IT2654

System Administration & Security

Topic 1: Introduction to Linux

Objectives

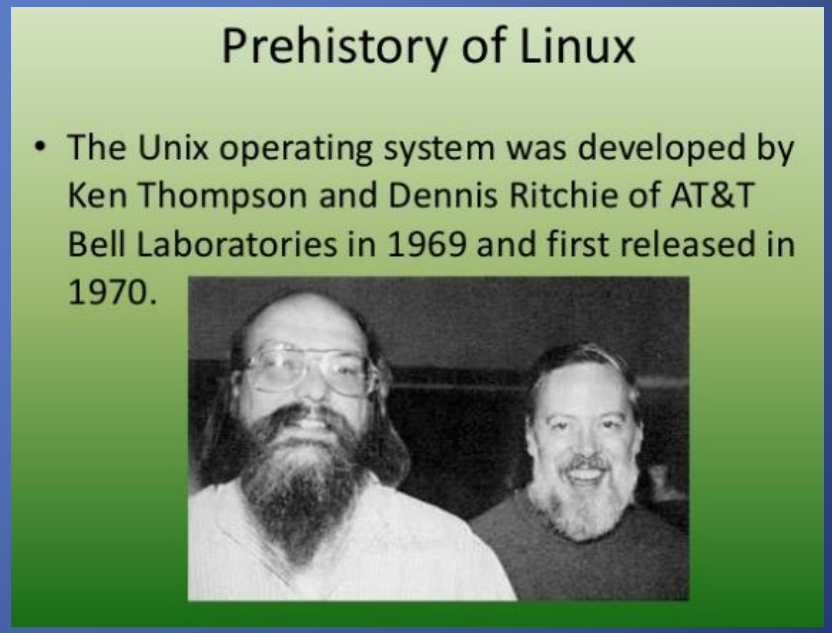
- Introduction to Linux
- Familiarization of Desktop
- Getting Help
- Disk Management
- File Management
- Basic Linux Commands

Unix

- Unix is a portable, multi-user, multi-tasking operating system.
- You can have many users logged into a system simultaneously, each running many programs.
- It's the kernel's job to keep each process and user separate and to regulate access to system hardware, including cpu, memory, disk and other I/O devices.
- Written in C language; portable to different hardware platforms.
- Unix customers include – HP (HP-UX), IBM (AIX), Oracle (Solaris), Microsoft (Xenix), Apple (MacOS), Berkeley (BSD)
- Used mainly for internet servers, workstations, mainframes

History of Unix

- First Version was created in Bell Labs in 1969.
- Some of the Bell Labs programmers who had worked on this project, Ken Thompson, Dennis Ritchie, Rudd Canaday, and Doug McIlroy designed and implemented the first version of the Unix File System on a PDP-7 along with a few utilities. It was given the name UNIX by Brian Kernighan.



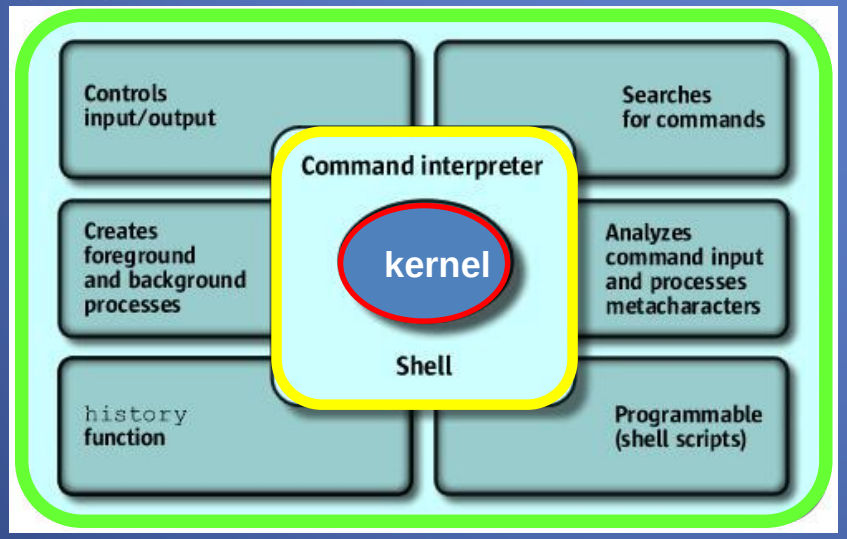
What is Linux?

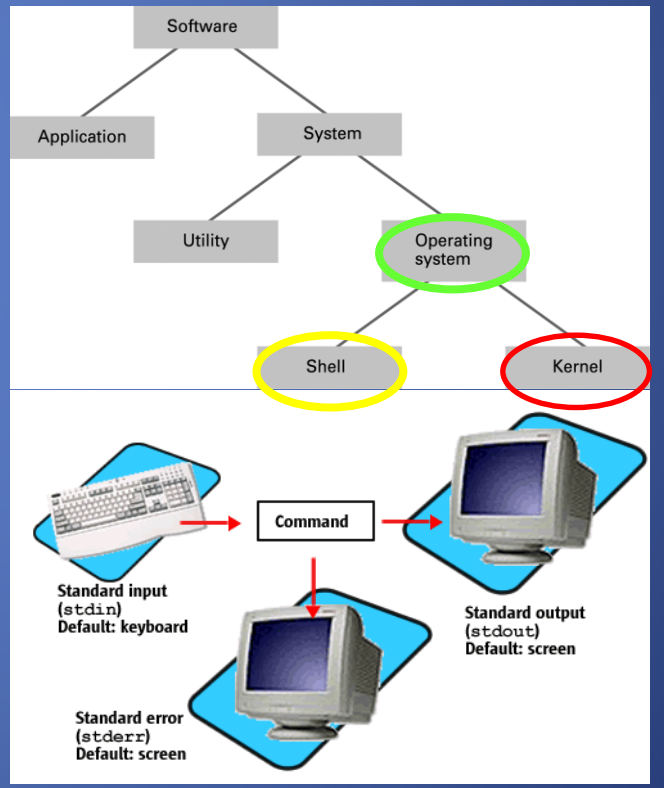
- A clone of Unix – portable, multi-user, multi-tasking
- Developed in 1991 by Linus Torvalds, a Finnish graduate student
- Open source
- Consist of
  - Linux Kernel
  - GNU (GNU is Not Unix) Software
  - Others

- Torvalds made the code of Linux freely available to everyone on the internet, and therefore lots of people created their own versions of Linux.

OS = Kernel + Shell

- Kernel (engine)
  - Vital/core system software (protected, not accessible to normal users)
  - Loaded first to run when computer starts up.
- Shell
  - Command Line Interpreter/Interface (CLI)
  -

