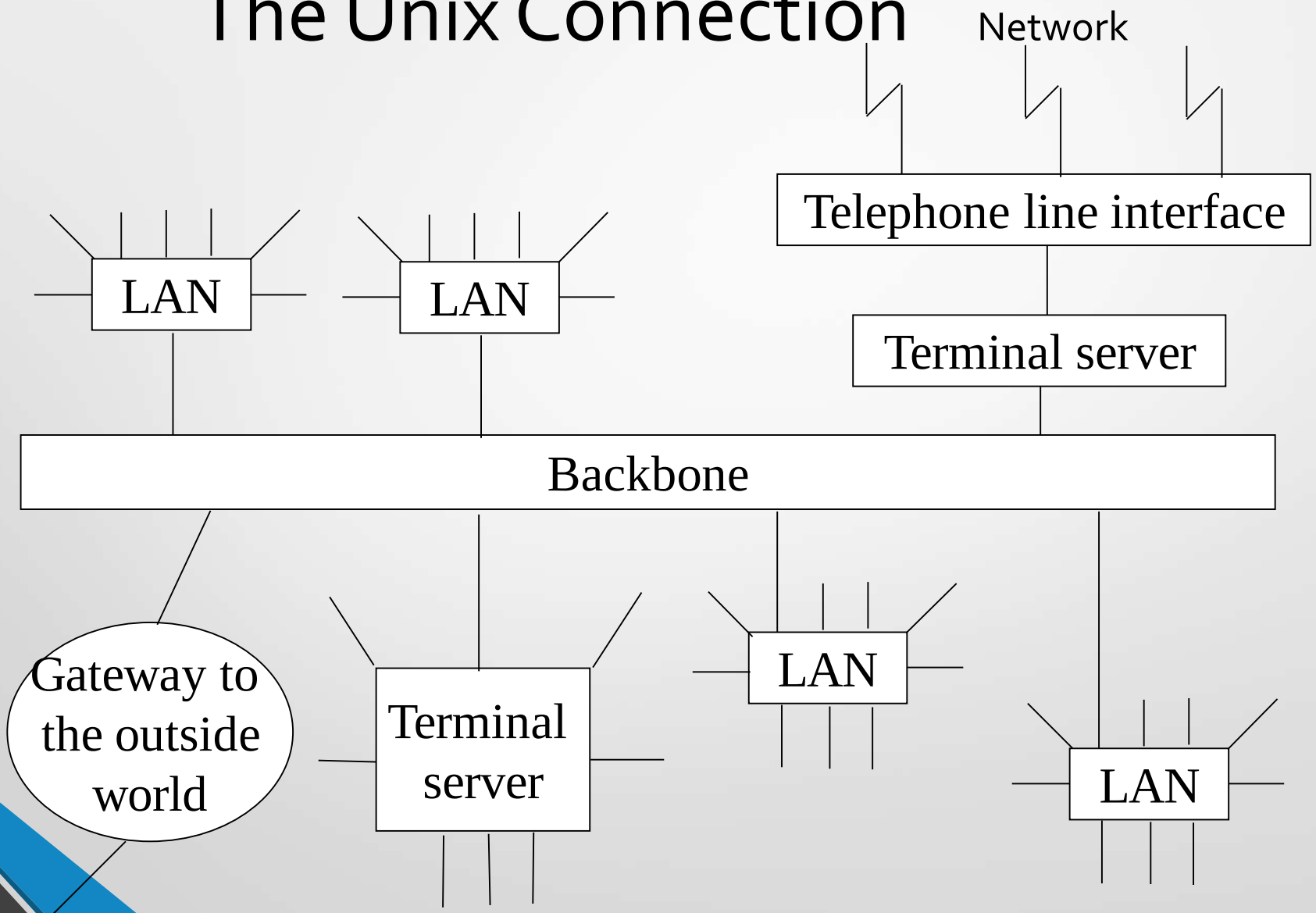
The Unix Connection Host- Terminal



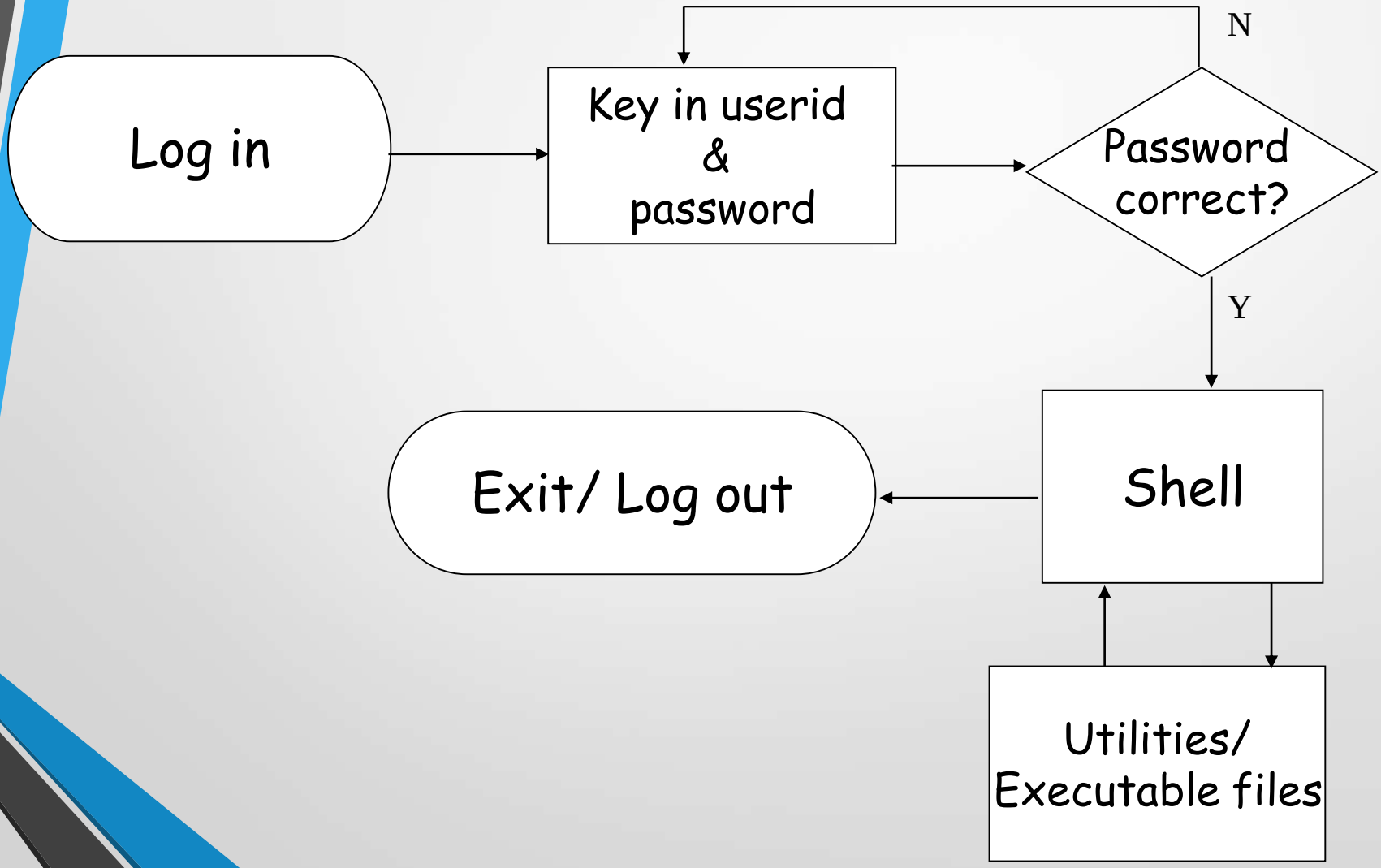
The Unix Connection Terminal server



The Unix Connection



Starting to Use Unix



虛擬化好處

- 能善用CPU、MEM 資源
- 省空間
- 省電
- 能避免因硬體故障、維修而服務中斷的時間過長

Using the keyboard with unix

The first terminals : Teletype ASR33

Control keys

intr ^C quit ^\ erase ^? werase ^W

kill ^Ueof ^D start ^Q stop ^S

susp ^Z

- List the keys

stty -a

- Change the keys

stty erase ^H

The online unix manual

Display the online manual

man *name*

- *name* online manual name
- Press <space> to display next page
- press q to quit displaying manual page

- NAME
  - the name & purpose of the command
- SYNOPSIS
  - the syntax of the command
- DESCRIPTION
  - a full description
- OPTIONS
  - detail of options

The format of a manual page

- Exit status
  - diagnostic, return value
- ENVIRONMENT
  - shell environment variables
- FILES
  - list of files important to this command
- SEE ALSO
  - where to look for related information

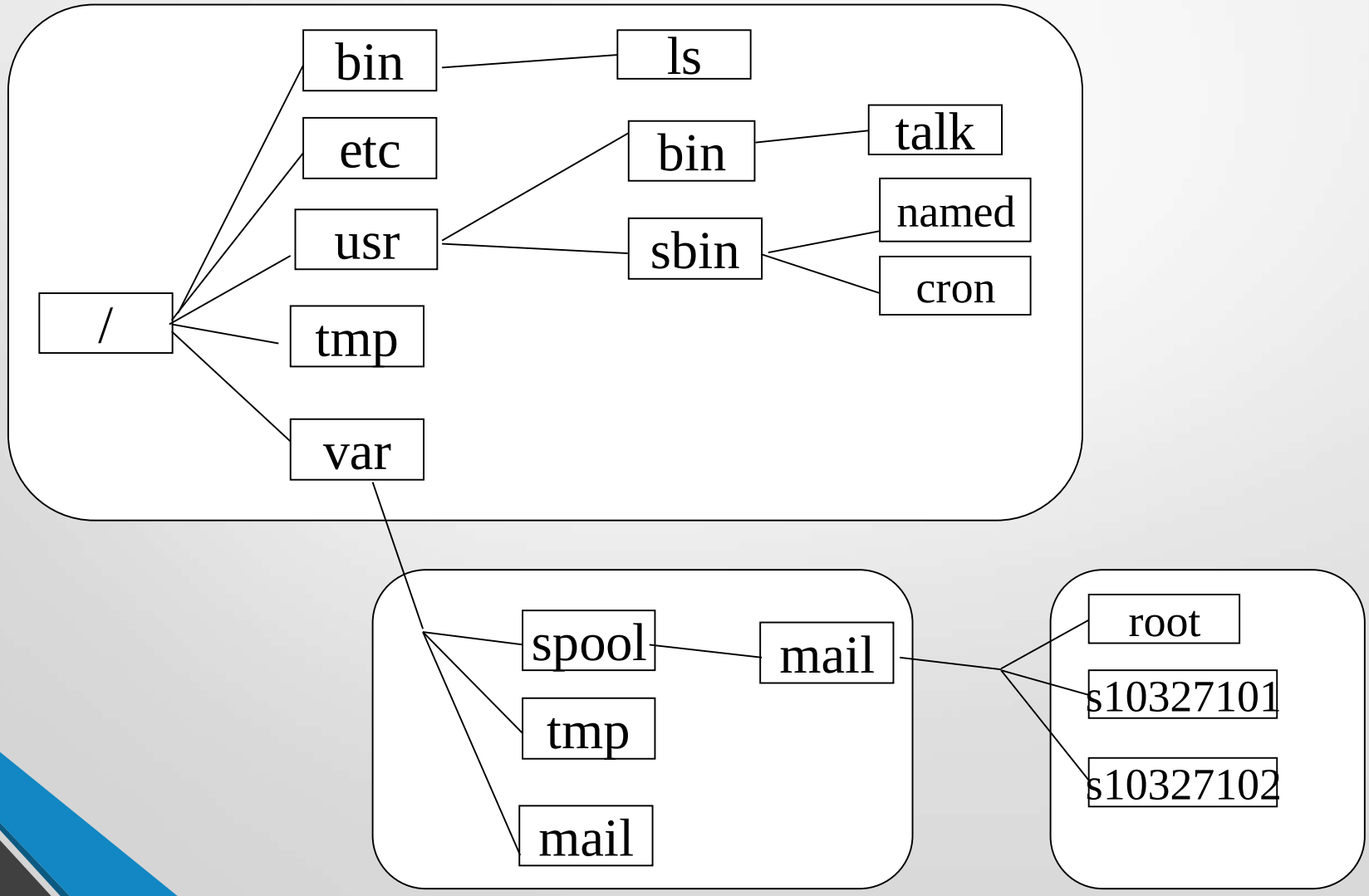
Manual sections

	BSD	SystemV
• user commands	1	1
• system calls & kernel error code	2	2
• library calls	3	3
• standard file formats	5	4
• Miscellaneous: character sets, filessystem types,date type defs.	7	5

Manual sections

	BSD	SystemV
games & demons	6	6/1
Special files & hardware	4	7
system admin. Commands	8	1m
Device drivers	4	7/9
maintainance commands	8	8

