

Linux Torvalds

Finnish college - Project 1991

operating system
software hardware

Linux
Symbol - Penguin
GPL license - freedom to use

change
share

Linux Foundation

Collaborative Project
Event

Context / Update & Maintenance

Developer → Patches → Senior Linux kernel developer / maintainer → Linux creator

Terminology

Kernel - interact - hardware application

Distribution / Distros - Linux kernel + collection of program

Boot loader - program → OS
• GRUB
• ISO LINUX

Service - Program → background process
httpd, nfsd, ntpd, ftpd & named

Filesystem - Method for storing & organizing files
ext3 FAT XFS NTFS Btrfs
ext4

X-window system - standard toolkit & protocol for Graphical User Interface (GUI)

Desktop environment - GNOME, KDE, Xfce & fluxbox

Command Line - Interface for typing command

Shell - Command Line Interpreter
bash, tsh, zsh

Boot Process - initialize system

Power-On

BIOS - Basic Input Output System (BIOS)
Software on ROM chip → Motherboard
initialize hardware - screen, keyboard } Power on self test (POST)
test main memory

Master Boot Record (MBR)
first sector of hard disk

Stored hard disk

Traditional boot sector - BIOS/MBR systems
first sector of hard disk (MBR)
512 bytes

examine partition table → bootable partition
boot loader → RAM
GRUB

Boot loader

1st stage
2nd stage

UEFI Partition
Variable Unified Extension Firmware Interface

Boot manager data (which data partition → UEFI application launch GRUB firmware boot manager)

Linux Kernel - RAM

initialize & configure

memory

hardware attached

all processor

subsystems

storage

Initial RAM Disk - RAM

initramfs file system image

program binary files

mount proper root filesystem

kernel functionality

file system

device drivers

facility -udev

user device

mass storage controller

which device is present

locate & load driver

/sbin/init & Services

execute init program

/sbin/init

mounting & final root file system

OS

file system ready-use

associate - mount point

check error

mount

initramfs - clear from RAM

initial process → other process - to get system running

manage internal OS details / manager for run kernel process

run & shut down → system

1980 System V Variety of UNIX - SysVinit
Serial process sequence of run levels - scripts - start stop

Upstart - Ubuntu 2006

systemd - Fedora 2011

parallelization
large computer - rarely shut down

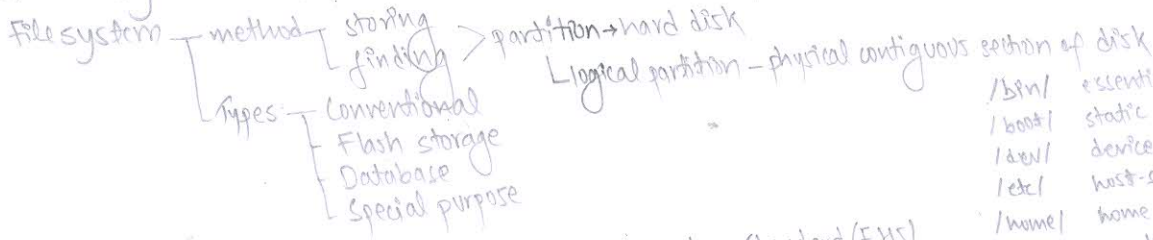
default
bash (GNU Bourne Again Shell)

text prompt

Command line operation - terminal that run command shells

GUI

Linux Filesystem Basics



Linux Foundation

Standard Layout - Filesystem Hierarchy Standard (FHS)