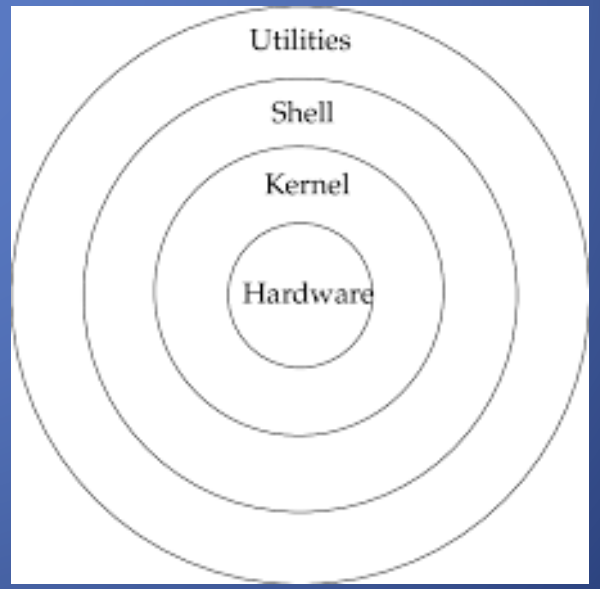




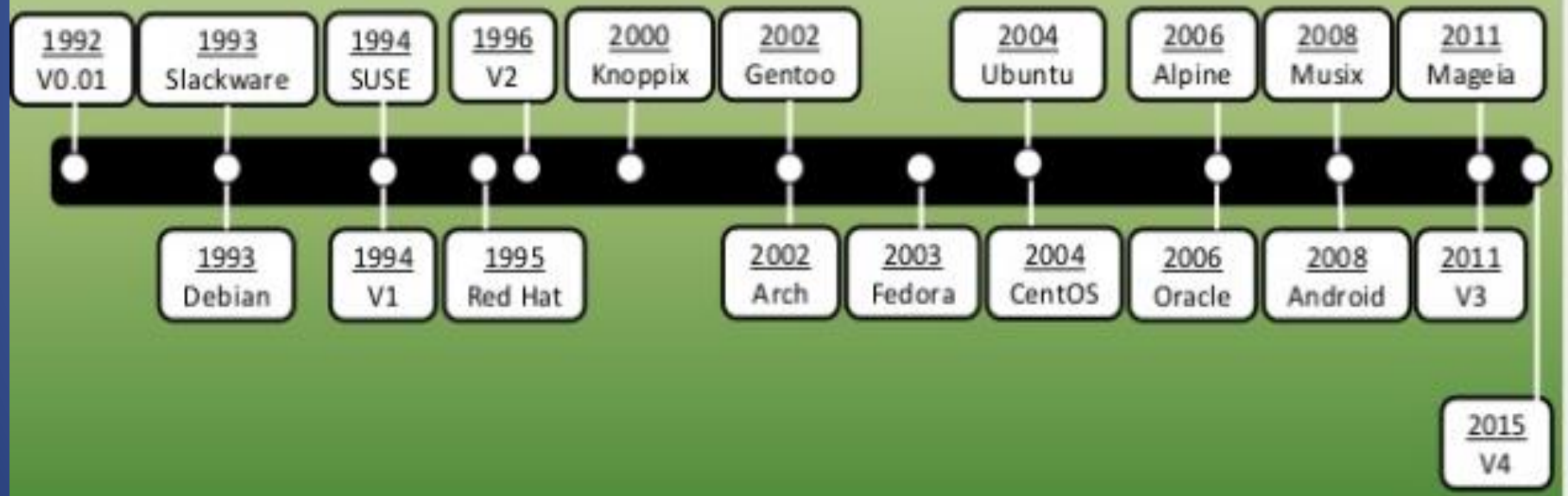
The Kernel

- The operating system software file (program) which is copied into RAM, usually from the hard disk drive, during the boot-up.
- The kernel remains in RAM while the computer is on and is in charge of the overall operation of the computer system.
- The kernel contains the “internal programs” for the most often used operations like copying files.

- kmem (Linux)
- command.exe (Microsoft)



Timeline of Linux



Distro Landscape

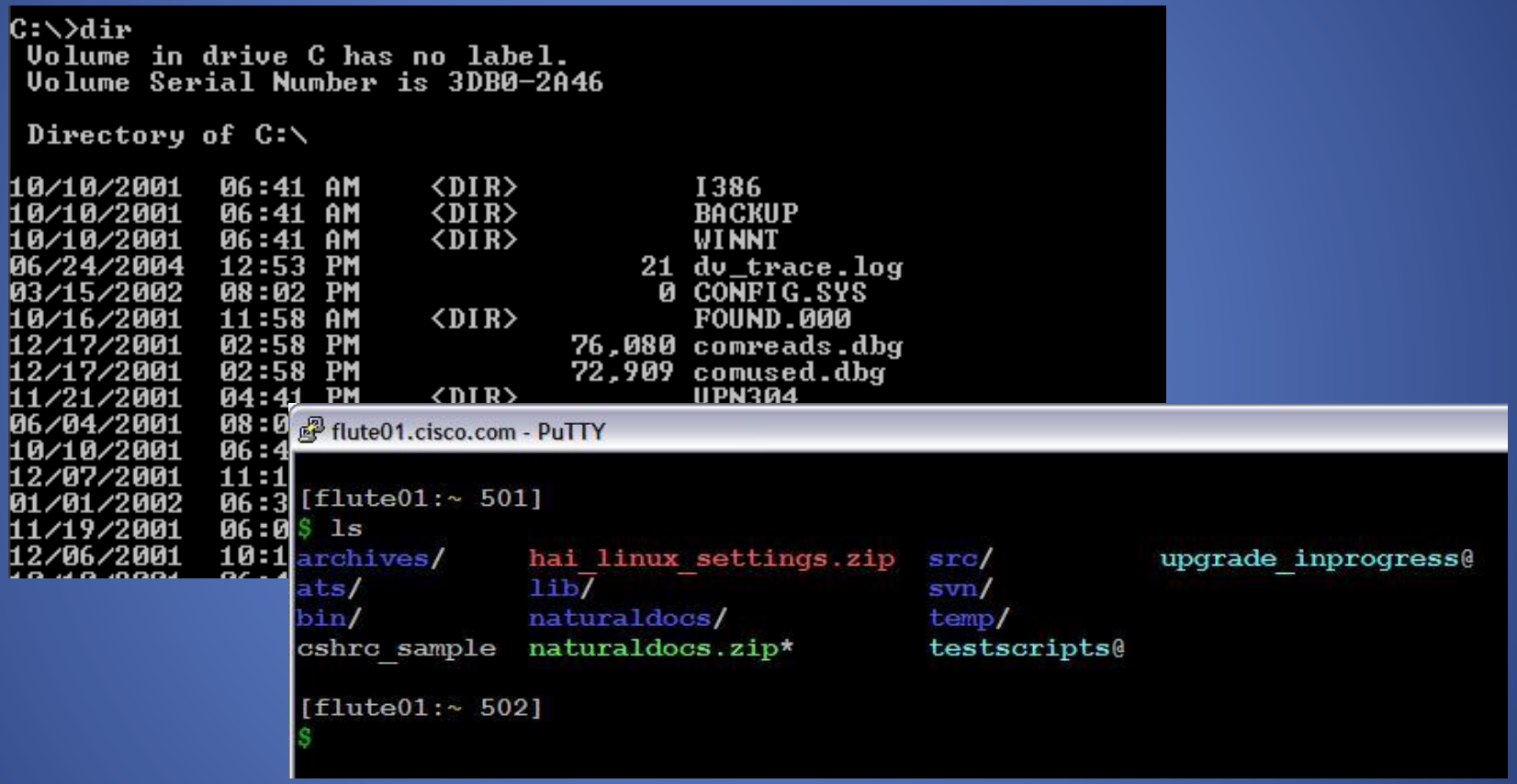
Log in — Super User

- This is the administrative account.
- Most powerful account.
- Has complete control over the host.
- Usually has a default name of **root**
- Do not confuse it with the root directory!
  - **$** prompt → normal user
  - **#** prompt → super user

GNOME

- *GNU Network Object Model Environment*
- Desktop GUI for linux systems
- Within GNOME, we can also have pseudo text consoles.
- These are activated by:-
  - Applications-> System Tools ->Terminal
  - Right-click on desktop -> Open in Terminal

Command Line Interface (CLI)



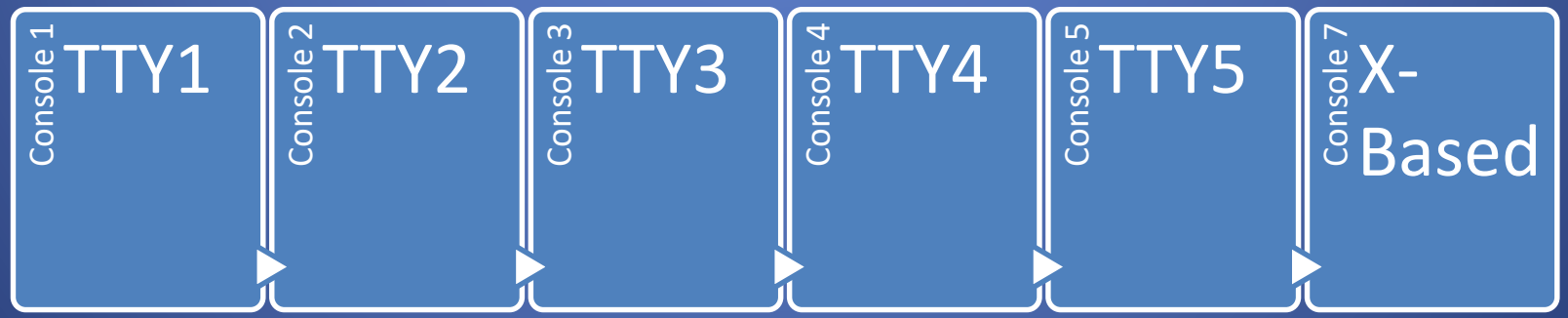
CLI will refer to the terminal window or console