Tree-Structured File System



The Unix File System

- File
  - Any source from which data can be read, or any target to which data can be written
- File types
  - ordinary file(regular file)
  - directory
  - special file(device file)
- Name rule
  - any characters except /
  - better not use < > | ! & ? * [ ] $ # ^ \ : “ ( )

How to specify a file?

- relative path
  - Related to current working directory
- absolute path
  - Path begin at root directory

Command Syntax

command-name options parameters

Ex.

ls -l /usr

Multiple commands

command_1;command_2; command_3 . . .

Ex.

cd /; ls -a; cd /etc

Listing the contents of a directory

ls [-aAdFilnRs] [file...]

-a all entries

-A all entries except . and ..

-d If an argument is a directory, list only its name (not its contents)

-F Put a slash (/) after directory name, an asterisk (*) after an executable, and an at-sign (@) after a symbolic link

Listing the contents of a directory

ls [-aAdFilnRs] [file…]

-i print i-node number

-l list in long format

-n print uid, gid in numberic

-R recursively list subdirs

File types

Leftmost character of each line of ls –l output

- regular file

d directory

c character device file

b block device file

l symbolic link(soft link)

p named pipe(fifo)

s socket

File name substitution

Symbol	Meaning
*	match any sequence of zero or more characters
?	match any single char.
[ ]	match one of the enclosed char.