mount ← single filesystem → multiple partitions

Graphical Interface for filesystem

Linux Distribution

- Server
- Desktop
- Embedded

/bin/ essential user command binaries

/boot/ static files of boot loader

/dev/ device files

/etc/ host-specific system configuration

/home/ home user directories

/lib/ essential shared libraries & kernel

/media/ mount - removable media

/mnt/ mount - temp mounted filesystem

/opt/ add-on software package

/sbin/ system binaries

/srv/ data for services provided by system

/tmp/ temporary files

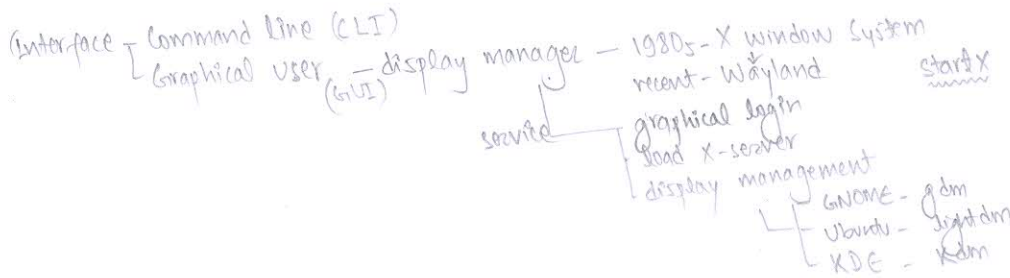
/usr/ user utilities & applications

/var/ variable files

/root/ home directory for root user

/proc/ virtual filesystem documenting kernel and process status as text files

GRAPHICAL INTERFACE



Desktop Environment

- session manager - graphical session
- window manager
- other utilities

setting

- background
- theme
- gnome-tweak-tool

Start

Maintain

Session Management

- Logging in
- locking screen
- Switching Users
- Suspend/Sleep
- Restart/shut down

Basic Operation

- Application Locate → open
- File manager utility - nautilus
- Edit file
- Delete file
- local/share/trash/files
- permanent shift + Delete

Search Ctrl-F

Locate Ctrl-L

hidden Ctrl-H (*)

SYSTEM CONFIGURATION - GRAPHICAL INTERFACE

System - system setting panel ← GNOME desktop manager

Display

- resolution
- multiple screen - one big screen
- minor display

gnome-tweak

Date & Time

- default - internal time keeping
- Internet - Network
- Co-ordinated Universal Time (UTC)
- Greenwich Mean Time (GMT)
- Network Time Protocol

Network Manager - Network configuration file

- Wired
 - Dynamic Host Configuration Protocol (DHCP)
 - static connection ← ethernet
- wireless
- Mobile Broadband Network
- Virtual Private Network

network card → Unique hexadecimal no.

Installing & Updating Software

package - one piece of system

interdependencies

utility

- low level - unpack a package → place
- high level - download & manage interdependencies

Debian dpkg

Red Hat Family RPM (Red Hat package manager)

yum, dnf, zypper

advanced package tool

GNUP Network Object Model Environment (GNOME) - PackageKit

yellowdog updater modified

Command line operation

dpkg

- list
- info
- remove

apt

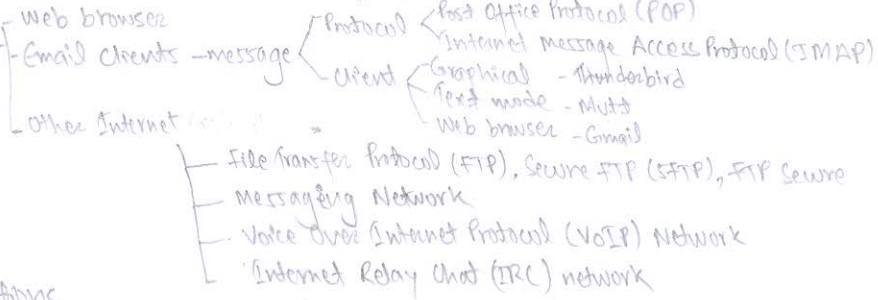
- cache
- get
- install
- remove

clear

COMMON APPLICATIONS

Internet Application

Global network - application



Productivity & Development Applications

Office Applications/Suiter

- Word Processing - Writer
- Spreadsheet - Calc
- Presentations - Impress
- Graphical Obj - Draw