CLI Syntax

- On the CLI, the standard syntax is as follows:-
  - ***command option(s) argument(s)***
- Each item must be separated by one or more spaces.
- Linux commands are **CASE SENSITIVE** eg. pwd <> PWD
- Options modify command behaviour
  - single letter options usually preceded by **-**
    - ***-a -l or -al***
  - Full word options preceded by **--**
    - Example **--help**
- Arguments are file names or data needed by the command
- Multiple commands can be separated by ***;***
- Typically, successful commands do not give any output
- Messages are displayed in the case of errors

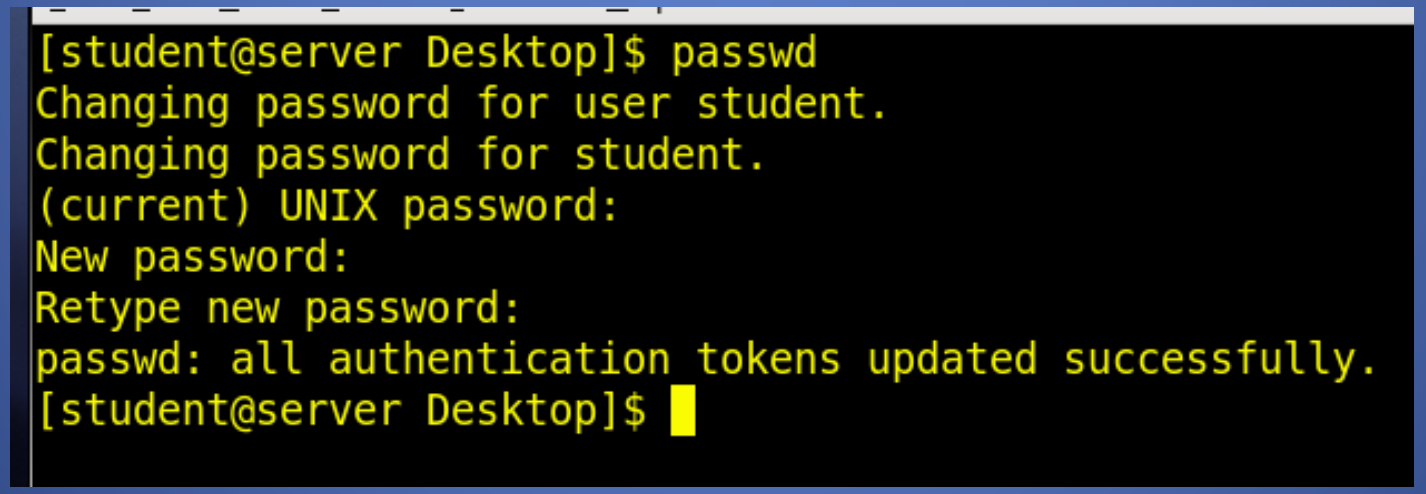
Virtual Consoles

- There are 6 virtual consoles a.k.a. virtual machines.
- 5 of them are text-based consoles, one is GUI X-based
- Command is change between them is :-
  - CTRL-ATL F[1 to 6]
- tty – determine terminal type



Passwords

- Can be accessed from:-
  - GUI: System->Preferences->About Me->Change Password
  - CLI: ***passwd***



**** CLI -> Command Line Interface (terminal window)***

Changing Identities

- Must be done on the CLI.
- 2 ways to do so:-
  - ***su –*** creates a new shell as the root user
  - ***sudo*** command runs commands as the root user
    - need to be configured via sudoers
- the ***id*** command can be used to establish which identity is currently login.

what is the difference between su and su - ?

Auto completion on CLI

- Type ***TAB*** to complete command lines:-
  - Used for completing **command names**.
  - Used for completing **file names**.
  - Cannot be used for anything else other than the above.
- Example:

  $ tr <Tab> <Tab>

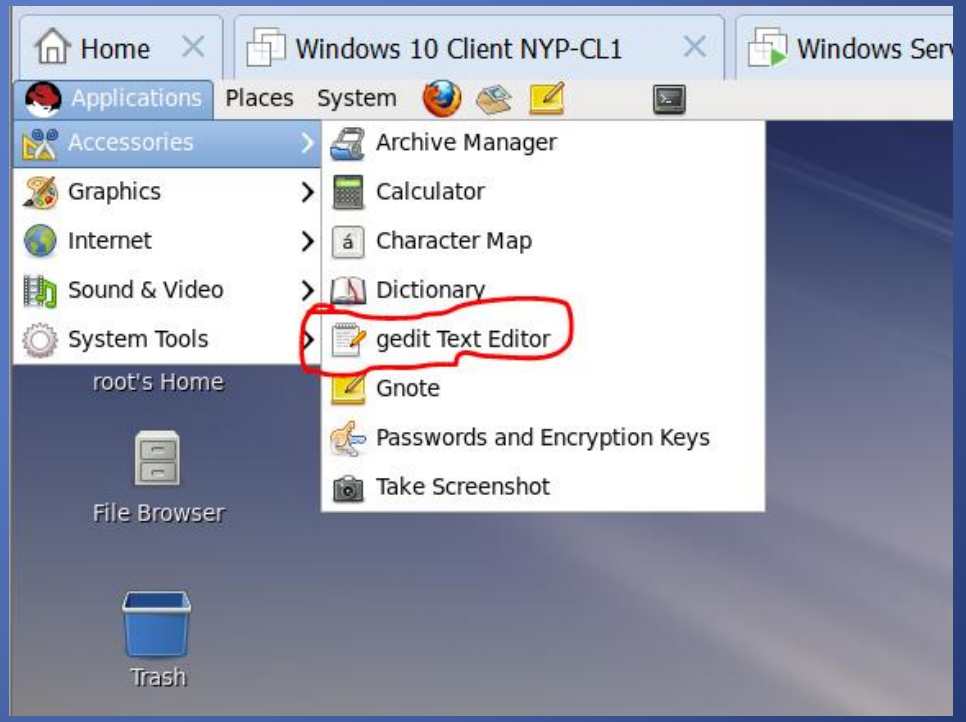
  $ tra <Tab> <Tab>

History command

- The default login shell (CLI) is the bash shell.
- Type ***history*** command to review past commands entered.
- Use ***up*** or ***down*** arrow keys to scroll thorough command history.
- Hit ***Enter*** to select command based on history.
- Use ***CTRL-r*** to search for a command in the history list.
- To recall last ***argument(s)*** from previous command:-
  - ***ESC*** followed by ***.***

Editing files

- On the CLI, type ***nano*** command to activate text editor (or gedit)
- GUI editor – ***gedit***



--help Option

- Displays command summary and argument list
- Activated by the **--help** option
  - Example: $ **passwd --help**
- You must understand how to read the symbols used in the summary:-
  - Anything in braces(**[]**) is optional.
  - Anything followed by **…** means that there can one or more of the preceding item.
  - Multiple options are separated by (**|**), this means that you can only use one of them.
  - Any text enclosed with brackets (**<>**) represents variable data.