File permission

- r read the content of the file
- w change the content of the file
- x execute the file

File permission

- **s** Execute/search by owner/group; set user ID(group ID) on execution
- **S** No execute/search by owner/group; set user ID(group ID) on execution
- **t** Execute/search by others; set sticky bit on execution
- **T** No execute/search by others; set sticky bit on execution

File permission

with dir

- r read the names of the dir
- w make changes to the dir
- x search the dir

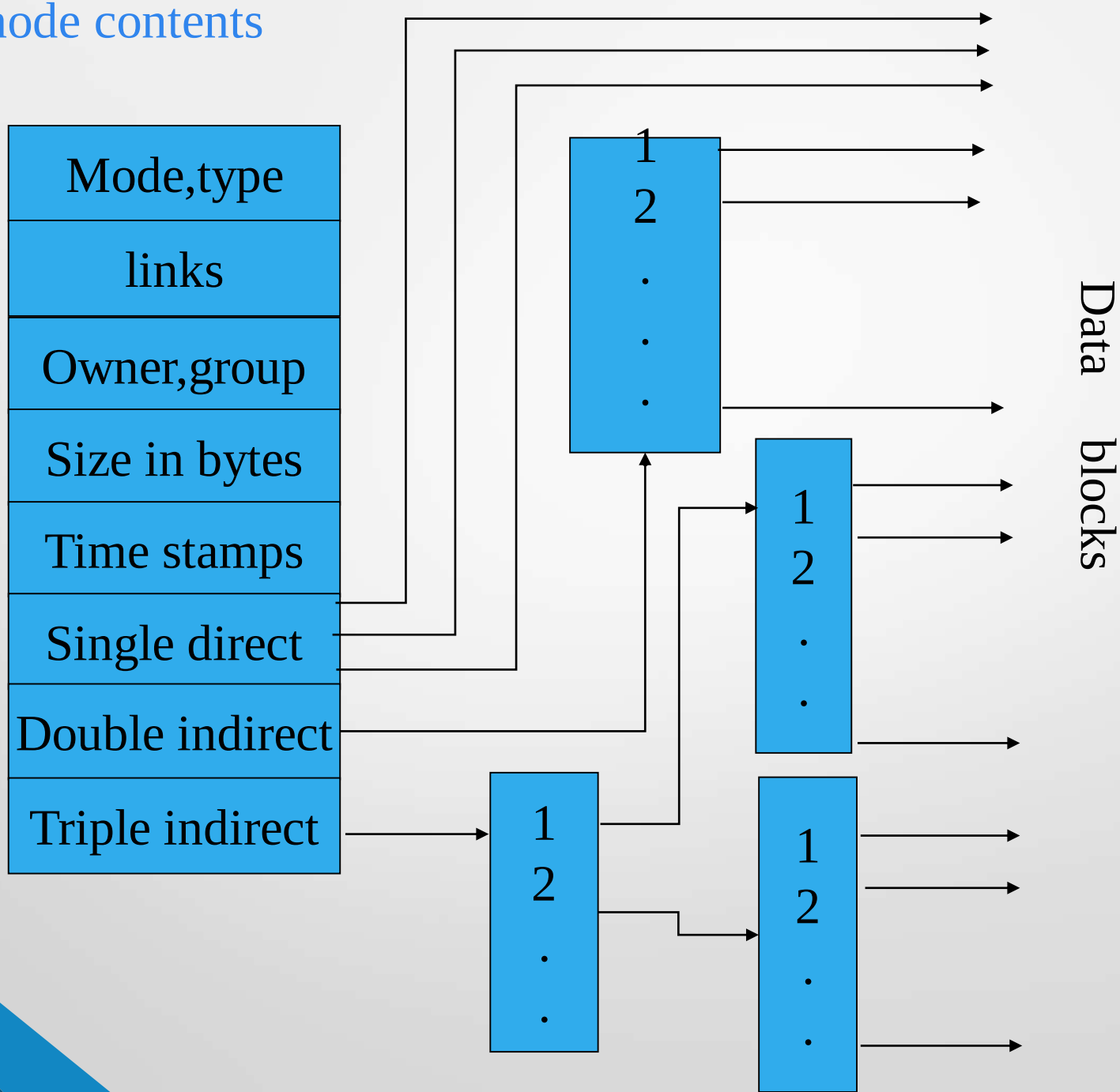
File system layout

- boot block
  - contain bootstrap code, typicaly the first secter
- super block
  - describe the state of the file system, how large it is, how many files it can store, where to find free space, and othe info.

File system layout

- inode table
  - echo inode contains file mode, file type, owner, group, size, time stamps.
- data block
  - contain file data

Inode contents



Changing file permission

chmod [-R] <absolute-mode> file…

chmod [-R] <symbolic-mode-list> file…

mode changing for	Operator
u(user)	- remove
g(group)	+ add
o(other)	= set
a(all)	

Changing owner

chown [-R] owner[:group] file…

-R recursive

Changing group owner

chgrp [-R] group file….

-R recursive

Changing group owner

chgrp [-R] group file….

-R recursive

Working with directories

- working directory (current directory)
- handy pathname abbreviations

  .

  ..

  ~

  ~username

Working with directories

- Moving arround the directory tree

  cd [directory]

  pwd

- Making a new directory

  mkdir [-m mode] [-p] dir …

  -p create dir by creating all non-existing parent dirs

Removing directory

rmdir [-p] dir …

-p remove parent dir if parent dir becomes empty

Moving directory

mv [-fi] sourcedir targetdir

-f move file(s) without prompting even if it is writing over an existing target. Default if stand input is not a terminal

-i will prompt for confirmation whenever the move would overwrite an existing target

Copying file

cp [-Rfip] sourcefile targetfile

-f unlink the destination file and proceed

-i interactive

-p preserve source uid,gid,permission, modify access time

-R recursive

Moving file

mv [-fi] sourcefile targetfile

-f fource

-i interactive

Removing file

rm [-Rfi] file ….

-f Remove all files (whether write-protected or not) in a directory without prompting the user.