Development Application

- Advanced Editor - vi, emacs
- Compiler - gcc
- Debugger - gdb, valgrind
- Complete Integrated Development Environment (IDE) - Eclipse

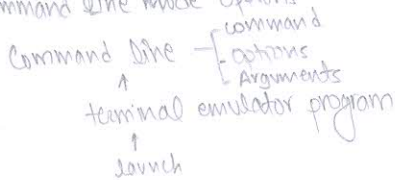
Multimedia Applications

- Sound Players
- Movie Players
- Movie Editor

Graphics Editors & Utilities

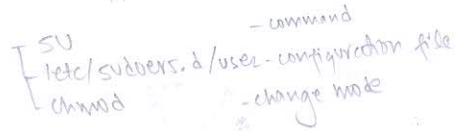
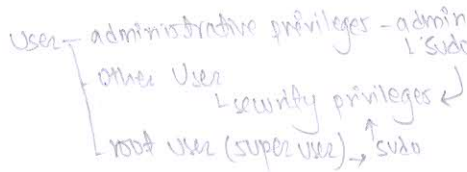
- GNU Image Manipulation Program (GIMP)
- Graphic Utilities

Command Line Mode Options



COMMAND LINE OPERATIONS

GUI makes easy tasks easier while command line interfaces makes difficult tasks possible



CTRL-ALT-funknkey

Virtual Terminals

Provide session users display & keyboard outside a graphical environment

many active terminal, only one terminal remains visible

Graphical Desktop

- start
- stop
- telinit
- systemctl

Basic Operation

- log in/out - login
- shutdown - remote system - Secure shell utility (SSH)
- shutdown -h halt
- shutdown -r restart
- Application
 - executable - program
 - script - /bin /opt /sbin
 - locate - which
 - whereis

Accessing Directories

- pwd - present working directory
- cd - change directory
- cd .. - parent directory
- cd - - previous directory

Path

- absolute - /
- relative - ./

Explore Filesystem

- ls - list contents
- ls -a - all
- tree - tree view

Links

- hard link ln
- Symbolic link ln -s

ls -li

- inode number - unique quantity for each file
- hard link - same
- soft link - pointer

Navigating directory history

- cd -
- pushd
- popd

Working with files

- view
- cat
- tac
- less
- head
- tail

touch

- creates/update
- t set

- access
- time
- change
- modify

- mv - move/rename
- rm - remove
- f forcefully
- i interactively

cp copy

Directory

- make - mkdir
- remove - rmdir
- rm -rf

Common Line Prompt

\$PS1

Searching for files

Standard file streams/descriptors

Always open for use

- stdin 0
- stdout 1
- stderr 2
- < input
- > output
- >> error file

I/O Redirection

Pipes

! output - input

Searching

- locate
- find
- database of files & directories
- filesystem tree
- all current dir & sub-dir
- name: certain pattern
- iname " " + ignore case
- type type d - directory l - symbolic link f - regular file
- exec run command { } ;
- ok
- placeholder

wildcard & matching file names

- time
- ctime last change
- atime last accessed
- mtime last modified
- n # of days
- n <

Size

- size
- c - bytes
- k - kilobytes
- m - megabytes
- G - gigabytes

Match

- ? any single char
- * any string of char
- [] any given set of char
- [] " " " " " " not negation

FINDING LINUX DOCUMENTATION

Linux Documentation Sources

man page / Manual page

1970 UNIX

Linux man page

man -f all pages on topic
-k all pages discussed
-a page info/chapter

GNU Info

GNU project's standard documentation info

help command

--help

Other documentation

Desktop help system
Package documentation
Online resources

Processes & Process Attributes

PROCESSES

Command Program

Operating system (OS)
Interactive environment
background

Kernel

allocate

System Resources

memory

cpu cycles

Instance

Threads

Processor

Type

Processor states

Running

Waiting

Sleep

Zombie

time slice

user/action

Process Scheduling

Kernel

Scheduler

Process

on/off CPU

time

needed

share

priority

Process IDs

OS - track process

unique Process ID (PID)