Reading help summaries

- Arguments in [ ] are optional
- Arguments in CAPS or <> are variables
- Text followed by … means can be one or more of the preceding item.
- x|y|z means “x or y or z”
- -abc means “any mix of -a, -b or -c”

The man Command

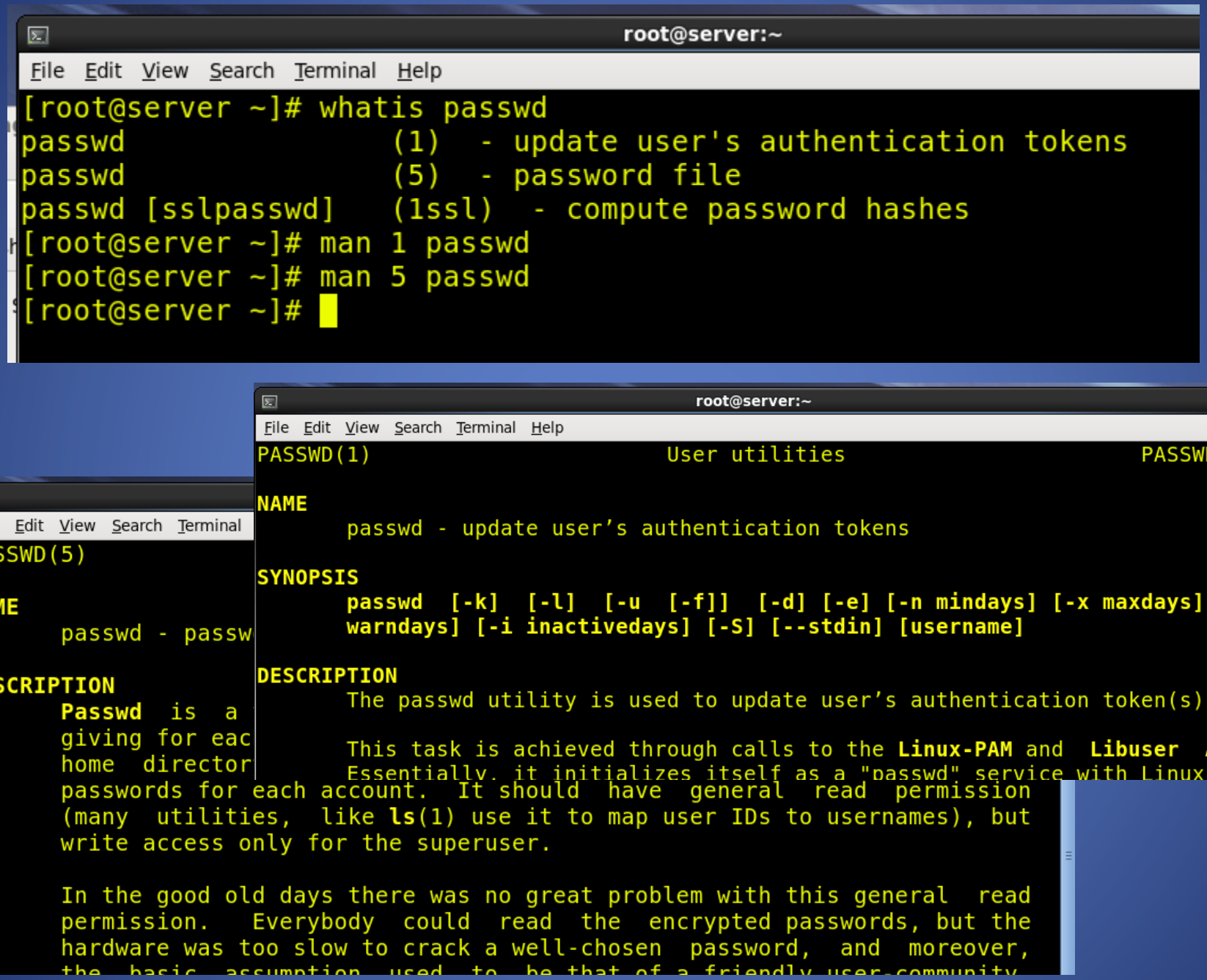
- The syntax for the man command is :-
- **man [<chapter>] <command>**
- Navigate with **arrows, PgUp, PgDn**
- ***/text*** searches for text
- **n** goes to next/previous match
- **q** quits

Getting Help

- Manpage
  - $ man ls
  - $ man 2 mkdir
  - $ man man
  - $ man -k mkdir

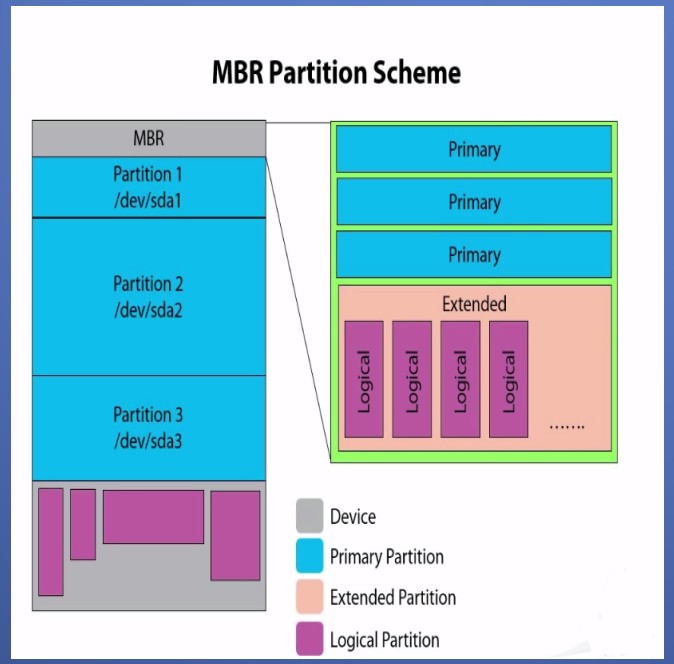
whatis command - get a one-line manual page description

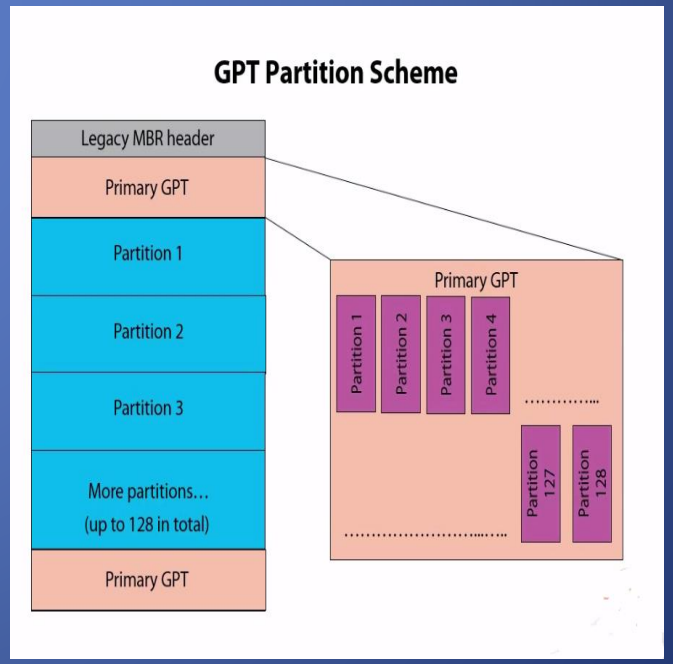
$ whatis passwd


root@server:~
File Edit View Search Terminal Help
[root@server ~]# whatis passwd
passwd (1) - update user's authentication tokens
passwd (5) - password file
passwd [sslpasswd] (1ssl) - compute password hashes
[root@server ~]# man 1 passwd
[root@server ~]# man 5 passwd
[root@server ~]#
root@server:~
File Edit View Search Terminal Help
PASSWD(1) User utilities PASSWD(1)
NAME
passwd - update user's authentication tokens
SYNOPSIS
passwd [-k] [-l] [-u [-f]] [-d] [-e] [-n mindays] [-x maxdays] [-w warndays] [-i inactivedays] [-S] [--stdin] [username]
DESCRIPTION
The passwd utility is used to update user's authentication token(s).
This task is achieved through calls to the Linux-PAM and Libuser API.
File Edit View Search Terminal
PASSWD(5)
NAME
passwd - passw
DESCRIPTION
Passwd is a
giving for eac
home director
passwords for each account. It should have general read permission
(many utilities, like ls(1) use it to map user IDs to usernames), but
write access only for the superuser.
In the good old days there was no great problem with this general read
permission. Everybody could read the encrypted passwords, but the
hardware was too slow to crack a well-chosen password, and moreover,