-i interactive

Hard & Symbolic(soft) links

ln file linkname

- Hard link
  - same inode
  - cannot link to dir
  - cannot link to file in different file system

ln -s file linkname

- Symbolic link(soft link)
  - different inode system

Displaying files

- Displaying the beginning of a file

head [-n count] [file…]

- Displaying the end of a file

tail [-n count] [file]

Displaying files using more

more [-cs] [+startline][+/pattern][file…]

- -c clear screen
- -s squeez. Replace multiple blank lines with a single blank line
- +startline Start up at linenumber
- +/pattern Start up two lines above the line containing the regular expression pattern

Basic commands of more

h	display help info.
<space>	display the next screenful
q	quit the progrem

Advances commands of more

<enter> go forward one line

n<enter> go forward *n* lines

f go forward one screenful

b go backward one screenful

Advances commands of more

/pattern search forward for specified pattern

n repeat the previous search command

v start the vi editor using the file

!command execute the specified shell command

= display current line number

Redirection and pipes

- Standard input
  - keyboard
- standard output
  - screen
- standard error output
  - screen

Redirecting standard output

Command > file

Command >> file

- > If file exists, will replace existing file. If file does not exist, the file will be created
- >> append to tail of the file

Note: if the shell inovked with the option –C (noclobber is enabled) , > could not replace an existing file. Must use >| to replace existing file

Redirecting standard error output

Command 2> file

Command 2>> file

Redirection and pipes

- Redirecting standard input

Command < file

- Pipelines

cmd1 | cmd2 | cmd3 |cmd 4…

Other Utilities

- Displaying time & date

date

- how long has the system been up?

uptime

Other Utilities

- Who am I?

whoami

- displaying userid that are logged in

users

- Info. about logged-in users

who

- Finding out what someone is doing

w

Filters

- Filters reads from standard input & write to standard output
- cat - concatenate and display files

cat [-nb] [file ….]

-n output with line number

-b omit the line numbers from blank lines

Filters

- Cut out selected fields of each line of a file

cut -f list [-d delim] [file…]

-f a list of fields assumed to be separated in the file by a delimiter

-d the field delimiter

Filters

- merge corresponding or subsequent lines of files

paste [-s][-d list] file…

-s Concatenate all of the lines of each separate input file in command line order

-d Unless a backslash character (\) appears in list each character in list is an element specifying a delimiter character

Filters

- sort, merge, or sequence check text files

sort [-fru] [-o outfile][infile…..]

-f fold lower case into upper case

-r sort in reverse order

-u unique

-m merge only; all files must be sorted

Filters

- report or filter out repeated lines in a file

uniq [-cdu] [infile][outfile]

-c Precede each output line with a count of the number of times the line occurred in the input

-d retain one copy of all lines are duplicated

-u retain only lines that are not duplicated

Filters

- Counting lines, words & characters

wc [-lwc] [file….]

-l lines

-w words

-c characters

Filters

- search a file for a pattern

grep [-cilnv] pattern [file…]

-c Print only a count of the lines that contain the pattern

-i ignore upper/lower case

-l print only names of files with matching lines

-n Precede each line by its line number in the file

-v Print all lines except those that contain the pattern

Regular expression

Symbol	Meaning
.	Match any single char. Except newline
*	match zero or more of the preceding char.
^	match the beginning of a line
$	match the end of a line

Regular expression

Symbol	Meaning
[ ]	match one of the enclosed character
[^]	match any char. that is not enclosed
\	take the following symbol literally

Command substitution

`commands`

Conditional command execution

1st cmd succeeds	operator	2nd cmd excutes
yes	||	no
no	||	yes
yes	&&	yes
no	&&	no

The shell

- command processor
- a program that reads and interprets the commands you enter
- a programming language

Shell Family

Bourne shell family:

Bourne shell sh

Korn shell ksh

Bourne again shell bash

C shell family:

C shell csh

Tcsh tcsh

Job

- Job
  - consisting of commands specified in a command line
- Forground job
  - wait until it finishes. Shell displays its prompt when it is ready for our next command
- Background job
  - do not need to wait until it finishes. Shell display its prompt imemediately

Forground job

Job control 2

- How to suspend a forground job?

^Z

- How to restart the suspended job?

fg [*job*]

Listing jobs

- List jobs

jobs

- List jobs with pid

jobs –l

Background job

Job control 4

- How to run background job

comand&

- How to suspend a background job?

kill -19 *pid*

How to resume background job?

bg [*job*]

Background job

Job control 5

- force shell suspend background job that attempts to write to the terminal

stty tostop

- not suspend background job that attempts to write to the terminal

stty -tostop

Terminate Job

- By process id

kill *pid*

kill -9 *pid*

Detached jobs

- a background job that continues to run after you logout

nohup command&

Alias

- **Create an alias**

alias [name [= value]]

- **list all alias and their definition**

alias

Alias

- **display alias definition**

alias name

- **release alias**

unalias name

- **release all alias**

unalias –a

Alias

How does the shell execute aliases and in what order?

1. Alias substitution
2. Build-in commands
3. Commands in your search path

History

- the number of previously entered commands accessible to this shell

export HISTSIZE=*size*

- Command history

history

!*number*

!*patten*

Arrow keys

Setting up shell variable

variable=value

- variable name must begin with a-z/A-Z and followed by a-z/A-Z/0-9/_
- Value of shell variable substitution

$variable

${variable}ext

“$variable”ext

- Length of shell variable

${#variable}

Setting up shell variable 2

- export shell variable

export [variable[=value]]

- Setting up read only variable

readonly [variable[=value]]

- Unset variable

unset variable

Environment variables 3

LOGNAME user name
SHELL login shell name
HOME user's login dir.
PATH search path for cmds
CDPATH search path for the cd cmd
PS1 system prompt
PS2 system prompt
TERM terminal type

Variables automatically setted 4

? returned value of last executed cmd.

$ the process id of this shell

! the process id of last background cmd.

Login/Logout script

Login scripts

- /etc/profile The systemwide initialization file, executed for login shells
- ~/.bash_profile ~/.bash_login

~/.profile individual initialization file for login shells

Logout script

- ~/.bash_logout individual logout script

Escaping

Escaping character

- back slash \

Escaping strings

- dobule quotation marks "…"
  - allow variable expansion
  - allow command substitution
- single quotation marks '…'
  - do not allow variable expansion
  - do not allow command substitution

Command parsing order

- finding words
- parsing the sequence of words
  - Quoting with ' ' and " "
  - Alias substitution
  - I/O redirection, background execution, and pipes
  - Variable substitution
  - Command substitution
  - Filename expansion
- execute the command

How to execute shell script?

- bash script_file
- bash < script_file
- chmod u+x script_file script_file(or ./script_file)

Add group

Account management 1

- groupadd [-g gid] group
  - -g gid gid must be unique
    - 0~999 for system accounts
- add entry for the user into file /etc/group /etc/gshadow manually

Remove group

Account management 2

- groupdel group
- remove entry of the user from /etc/group /etc/gshadow manually

Modify group

- groupmod [-g gid] [-n *grp*] *group*
  - -n grp the group name will be changed from *group* to *grp*
- edit /etc/group /etc/gshadow file manually

/etc/group file format

name:password:gid:user_list

- name- group name
- password – encrypted group password
- gid – numerical group id
- userlist – group member user names ,seperated by comma

/etc/gshadow file format

name:password:administrators:members

- name- group name
- password – encrypted group password
- administrators – comma-separated list of user names
- members – comma-separated list of user names

Add user

- Add by command

useradd [–u uid] [-g grp] [-c comment] [-d home-dir] [-m [-k skel-dir]] [-s shell] login

  - **skel-dir default /etc/skel**

- Add manually
  - add entry for the user into file /etc/passwd, /etc/shadow
  - create home directory for the user
  - create login files for the user
  - setup password for the user