Parent Process ID (PPID)

Thread ID (TID) - One process can have many threads

User & Group IDs

many users -> system

user start - Real User ID (RUID)

" determine access rights - Effective UID (EUID)

terminate

Kill - SIGKILL <pid>

Kill -9 <pid>

Priorities

cpu - one task at a time

Linux value (-20 to 19)

lower the value - higher the priority

group - RGID

-EGID

Process Metrics & Process Control

Load Average - avg of the load number / period of time

actively running CPU

runnable but waiting for CPU

sleeping & waiting resource - uninterruptible sleepers

Managing Jobs

command -> jobs

Listing Processes

ps - information currently running processes keyed by PID

style - System V style

BSD style - option without preceding dashes

ps -u username

-ef - all process with full detail

ps aux

process tree - pstree

top - interactive keys for monitoring

Starting processes in future

at - non interactive command at a specified time

cron - time based scheduling program

by system - crontab file - cron expression

configuration file - /etc/crontab -> crontab -e

MIN HOUR DOM MON DOW CMD

sleep - delay

s, m, h, d

Background & Foreground Processes

w

top

uptime

free shell for other tasks

lower priority

suffix &

bg

launched from terminal / shell

& wait till complete

ctrl-z suspend

ctrl-c terminate

live update

top

htop

atop

cpu cycle

memory

1. system up, # users, load average
2. processor - running, sleeping, stopped, zombie
3. %CPU time user (us), kernel (sy), idle mode (id), jobs waiting (wa)
4. memory - hardware (hi), software (si), steal time (st), LVM
5. PID - process identification number
- USER - process owner
- PR (Priority) & nice value (NI)
- virtual (VIRT), physical (RES) & shared (SHR)
- STATUS (S)
- %CPU & %MEM
- TIME + Command

File System

Hierarchical file system - root/trunk

File Operations

user
system
devices

Many filesystem varieties

Partition - organize files

Mount points → attach ← file system

df -lh

mount

umount

automatically
/etc/fstab

file system table

NFS & Network filesystem

Data - Physical System

1 machine

> 1 machine

same location

other location - Internet

Type

NFS - Network filesystem - Sun Microsystems

CIFS/SAMBA -

- Microsoft

NFS

Server

- daemons

sudo

systemctl

start nfs

restart

enable

Client

sudo mount

/etc/fstab

/etc/exports - config

- configuration - automatically upon system boot

File Architecture

- /root

/home

user/group

- /bin

/usr/bin

executable binaries with essential commands

- /sbin

pseudo file system

virtual

files

directories

→ mimic

kernel structure

- /proc

runtime system information

configuration info

system memory

device mounted

hardware configuration

- /dev

device nodes - pseudo file

not mounted - empty on disk partition

mounted - creates & manage device nodes

- /var

variable directory Δ - size as the system is running

log, print queue, package & database file, temp file

- /etc

system configuration files, executable scripts

- /boot

files to boot the system

Each kernel

- vmlinuz

- compressed linux kernel

- initramfs

- initial ram filesystem

- config

- kernel configuration file

- System.map

- kernel symbol table

- /lib

/lib64

library to run essential program

- /run

/media

/mnt

removable media

- /opt

optional application software package

- /sys

virtual pseudo-filesystem

information - system

hardware

- /srv

site specific data

- /tmp

temporary files

- /user

multiuser application

Comparing files & filetypes

diff compare two files/directory

diff3 compare three " "

patch apply patch

file categorize file type (& extension)

Backup & Compress Data

Backup

copy cp

sync

rsync

- efficient & robust

Compress

gzip, bzip2, xz

- linux

- across OS

zip

tar

- group & compress

stage archive

Disk to disk copy

dd

- copy raw disk space

Text Editors

Basic Text Editors

nano
gedit ← Graphical desktop environment

Create file without an editor

echo
cat << EOF

> output to file
>> append

Advanced Text Editors

vim
gvim ← GNOME
vim tutor - tutorial
emacs
!mode
- ctrl
meta(ALT, Esc) > special command