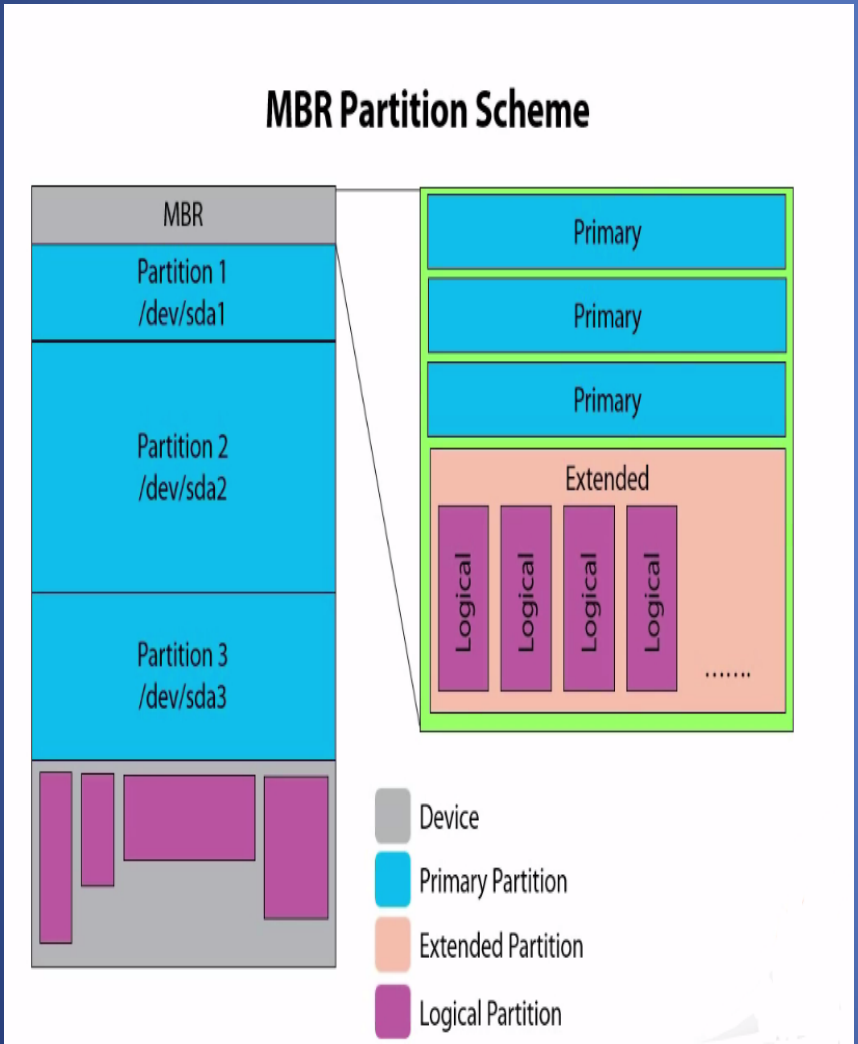
Disk Management

- The physical disk can be divided into several partitions
- Each partition is an independent logical disk within the physical disk
- 2 types of partitioning scheme
  - MBR
  - GPT





Disk Management



Types of partitions

- MBR
  - Holds the information on how the logical partitions, containing file systems, are organized on that medium.
- Primary
  - Up to 4 primary partition
  - One of them active to boot the system
- Extended
  - Used to create additional partitions
- Logical
  - Up to 15 logical partitions per disk
  - Cannot boot the system from there
- Support up to 2TB disk size

Disk Management Commands

- fdisk – view/create/modify/delete hard disk partitions
- parted - add, delete, shrink and extend disk partitions along with the file systems located on them
- mkfs - build a linux file system on a device, usually a hard disk partition.
- mount - serves to attach the filesystem found on some device to the big file tree.
- umount - detaches the file system from the file hierarchy.

Linux File Systems

- Linux file systems include:
  1) ext2, ext3, **ext4**
  2) jfs
  3) ReiserFS
  4) XFS
  5) Btrfs
  6) Swap

Linux File Systems

ext2, ext3, ext4	These are the progressive version of Extended Filesystem (ext), which primarily was developed for MINIX. The second extended version (ext2) was an improved version. Ext3 added performance improvement. Ext4 was a performance improvement besides additional providing additional features.
jfs	The **Journaled File System** (**JFS**) was developed by IBM for AIX UNIX which was used as an alternative to system ext. JFS is an alternative to **ext4** currently and is used where stability is required with the use of very few resources. When CPU power is limited JFS comes handy.
ReiserFS	It was introduced as an alternative to **ext3** with improved performance and advanced features. There was a time when **SuSE Linux**‘s default file format was **ReiserFS** but later Reiser went out of business and SuSe had no option other than to return back to **ext3**.

Linux File Systems

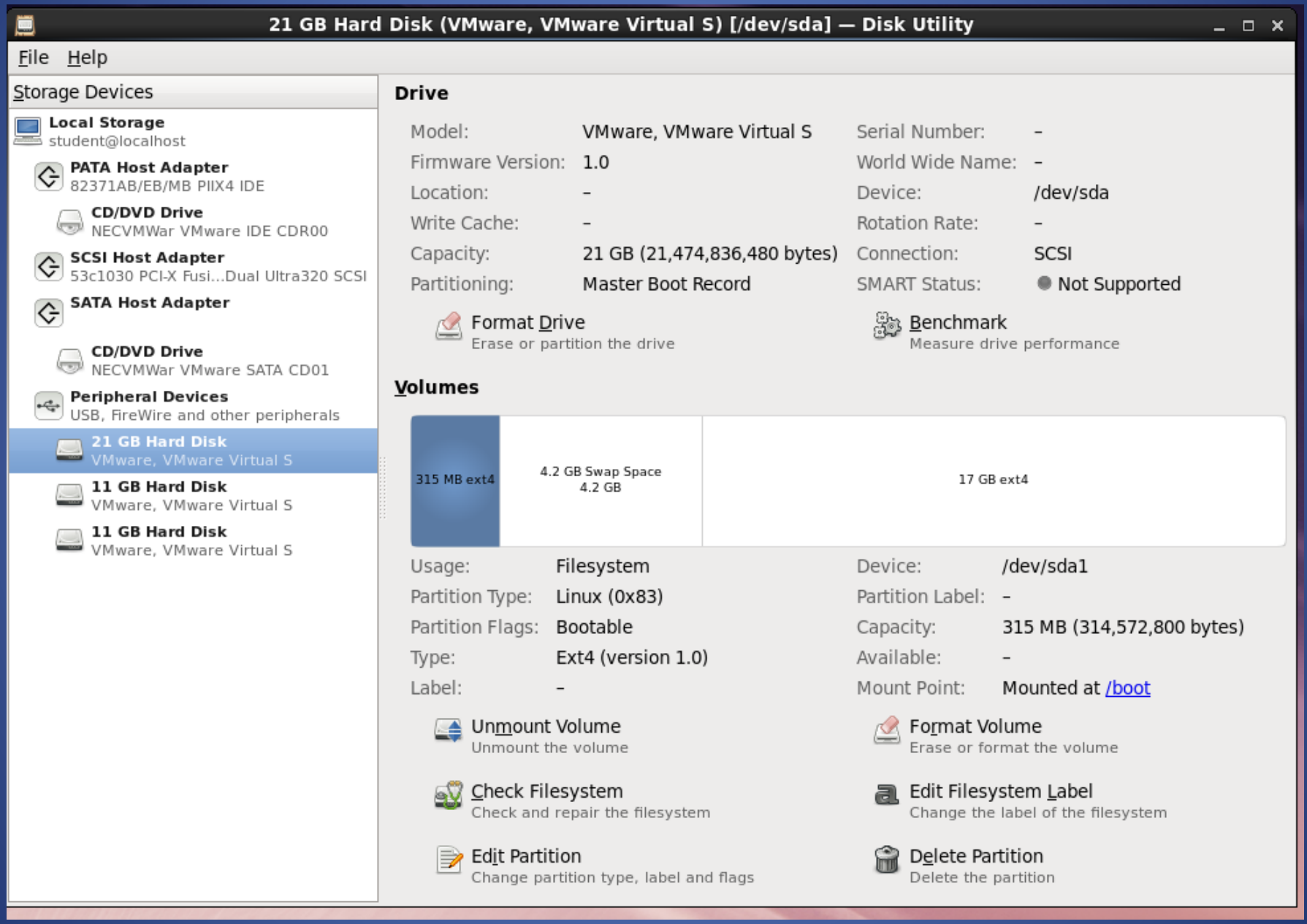
XFS	**XFS was a high speed JFS which aimed at parallel I/O processing. NASA still usages this file system on their 300+ terabyte storage server.**
Btrfs	**B-Tree File System** (**Btrfs**) focus on fault tolerance, fun administration, repair System, large storage configuration and is still under development. Btrfs is not recommended for Production System.
Swap	Swap is a space on a disk that is used when the amount of physical RAM memory is full. When a Linux system runs out of RAM, inactive pages are moved from the RAM to the swap space.