Remove user

Account management 7

- remove by command

userdel [-r] login

-r remove user's home dir and mail spool

- remove manually
  - remove entry of the user from /etc/passwd /etc/shadow
  - remove all files belong to the user

/etc/passwd file format

name:password:uid:gid:gcos-field:home_dir:login_ shell

- name – name of user
- password – encrypted password
- uid – numerical user id
- gid – numerical group id
- gcos-field – optional and only used for informational purposes
- home_dir – user's home directory
- login_shell – program to run at login

/etc/shadow file format

Account management 9

- Field seperator :
- Fields
  - name of user
  - encrypted password
  - days since Jan 1 1970 that password was last changed
  - days before password may be changed
  - days after which password must be changed
  - days before password is to expire that user is warned
  - days after password expires that account is disabled
  - days since Jan 1 1970 that account is disabled
  - a reserved field

Mount & Unmount

Adding new devices 1

Mount

- the process that makes a disk's contents available to the system, merging it into the system directory tree

Unmount

- the process that remove a disk's contents from the system directory tree

Steps for adding a new disk

Adding new devices 2

- **connect the disk to the computer**
- **create devices files through which the disk can be accessed**
- **create filesystem within disk partition**
- **Mount the filesystem**
- **set up automatic mounting**

Linux naming scheme

Adding new devices 3

- https://www.mjmwired.net/kernel/Documentation/devices.txt
- Device files are located in /dev
  - Major number
  - Minor number

Create device file

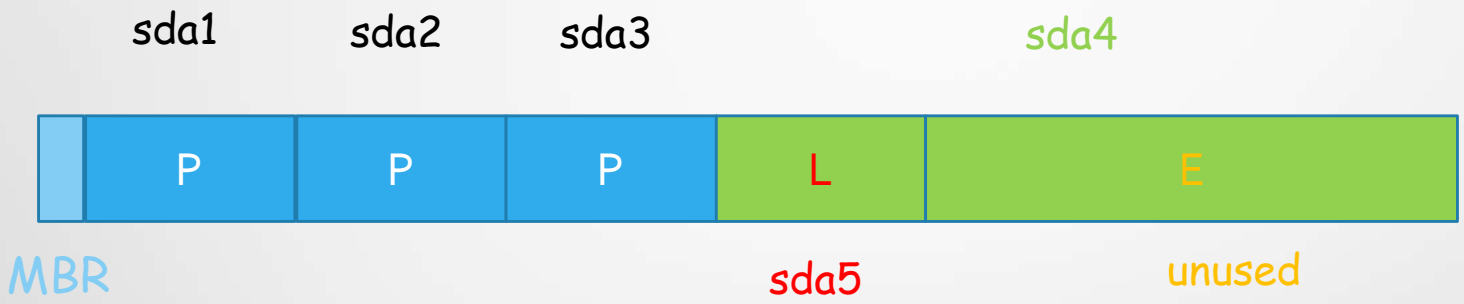
Adding new devices 4

mknod [option]… name type [major |minor]

- -m mode
- type
  - p FIFO
  - b block device
  - c character device

Describe MBR, Primary, Extended, and logical partitions

- IBM PC Disk Partition graphic



- MBR only permits 4 primary partitions
- One primary can be an extended partition, a container for other logical partitions

Partition disk

Adding new devices 6

fdisk *device*

- m help
- p print patition table
- n add a new partition
- d delete a partition
- l list known partition types
- t change a partition's system id
- w write table to disk and exit

create new file system

Adding new devices 7

mkfs [-v][-t fstype] [fsoption] file [blocks]

- -v verbose output
- -t fstype specify file system type
- fsoption options for the file system type
- file device file
- block no. of blocks used for the filesystem

Mount filesystem

Adding new devices 8

- make mount point

mkdir name

- Mounting file system

mount [-t fstype] device-file mount-point

Setting up automatic mounting

Adding new devices 9

- add entry to /etc/fstab

File format

special file mount point type mount options
  backup frequency pass number comment

Ex.

/dev/sdb /std ext4 rw 0 0 #mydata

Validate a filesystem

Adding new devices 10

fsck [-sARV][-t fstype] [filesystem …][-- fsck-options]

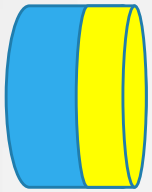
- -s serialize the fsck operation
- -A check file system listed in /etc/fstab. Skip all fs_passno 0.
- -R do not check root file system when with –A
- -V verbose
- -t fstype specify filesystem type
- fsck-options options to pass to filesystem specific checker

General LVM Concepts and Terms

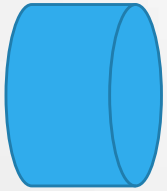
Adding new devices 11

- Physical storage
- Physical volume(PV)
- Volume group(VG)
- Logical volume(LV)
- Physical extent(PE)
- Logical extent(LE)

LVM



Create logical volume(LV)



Create volume group(VG)

Create physical volume(PV)

Partition physical storage

Initial LVM Deployment

Adding new devices 13

- Create new partition
  - Use Disk utility to create new partition
  - Change the partition type to Linux LVM(ox8e)
- Create PV

pvcreate *DevPath*

- Create VG

vgcreate *VG-Name DevPath…*

Initial LVM Deployment

Adding new devices 14

- Create LV

lvcreate *–l extent_no | -L size [-n lvname] Vgname*

- Create filesystem on LV

mkfs *–t type LV-path*

- Make mount point if needed

mkdir *mount_point*

- Mount the LV

mount *LV-path mount_point*

Displaying current LVM usage

- Display PV

pvdisplay –v *DevPath*

- *Display VG*

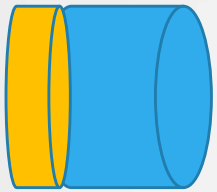
vgdisplay –v *VG-Name*

- *Display LV*

lvdisplay –v *LV-Path*

Extending a Volume Group

Adding new devices 16



Extend volume group(VG)

Create physical volume(PV)

Partition physical storage

Extending a Volume Group

Adding new devices 17

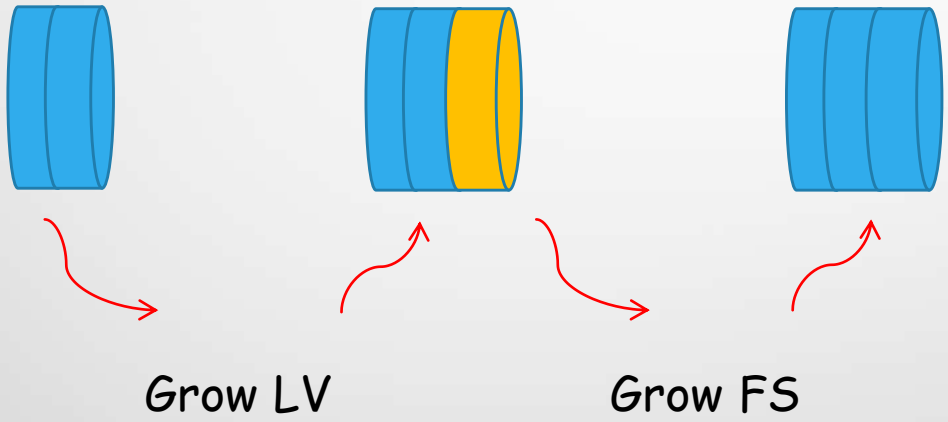
Steps

- Partition physical storage
- Create physical volume(PV)
- Extend volume group (VG)