- working mode
 - command
 - insert
 - line
- cursor position
- search
- external command

User Environment

Accounts, Users & Groups

Current User whoami, who

User Startup files - configure user environment

/etc/profile
~/.bash.profile
~/.bash_login
~/.profile

~/.bashrc - alias - customized commands

Users & Groups

User - Unique User ID (UID)

Group - Group

(GID)

group - shared permission

access
privileges
security

Adding & Removing

User
id
useradd
userdel

New group
groups
groupadd
groupdel

Existing group
usermod
groupmod

Account

Root/administrator/superuser

Elevated privileges

- su (switch/substitute user)
- sudo
temporary
specific command
assign

sudo configuration files
/etc/sudoers
/etc/sudoers.d

Environment Variables (EV)

specific value → utilized by command shell
default
overwritten
- view
- set
- env
- export

Variable

HOME pwd - present working directory
cd - current directory
PATH list of directory scanned for program or script
separated by :
current directory - ./ or ../
SHELL user's default command shell
PS1 prompt statement variable

Setting EV
echo \$HOME
export (~/bashrc)

Recalling Previous Command

bash - previous command statement → history buffer → ~/.bash-history

Finding & using
↑ ↓
!! - Recall previous command
Ctrl+R - search previously used command

executing
! - start history substitution
!\$ - last line with
!string - most recent command starting with

Environment variable
HISTFILE
HISTFILESIZE
HISTSIZE
HISTCONTROL
HISTIGNORE

Keyboard Shortcuts

File Permission

owner - chown
group - chgrp
other

read/write/execute
4 2 1
chmod owner:group:other

Manipulating text

Command line tools for manipulating text files

Linux system administrator → developer → user

browse → parse → extract → text files

file manipulation process

- concatenate view
- display
- cat
- tac
- interactively
- echo
- > create + add
- >> append
- CTRL+D
- cat > <filename> (CTRL+D)
- cat > <filename> <<EOF
- EOF/STOP

working with large & compressed files

- less
- head -n
- tail -n -f
- zcat
- zless
- zmore
- zgrep
- zdiff

Repeatedly edit/extract contents from a file

sed

- stream editor
- UNIX
- input stream → working stream → output stream
- awk - Bell Labs
- awk -f scriptfile file
- awk -F ' ' file
- field separator
- command
- sed s/pattern/replace-string/g file
- substitute
- global
- edit
- apply from script

File manipulation Utilities

- sort
- uniq
- c - count
- paste
- join
- split
- wc
- word count
- Regular Expression & search pattern
- character
- normal
- meta- . | \$ ^ *
- grep - text searching tool
- strings
- extract printable character strings in files
- human readable content embedded in binary files

Miscellaneous Text Utilities

- translate
- tr [options] set1 [set2]
- tee
- stdout
- standard output
- saves to file
- wc
- word count
- cut
- extract specific column - column based file

Network Operations

Introduction to Network

Network - group of computer devices

Internet - the network of networks

connected - communication channels

- cable
- wireless media
- uses
- communicate
- share devices over network
- share & manage information

IP Addresses

Network - unique network address identifies

IP (Internet Protocol) address - network

- routing packets of information
- exchange information - streams of small packets
- data buffer
- source
- destination
- header

IP address allocation

network admin

range of IP address

Internet Service Provider (ISP)

choose

assign

- static - manual
- dynamic - Dynamic host configuration protocol

IPV4 - version 4, 32 bit

4 x 8 bit octets

5 Classes

- A - Network ID - 1, Host ID - 2, 3, 4
- B - Net ID - 1, 2, Host ID - 3, 4
- C - Net ID - 1, 2, 3, Host ID - 4
- D - multicast address
- E - reserved for future use

limitation - # of unique address

IPV6 - version 6, 128 bit

Network Address Translation (NAT)