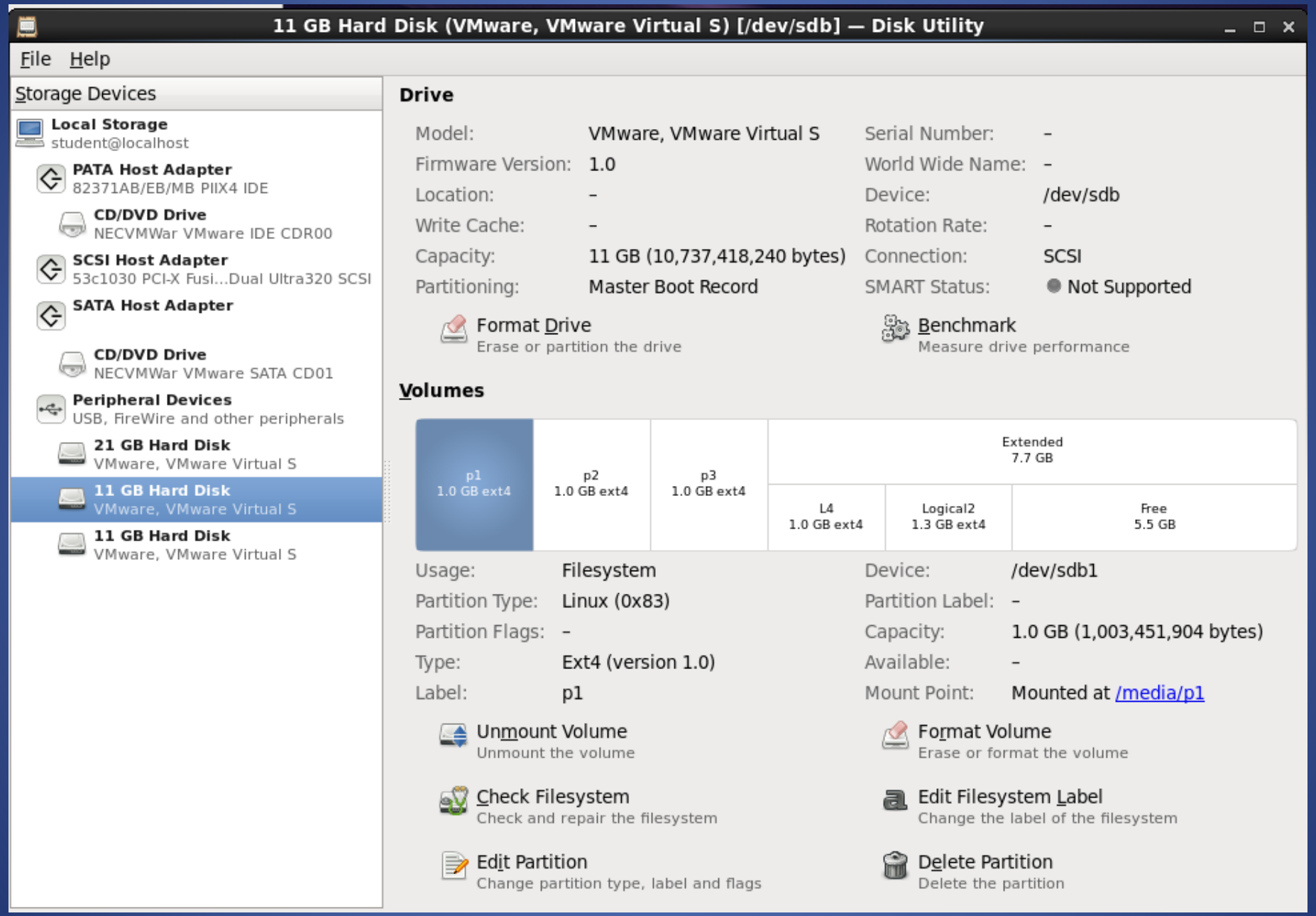
Default – use ext4

Linux File Systems Comparison

File System	Max File Size	Max Partition Size	Journaling	Notes
ext2	2 TiB	32 TiB	No	Legacy
ext3	2 TiB	32 TiB	Yes	Standard linux filesystem for many years. Best choice for super-standard installation.
ext4	16 TiB	1 EiB	Yes	Modern iteration of ext3. Best choice for new installations where super-standard isn't necessary.
reiserFS	8 TiB	16 TiB	Yes	No longer well-maintained.
JFS	4PiB	32PiB	Yes (metadata)	Created by IBM - Not well maintained.
XFS	8 EiB	8 EiB	Yes (metadata)	Created by SGI. Best choice for a mix of stability and advanced journaling.

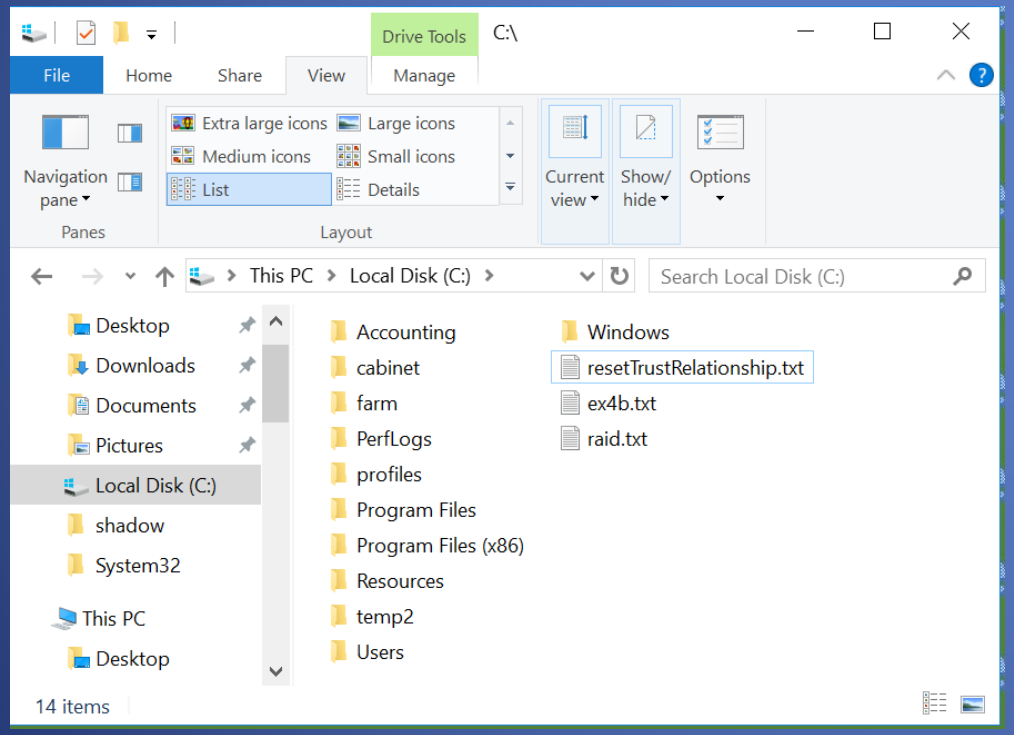
Applications -> Systems Tools -> Disk Utility