vgextend *VG-Name DevPath*

Extending a Logical Volume

Adding new devices 18



Extending a Logical Volume

Adding new devices 19

Grow LV

lvextend *–l [+]extent_no | -L [+]size lvname*

Grow FS

resize2fs *DevPath*

Removing a physical volume

- Migrate all physical extents from the physical partition which will be removed

pvmove *[sourcePV] [DestPV]*

- Remove the physical volume(PV) from volume group(VG)

vgreduce VG-name DevPath…

- Remove the physical volume(PV) from LVM

pvremove DevPath…

Planning disk quotas

Planning disk quotas

- **Which file system requires disk quotas**
- **What limits to set**
  - **soft and hard limits?**
  - **limits for each user?**
  - **How long can a user exceed soft limits?**

How to set up disk quotas

Adding new devices 22

- **Mount the filesystem with quota|usrquota|grpquota option**
- **Execute *quotacheck /Path* to create *aquota.user* file in root level of the file system**
- **Execute *quotacheck –g /Path* to create *aquota.group* file in root level of the file system**

How to set up disk quotas

Adding new devices 23

- **Set user quota by executing**

edquota user

- **Set group quota by executing**

edquota –g group

- **Execute *quotaon /Path***

Automatic mount filesystem with quota options

Adding new devices 24

Edit */etc/ fstab*

- special file, mount point, type, options, backup frequency, pass number , comment

Ex.

/dev/sdb /test ext4 rw,usrquota,grpquota 0 4 #userdata

Set user quotas

edquota [-p proto-user] ***username***

- block size = 1KB

Ex.

Disk quotas for user xxx (uid zzz):

Filesystem blocks soft hard inodes soft hard

/dev/hdb 124 900 1024 50 90 100

Set user quotas

Adding new devices 26

- edquota -t

  Filesystem Block grace period Inode grace period

  /dev/sdb 7days 7days

User quotas

Adding new devices 27

- Summarize quotas for a file system (each user)

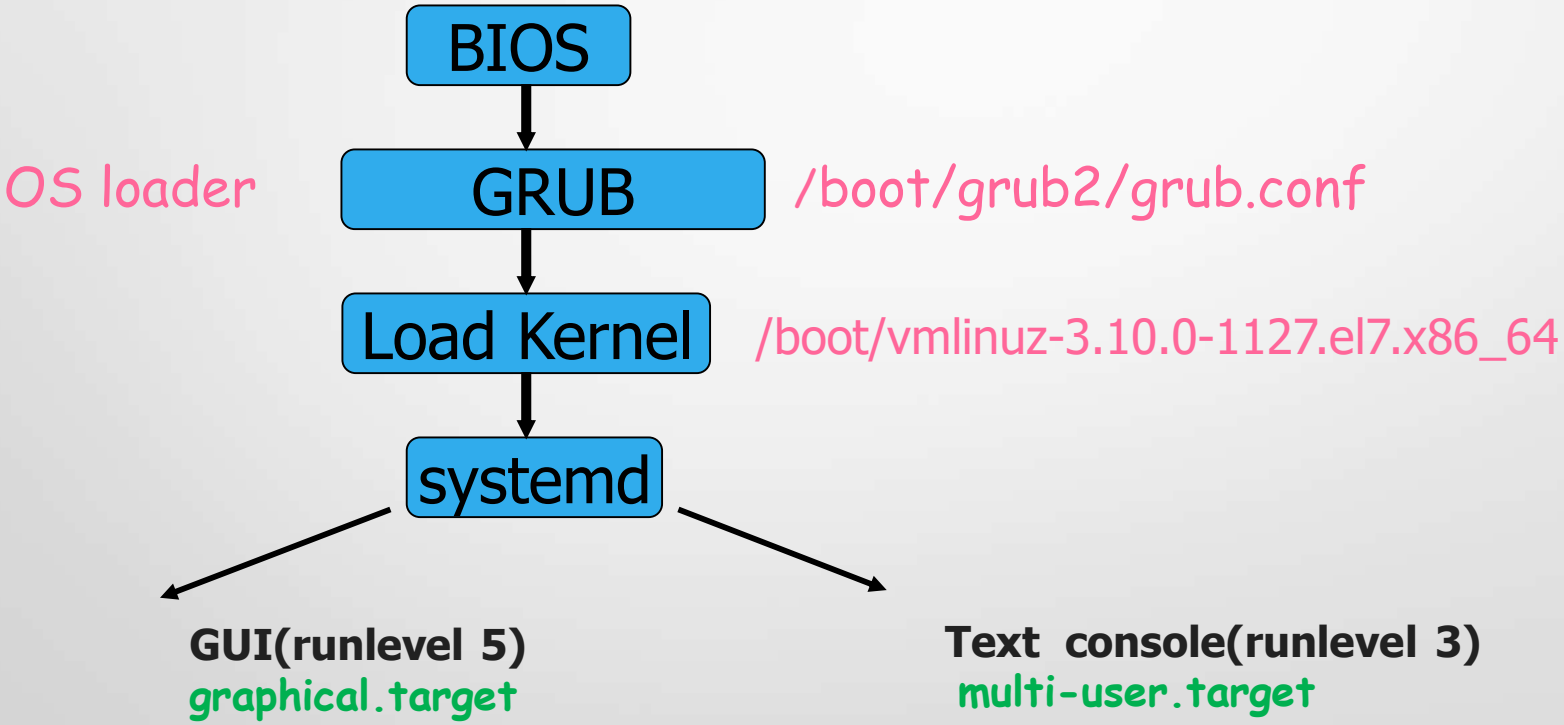
  repquota /Path

- Report individual Usage

  quota -v user

Boot process

Startup & Shutdown 1



Initial loader & System startup

- BIOS:Firmware that runs at power on, enables features of built-in hardware and determines device to boot from
- GRUB(Grand Unified Bootloader): program loaded from the boot device that determines the operating system kernel to load
- Linux Kernel: core operating system executable responsible for coordinating software access to hardware resoursces
- systemd : First linux process started, ultimately starts all other processes

Run levels

Run levels:	
0 - for halt system	poweroff.target
1 - for system maintainance	rescure.target
2 - multiuser mode without NFS	multi-user.target
3 - full multiuser mode	multi-user.target
4 - not used	multi-user.target
5 - for X11 environment	graphical.target
6 – for reboot	reboot.target

Change run level:

init [0123456]

Getting Past a GRUB Misconfiguration

- Interrupt Grub countdown
- Use ‘e’ to edit current configuration
- append *number* at the end of the *linux16* line
- The *number* has to be a separate argument so a space is required before the *number*

Making persistent GRUB changes

Startup & Shutdown 5

Edit /etc/default/grub

- GRUB_TIMEOUT=5
  - how long countdown occurs
- GRUB_CMDLINE_LINUX="crashkernel=auto rd.lvm.lv=centos/root rd.lvm.lv=centos/swap
  rhgb quiet"
  - rhgb redhat graphical boot
  - quiet hides the majority of boot messages before rhgb starts.