1 IP shared among many locally connected computers

Name resolution

ID address

human readable format

hostname

translate

Domain Name System (DNS)

Network Configuration & Tools

- /etc
- Network manager
- Graphical system administrator

Network interface

- device
- connection
- network
- physical - Network Interface Card (NIC)
- ping
- machine
- receive
- send
- data in network
- host is responding

Browsers, wget & curl

Browser

- Graphical
- Non-Graphical

wget - download files & information

- large file
- recursive file
- password-require downloads
- multiple file downloads

curl - information about URL

route

- source - data
- nodes
- multiple network
- destination
- server
- routing tables - address of each node - network
- IP routing protocols - forwarding table
- route, ip route

traceroute

- inspect route
- troubleshoot network delays & errors

Networking tools - ethtool, netstat, ...

Transferring Files

File transfer protocol (FTP)

- transfer file
- network
- Internet
- Use
- browser
- stand alone client
- Client-server model
- FTP client
- graphical
- command line tool
- ftp
- sftp
- ncftp
- yafp
- 1970s
- user credential
- password
- encrypted
- rsync
- secure shell protocol (ssh)
- cryptographic network protocol
- secure copy (scp)

Bash Shell and Basic Scripting

Features & Capabilities

Shell Scripting

- automate long & repetitive command
- share process among user
- quick prototyping & compile new commands & utilities

script → Interpreter → Command Shell

Choice - sh, bash, tch, csh, ksh, zsh

Command Line Interpreter

terminal window - run script (user interface) → interactive session / non-interactive

can take user input

Syntax

Basic syntax & special character

- Split long commands over multiple lines - \ (concatenation operator)
- Putting multiple command in a single line
- execute sequentially ;
- abort when fail &&
- proceed until success ||

Output Redirection write output > append output >>

Input Redirection input <

comment #

Built-in Shell Commands

- compiled application - rm, ls, df, vi, gzip
- Built-in bash commands - cd, pwd, echo, read, help
- shell scripts - script parameters

- \$0 - script name
- \$n - nth parameter
- \$* - all parameters
- ## - number of argument

Command Substitution \$()

Environment Variables \$ env, set, printenv, export

Functions sub-routines Declare - function name() { command }

Constructs

if statement if condition; then statement; else statement

Boolean Expression && and multiple condition || or → proceed ! not

Arithmetic Expression expr \$(...) let

String Manipulation

[[string1 == string2]] - compare \$? # string string0:n

Case Statement

case expression in pattern1) execute command;; pattern2) execute command;; *) execute default command esac

Looping Constructs

for var-name in list do command while condition is true do command until condition is false done

Script Debugging

debug mode - bash -x ./script-file bracketing pairs set -x set +x redirecting errors stdin -0 stdout -1 stderr -2

Useful Techniques

Creating temporary files & Directory - mktemp Discarding Output - /dev/null bid bucket Random number & data - RANDOM black hole

① Special hardware number generators

noise signal → thermal noise → transducer → electric signal → A/D converter → digital signal → random ← digital number → entropy pool of random bits → /dev/random - quality → /dev/urandom - faster

② boot → event

Local Security Principles

Understanding Linux Security

User account → database → User ID (UID) | useradd
Group ID (GID) | userdel

Types of account

- root
- system
- Normal
- Network

- Set owner User ID (SUID)

sudo vs su

- configuration - /etc/sudoers
- command logging - /var/log/sure

last - last time each user
logged in the system

Process Isolation & resources

- control groups (cgroups)
- container
- virtualization

Hardware Device Access
Keeping current

Passwords

stored - /etc/shadow - encrypted

SHA-512 (Secure Hashing Algorithm 512 bits) ← US National Security Agency (NSA)

Practice

- Password aging - change
- Pluggable Authentication Modules (PAM)
- password cracking programs

Securing the boot process & hardware resources

Requiring boot loader password

Hardware Vulnerability

- key logging
- Network sniffing
- Booting with live or rescue disk
- Remounting & modifying disk content

Software Vulnerability