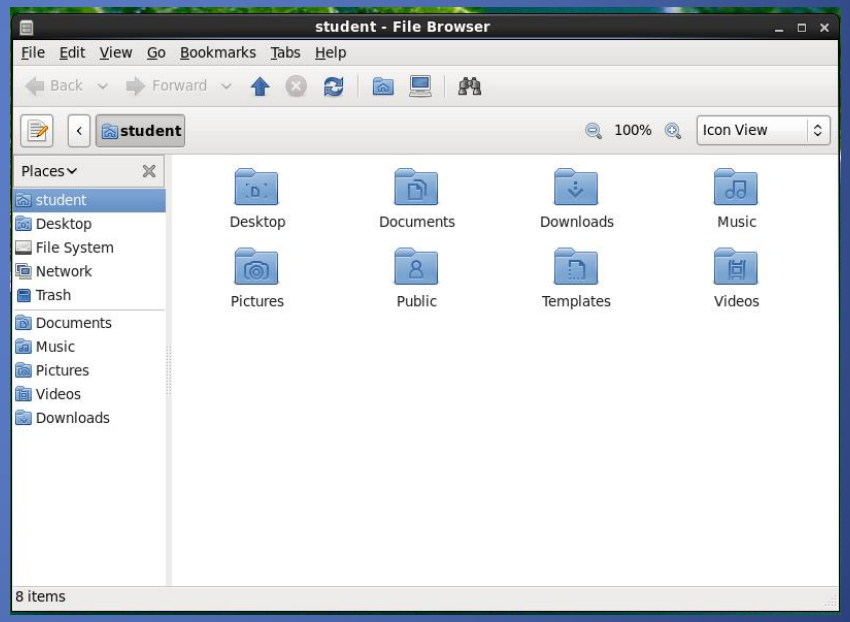

11 GB Hard Disk (VMware, VMware Virtual S) [/dev/sdb] — Disk Utility
File Help
Storage Devices
Local Storage
student@localhost
PATA Host Adapter
82371AB/EB/MB PIIX4 IDE
CD/DVD Drive
NECVMWar VMware IDE CDR00
SCSI Host Adapter
53c1030 PCI-X Fusi...Dual Ultra320 SCSI
SATA Host Adapter
CD/DVD Drive
NECVMWar VMware SATA CD01
Peripheral Devices
USB, FireWire and other peripherals
21 GB Hard Disk
VMware, VMware Virtual S
11 GB Hard Disk
VMware, VMware Virtual S
11 GB Hard Disk
VMware, VMware Virtual S
Drive
Model: VMware, VMware Virtual S
Serial Number: –
Firmware Version: 1.0
World Wide Name: –
Location: –
Device: /dev/sdb
Write Cache: –
Rotation Rate: –
Capacity: 11 GB (10,737,418,240 bytes)
Connection: SCSI
Partitioning: Master Boot Record
SMART Status: Not Supported
Format Drive
Erase or partition the drive
Benchmark
Measure drive performance
Volumes
p1
1.0 GB ext4
p2
1.0 GB ext4
p3
1.0 GB ext4
Extended
7.7 GB
L4
1.0 GB ext4
Logical2
1.3 GB ext4
Free
5.5 GB
Usage: Filesystem
Device: /dev/sdb1
Partition Type: Linux (0x83)
Partition Label: –
Partition Flags: –
Capacity: 1.0 GB (1,003,451,904 bytes)
Type: Ext4 (version 1.0)
Available: –
Label: p1
Mount Point: Mounted at /media/p1
Unmount Volume
Unmount the volume
Format Volume
Erase or format the volume
Check Filesystem
Check and repair the filesystem
Edit Filesystem Label
Change the label of the filesystem
Edit Partition
Change partition type, label and flags
Delete Partition
Delete the partition

Windows vs Linux

- Windows – drive, folder, files
- Linux – folder, files

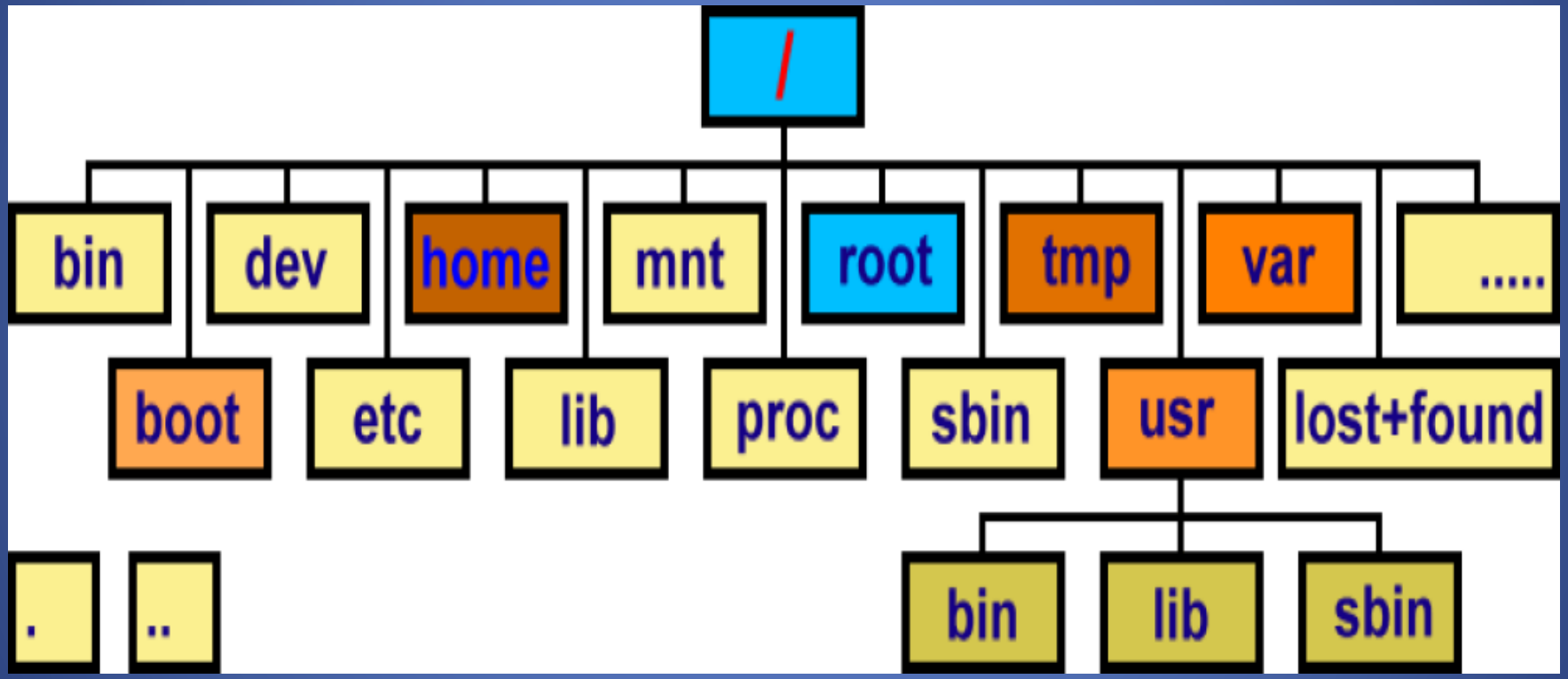


Windows



Linux

File Management



Linux File Management

/ – > root
every single file and directory starts from the root directory.
/bin – > user binaries
common linux commands you need to use in single-user modes are located under this directory.
/dev – > device files
 contains the special device files for all the devices. the device files are created during installation
/home – home directories
home directories for all users to store their personal files.

File Management

/mnt – mount directory

temporary mount directory where sysadmins can mount filesystems.

/root – root home directory

/var – variable files

system log files (/var/log); packages and database files (/var/lib); emails (/var/mail); print queues (/var/spool); lock files (/var/lock); temp files needed across reboots (/var/tmp);

/boot – boot loader files

contains boot loader related files.

File Management

lib – system libraries

contains library files that supports the binaries located under /bin and /sbin

/proc – process information

contains information about system process.