Update /boot/grub2/grub.cfg

- grub2-mkconfig -o /boot/grub2/grub.cfg

Changing default runlevel

- cat /etc/inittab
- To view current default target

systemctl get-default

Changing default runlevel

- To set a default target

systemctl set-default *TARGET.target*

  - *poweroff.target*: runlevel 0
  - *rescue.target:* runlevel 1, s, single
  - *multi-user.target* : runlevel 3
  - *graphical.target* : runlevel 5
  - *emergency.target*: emergency

Why shut down the system?

Startup & Shutdown 8

- **to conduct administrative activities**
  - **check file systems**
  - **system updates**
  - **add hardware**
  - **…**
- **to halt the system so it can be turned off**

Shutdown command

shutdown [-hrc] time [message]

- **-h halt after shutdown**
- **-r reboot after shutdown**
- **-c cancle an already shutdown**
- **time hh:mm/+m/now**
- **message warning message**

Shutdown & reboot cmds

halt [-p]

-p do poweroff after halt

reboot

poweroff

TCP/IP network model Concept

TCP/IP networking 1

- **Application layer**
  - **end-user application programs**
- **Transport layer (TCP/UDP)**
  - **communication among programs on the net**
- **Network layer (IP)**
  - **basic communication, addressing, and routing**
- **Link layer**
  - **network hardware & device driver**

Packet addressing

TCP/IP networking 2

- **Hardware addressing**
  - **the lowest addressing**
- **Internet addressing**
  - **IP addressing**
  - **mapping between IP address & hardware address is implemented at the link layer**
- **Ports**
  - **address particular processes or services**

Internet address(IP address)

TCP/IP networking 3

Internet address(IP address)

- 4 bytes
- N: network part
- H: host part
- Class A 1-126.X.X.X N.H.H.H
  - Private ip 10.0.0.0 ~ 10.255.255.255
- Class B 128-191.X.X.X N.N.H.H
  - Private ip 172.16.0.0 ~ 172.31.255.255
- Class C 192-223.X.X.X N.N.N.H
  - Private ip 192.168.0.0 ~ 192.168.255.255
- Class D 224-239.X.X.X H.H.H.H
- Class E 240-255.X.X.X for IETF research

Concept

steps in setting up a network

- **Obtain an unused IP address from network administrator**
- **Install the network hardware**
- **configure network interfaces (at boot time)**
- **Set up default gateway**

Configure network interface

TCP/IP networking 5

ifconfig [interface]

ifconfig interface [address_family] options | address …

- **interface name of the interface, driver name followed by a unit number.**
- **address_family**
  - **inet TCP/IP, default**
  - **inet6 IPv6**
  - **ipx Novell IPX**
  - **…**

Configure network interface

TCP/IP networking 6

options

- **up activate the interface**
- **down shutdown the interface**
- **netmask addr set netmask**
- **address IP address**

Manipulate routing table

route add [-net|-host] target [netmask *mask*] [gw *GW*] [dev] *if*]

route del [-net|-host] target [gw GW] [netmask *mask*] [[dev] If]

- **add | del** add/delete a route
- **-net | -host** specifies the type of target address
- **target** host name | net name | default

Manipulate routing table

TCP/IP networking 8

- **netmask *mask*** **set network mask to be used**
- **gw *GW*** **route packet via gateway GW**
- **dev *if*** **force the route to be associated with the specified device**

Network fault isolation

TCP/IP networking 9

Show routing table

route

netstat -r

Network fault isolation

TCP/IP networking 10

ping [-i interval] [-c count] destination

- **-i interval interval between sending packets**
- **-c count stop after sending count packets**
- **destination domainname or IP address**

Network fault isolation

TCP/IP networking 11

Show arp table

arp –a

Delete entry in ARP table

arp -d hostname

Network fault isolation

TCP/IP networking12

Obtaining & assigning internet addresses

- **/etc/hosts**

ip_address canonical_hostname [alias…]

Network fault isolation

TCP/IP networking 13

Resolver configuration file

- /etc/resolv.conf
  - nameserver *IP* IP address of name server
  - domain *domainname* local domain name
  - search *list* search list for host-name lookup. each doma separates by space or tab
  - options *option…*
    - timeout:n wait response from name server for n second
    - attempts:n number of times the resolver will send a quer to a name server before giving up
    - rotate causes round robin selection of nameservers fron among those listed

Network fault isolation

TCP/IP networking 14

System databases and Name Service switch configuration file /etc/nsswitch.conf

File format:

Database: source [Status=Action] …

- **source**
  - **dns**
  - **nis**
  - **nisplus**
  - **file**
  - **…**

Network fault isolation

TCP/IP networking 15

- **Status**

success	**request entry was found**
unavail	**source is not responding or corrupted**
notfound	**source responded “no such entry”**
tryagain	**source was busy, might respond to retries**

Network fault isolation

TCP/IP networking 16

- **Action**

  continue **try the next entry in the list. Default for any status except SUCCESS**

  return **return now**

Protocol definition file

TCP/IP networking 17

/etc/protocols file format

protocol number aliases …

protocol native name for the protocol

number the official number for this protocol

aliases optional aliases for the protocol

Internet service list

TCP/IP networking 18

/etc/services file format

service-name port/protocol [aliases …]

service-name friendly name the service is known

port port number to use for the service

protocol type of protocol to be used

aliases optional

Identify installed packages

Manage system software 1

- RPM - an individual Red Hat package
- List installed packages

rpm -qa

- Find package

yum search *keyword*

- List available and installed packages

yum list

Install, Remove, and update packages(Patch)

Manage system software 2

- Install package

yum install pakage…

- Remove package

yum remove package…

- Update packages(patch)

yum update

Install & Configure a VNC server

Install & configure service 1

- Install tigervnc-server
- Copy config file

cp /lib/systemd/system/vncserver@.service /etc/systemd/system/vncserver@:1.service

- Edit /etc/systemd/system/vncserver@:1.service change <USER> to username
  - ExecStart=/sbin/runuser –l <USER> -c "/usr/bin/vncserver %i"
  - PIDFile=/home/<USER>/.vnc/%H%i.pid
- Reload system for changes

systemctl daemon-reload

Configuring a VNC server

Install & configure service 2

- Start service

systemctl start vncserver@:1.service

- Allow VNC service in firewall

firewall-cmd –permanent –add-service vnc-server

firewall-cmd –permanent –add-port=5901/tcp

firewall-cmd --reload

systemctl restart firewalld.service

- Enable service at startup

systemctl enable vncserver@:1.service

Secure Access to a Remote GNOME Desktop

Install & configure service 3

- Set VNC password for user who is allowed to login via vncviewer

su – username

vncpasswd

- Connect to a VNC server using ssh tunnel

vncviewer –via *user@host vncserver:display*

Install & Configure a VNC server-Rocky9

- Install tigervnc-server

dnf install tigervnc-server

- Set vnc password for each user

vncpasswd

Install & Configure a VNC server-Rocky9

- Edit /etc/tigervnc/vncserver.users add a line display N for user username

:N=username

Ex.

:1=root

:2=tom

…

5901 port for root，5902 port for tom…

Configuring a VNC server-Rocky9

- Add the following line to bottom of /etc/tigervnc/vncserver-config-defaults

alwaysshared

- Edit /etc/gdm/custom.conf

[xdmcp]

Enable=1

- Enable and start service for each user

systemctl daemon-reload

systemctl enable vncserver@:1.service

systemctl start vncserver@:1.service

systemctl enable vncserver@:2.service

systemctl start vncserver@:2.service

Configuring a VNC server-Rocky9

- Allow VNC service in firewall

firewall-cmd –permanent --add-service vnc-server

firewall-cmd --permanent --zone=public --add-port=5901/tcp

firewall-cmd --permanent --zone=public -add-port=5902/tcp --accept

firewall-cmd --reload

systemctl restart firewalld.service

- reboot system

init 6

Secure Access to a Remote GNOME Desktop- Rocky9

- Install vncviewer

sudo dnf install tigervnc

- Connect to a VNC server using ssh tunnel

vncviewer –via *user@host vncserver:display*

NFS Server

Network File System *1*

- Start NFS server service

systemctl start rpcbind nfs-server

- Export filesystem

exportfs –o option client:/path

- Allow NFS service

firewall-cmd --add-service=nfs --permanent

Firewall-cmd --reload

NFS server

Network File System *2*

- Share next boot

Edit /etc/exports

/filesystem client_ip(options)

  - Options

  rw

  ro

  no_root_squash

- Start NFS service at boot

systemctl enable rpcbind nfs-server

NFS client

- Identify the remote share

showmount –e

- Determine mount point
  - If the mount point does not exist

mkdir /path-of-mount-point

- Mount the network file system

mount host:/NFS-path /path-of-mount-point

NFS Server-

Network File System1-Rocky9

- Install packages

sudo dnf install nfs-utils rpcbind

- Start NFS server service

systemctl start nfs-server.service

- Start NFS service at boot

systemctl enable nfs-server.service

NFS Server-

Network File System 2-Rocky9

- Export filesystem

exportfs –o option client:/path

- Allow NFS service

firewall-cmd --add-service=nfs --permanent

firewall-cmd --add-service= mountd --permanent

firewall-cmd --reload

NFS server

Network File System3- Rocky9

- Share next boot

Edit /etc/exports

/filesystem client_ip(options)

- Options

rw

ro

no_root_squash

NFS client

Network File System 4- Rocky9

- Determine mount point
  - If the mount point does not exist

mkdir /path-of-mount-point

- Mount the network file system

mount host:/NFS-path /path-of-mount-point

Analyzing and storing Logs

syslog & logfiles 1

Section 1 – Determine Log Destinations

- Many programs use a standard protocol to send messages to rsyslogd
- Each messages is desribed by a facility(type of message) and a severity(how important)
- /etc/rsyslog.conf file uses the facility and serverity of the log message to determine where it gets stored in

Rsyslogd configuration file

syslog & logfiles 2

/etc/rsyslog.conf

selector action

- **selector**

  facility.level

  - **facility**
    - **auth, authpriv, cron, daemon, kern, lpr, mail, mark, news, syslog , user, uucp, local0~7**
    - *** all facility**
  - **level**
    - **emerg, alert, crit, err, warning, notice, info, debug**
    - **none used to diable a particular facility**
    - *** all levels**

Rsyslogd configuration file

syslog & logfiles 3

action

- Filename must be full path
- | pipefile logging to a named pipe
- Terminal must be /dev/console or tty
- @hostname
- @ipaddr messages are forwarded to the syslogd on the named host
- :omusrmsg:user1,user2,... message written to the terminals of users
- :omusrmsg:* message written to the terminals of all logged-in users

Rsyslogd

syslog & logfiles 4

- Start rsyslogd to receive remote messages

systemctl start rsyslog.service

- start rsyslog service at boot

systemctl enable rsyslog.service

- Restart rsyslogd

systemctl restart rsyslog.server

kill -1 $(cat /var/run/syslogd.pid)

kill -HUP $(cat /var/run/rsyslogd.pid)

Log server

- Act as log server
  - Edit /etc/rsyslog.conf
  - UDP
    - $ModLoad imudp
    - $UDPServerRun 514
  - TCP
    - $ModLoad imtcp
    - $InputTCPServerRun 514

Make entries in the system log

syslog & logfiles 6

logger [-p pri] [message…]

- -p pri enter the message with the specified priority
- message message to log

Log server-1

rocky9

- Act as log server
  - Edit /etc/rsyslog.conf
  - UDP
    - $ModLoad imudp
    - $UDPServerRun 514
  - TCP
    - $ModLoad imtcp
    - $InputTCPServerRun 514

Log server-2

rocky9

- Start rsyslogd to receive remote messages

```
systemctl start rsyslog.service
```

- start rsyslog service at boot

```
systemctl enable rsyslog.service
```

- Restart rsyslogd

```
systemctl restart rsyslog.server
```

- Allow syslog service in firewall

```
sudo firewall-cmd –permanent --add-port=514/tcp
sudo firewall-cmd –permanent --reload
```

Log client-1

rocky9

- Edit /etc/rsyslog.conf and append the following line

action(Type="omfwd" Target="server ip" Port="514" Protocol="tcp")

Log client-2

rocky9

- Start rsyslogd to reload new config

systemctl restart rsyslog.service

Logging policies

- Logs are "rotated" to keep them from filling up the file system containing /var/log
- when a log file is rotated, it is renamed with an extension indicating the date on which it was rotated. Ex. /var/log/messages-20120523
- Once the old log file is rotated, a new log file is created and the service that writes to it is notified
- After a certain number of rotations(typically after four weeks), the old log file is discarded to conserve disk space
- A cron job runs the logrotate program daily to see if any logs need to be rotated
- Most log files are rotated weekly, but logrotate rotates some faster, or slower, or when they reach a certain size

Locate and analyze a log summary report

- Install logwatch pacakge
- logwatch runs daily to generate report
- Report is e-mailed to the local root account
- Copy /usr/share/logwatch/default.conf/logwatch.conf /etc/logwatch/conf/logwatch.conf
- Change email address (/etc/logwatch/conf/logwatch.conf)
  - MailTo = user@where
- Run daily
  - /etc/cron.daily/0logwatch

Three kinds of Job scheduling

- Every day at specific time(cron)

crontab [-u user] file

crontab [-u user] [-e| -l | -r]

- -u user specify the user whose contab is to be tweaked
- -e edit crontab file
- –l list crontab file
- -r remove crontab file

Crontab file format

minutes hours day-of-month month weekday command

• name	SHELL, PATH, MAILTO
• minutes	0-59
• hours	0-23
• day-of-month	1-31
• month	1-12
• weekday	0-6