/sbin – system binaries

the linux commands located under this directory are used typically by system administrator, for system maintenance purpose.

/usr – user programs

contains binaries, libraries, documentation, and source-code for second level programs.

File Management

/etc – configuration files

contains configuration files required by all programs.

/opt – optional add-on applications

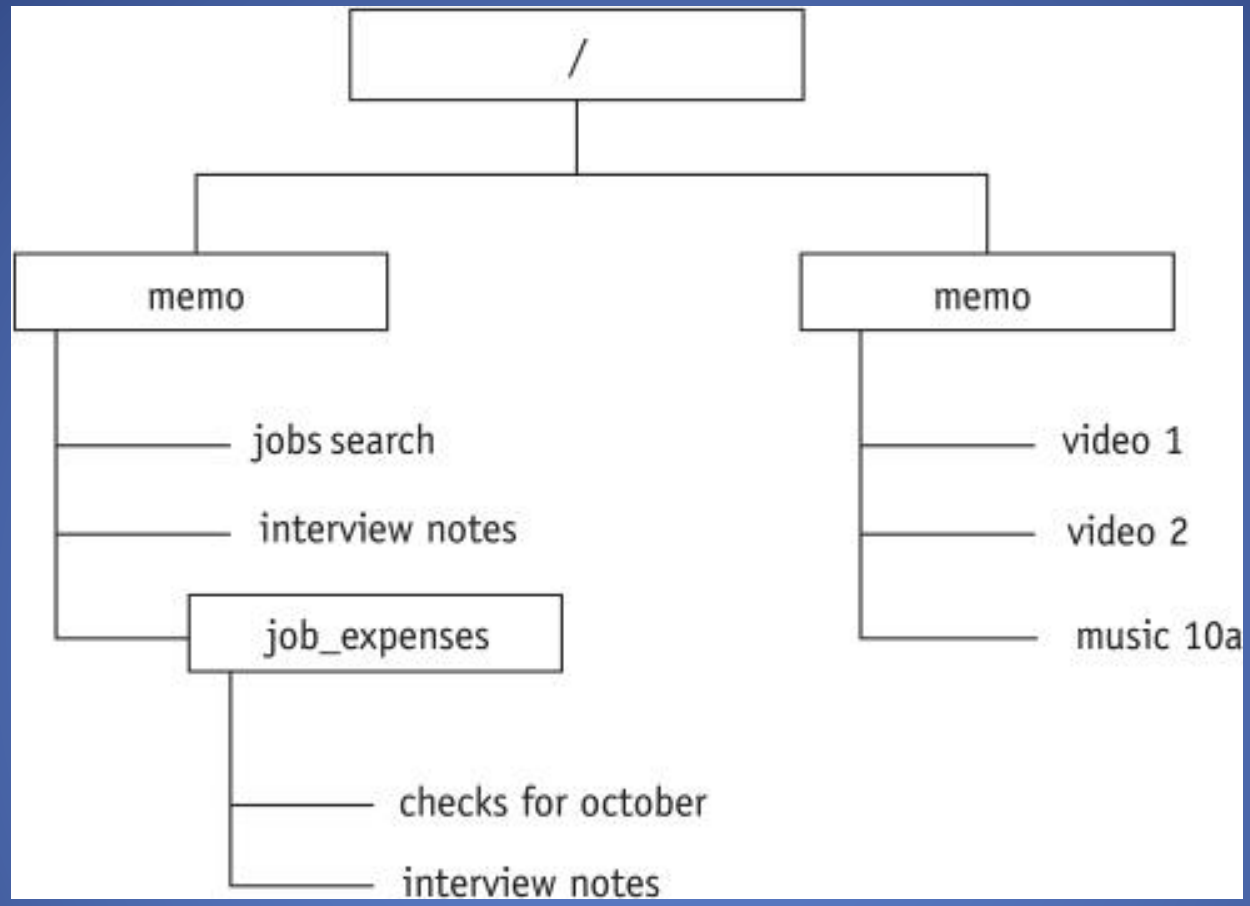
contains add-on applications from individual vendors.

/srv – service data

contains server specific services related data.

Filename Conventions

- Case sensitive
  - Recognizes uppercase and lowercase letters
- Up to 255 characters long
- Contain alphabetic characters, underscores, and numbers
- File suffixes: optional
- Can include space
  - Complications if running command-line programs
- File hierarchy
  - First slash indicates an absolute path name



A sample file hierarchy. The forward slash (/) at the top represents the root directory.

Filename Conventions (cont'd.)

- Path name rules
  1. Path name starting with slash: begins at root directory
  2. Path name
     - One name or list of names separated by slashes
     - Last name on list: name of file requested
  3. Two periods (..) in path name
     - Move upward in hierarchy: closer to root
     - Only way to go up the hierarchy

File Type	File Functions
Directory	A file that contains lists of filenames.
Ordinary file	A file containing data or programs belonging to users.
Symbolic link	A file that contains the path name of another file that it is linking to. (This is not a direct hard link. Rather, it's information about how to locate a specific file and link it even if it's in the directories of different users. This is something that can't be done with hard links.)
Special file	A file that's assigned to a device controller located in the kernel. When this type of file is accessed, the physical device associated with it is activated and put into service.
Named pipe	A file that's used as a communication channel among several processes to exchange data. The creation of a named pipe is the same as the creation of any file.

The file type indicates how each file is to be used.

Summary

- Introduction to Linux – Unix vs Linux
- Familiarization of Desktop – Gnome & CLI
- Getting Help – man pages, whatis, --help
- Disk Management - /dev/sda
- File Management – tree hierarchy
- Basic Linux Commands

Reference - Basic Commands

- ls
  - $ ls -l
  - $ ls -a
  - $ ls -la
  - $ ls -l --sort=time
  - $ ls -l --sort=size -r
- cd
  - $ cd /usr/bin
- pwd
  - $ pwd
- ~
  - $ cd ~
- *~user*
  - $ cd ~weesan
- which
  - $ which ls
- whereis
  - $ whereis ls
- locate
  - $ locate stdio.h
  - $ locate iostream
- rpm
  - $ rpm -q bash
  - $ rpm -qa
  - $ rpm -qa | sort | less
- find
  - $ find / | grep stdio.h
  - $ find /usr/include | grep stdio.h

Basic Commands (cont)

- echo
  - $ echo “Hello World”
  - $ echo -n “Hello World”
- cat
  - $ cat /etc/motd
  - $ cat /proc/cpuinfo
- cp
  - $ cp foo bar
  - $ cp -a foo bar
- mv
  - $ mv foo bar
- mkdir
  - $ mkdir foo
- rm
  - $ rm foo
  - $ rm -rf foo
  - $ rm -i foo
  - $ rm -- -foo
- chgrp
  - $ chgrp bar /home/foo
- chsh
  - $ chsh foo
- chfn
  - $ chfn foo
- chown
  - $ chown -R foo:bar /home/foo

Basic Commands (cont)

- tar
  - $ tar cvfp lab1.tar lab1
- gzip
  - $ gzip -9 lab1.tar
- untar & ungzip
  - $ gzip -cd lab1.tar.gz | tar xvf –
  - $ tar xvfz lab1.tar.gz
- touch
  - $ touch foo
  - $ cat /dev/null > foo
- Pipe
  - $ cal > foo
  - $ cat /dev/zero > foo
  - $ cat < /etc/passwd
  - $ who | cut -d' ' -f1 | sort | uniq | wc –l
- backtick
  - $ echo "The date is `date`"
  - $ echo `seq 1 10`
- Hard, soft (symbolic) link
  - ln vmlinuz-2.6.24.4 vmlinuz
  - ln -s firefox-2.0.0.3 firefox

Network Commands

arp - this program lets the user read or modify their arp cache.

ifconfig - configure a network interface.

ifdown - shutdown a network interface.

ifup - brings a network interface up. ex: ifup eth0

netstat -displays information about the systems network connections, including port connections, routing tables, and more. the command "netstar -r" will display the routing table.

nslookup - used to query dns servers for information about hosts.

ping - send icmp echo_request packets to network hosts.