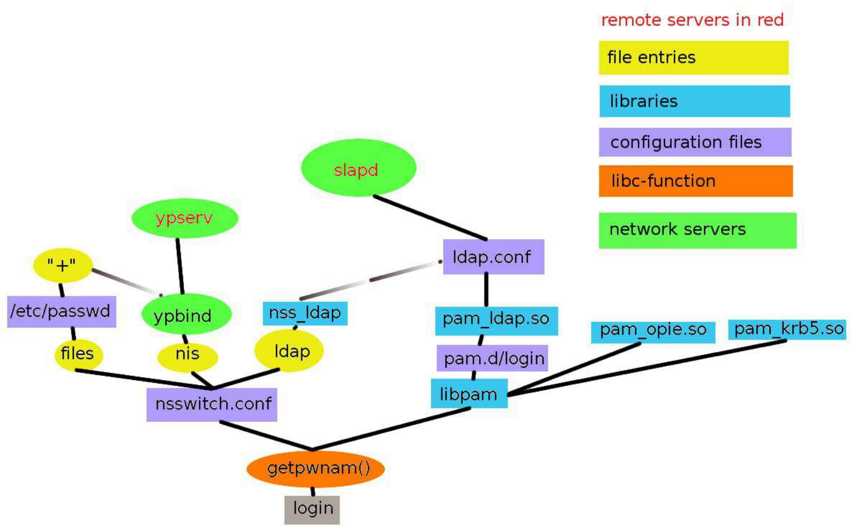


## Pluggable Authentication Module (1)

variety of authentication methods

- smartcards
- Kerberos
- one–time–passwords (OPIE)
- . . . (what next?)

configurable *modules* needed ⇝**PAM**

## Pluggable Authentication Module (2)

directory

`/etc/pam.d`

config files with sections

**auth** authentication functions

**account** account management functions

**session** session handling functions

**password** password management functions

entries (example):

```
auth          sufficient      pam_opie.so
```

## Managing Users: More Commands

password-related commands for users and admins

- `vipw` (root)
- `chpass` change password entries (root)
- `chsh` change shell (root/user)
- `chfn` change real name (root/user)
- `passwd` change password (root/user)
- `pw` swiss army knife to change password entries (FreeBSD)

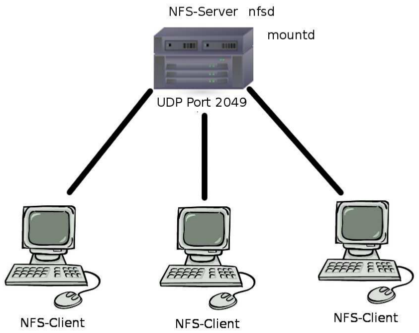
## Network File System: NFS (1)

distribute file system

example: `/home`

implementation: RPC

handbook section 27.3



## Network File System: NFS (2)

server host

- needs servers
  - `mountd` handles mount requests (`exports` file)
  - `nfsd` handles data requests at port `2049/udp`
  - `portmap` or `rpcbind` to handle RPC
- needs configuration
  - services above must be started at boot time
  - which filesystems are exported to other hosts `/etc/exports`

example entry

```
/home -maproot=bin: 134.96.216.81
```

## NIS/NFS security

no security issues since several years

summary of configuration issues

- NIS: separate NIS `passwd` map from local `/etc/passwd`
- NIS: control client access to NIS server
- NFS: no exports to the world
- NFS: map root to a non–root account
- NFS: firewalling the NFS–port

more details

`http://www.securityfocus.com/infocus/1387`

## Alternatives

OpenAFS (Andrew File System) `http://www.openafs.org/`

influenced NFSv4

CIFS / SMB `http://www.samba.org/`

## Special Feature: amd

Automount Daemon

can mount the network device, whenever a file is accessed

for example, if the user logs in

⤳no permanent connection to NFS server needed

## Limiting Users

- don't interfere with needs of other users
- don't interfere with system processes

## Limiting Users: Per-Process Limits (1)

```
$ ulimit -a
core file size         (blocks, -c) unlimited
data seg size          (kbytes, -d) 524288
file size              (blocks, -f) unlimited
max locked memory      (kbytes, -l) unlimited
max memory size        (kbytes, -m) unlimited
open files                     (-n) 3117
pipe size           (512 bytes, -p) 1
stack size             (kbytes, -s) 65536
cpu time              (seconds, -t) unlimited
max user processes             (-u) 1558
virtual memory         (kbytes, -v) unlimited
```

## Limiting Users: Per-Process Limits (2)

there are three limits:

- kernel limit (=absolute system limit), often in kernel header file
- hard limit (may only be lowered by user), set by
  - system admin in global login script `/etc/profile`, or
  - sysctl kernel variable, or
  - system–specific files (FreeBSD: `/etc/login.conf`)
  - user via `ulimit`
- soft limit (may be lowered/raised by user), ≤ hard limit (use `ulimit -S`)

## Limiting Users: Disk Quotas

- cannot be enforced on process level
- is a filesystem property
- must be enabled in kernel
- must be set when mounting a filesystem (see below)
- command `quota -v` lists disk usage
- command `edquota -u user` sets user limit

Note: quotas slow down writing to disk

# 6. File System

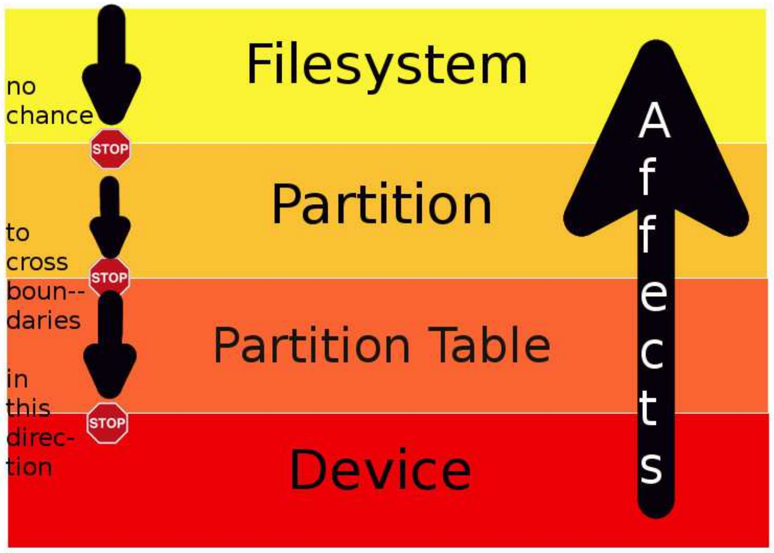
## Drives and Capacity

as of 2014

| Drive | Bandwidth (read) | Capacity | EUR/GB |
|---|---|---|---|
| hard disk drive | 1.6 GB/s | 60 GB. . . 4 TB | 0.06. . . 0.20 |
| solid state drive | 2.7 GB/s | 120 GB. . . 2 TB | 0.70. . . 0.85 |
| secure digital memory card | 150 MB/s | 4 GB. . . 128 GB | 0.68. . . 0.85 |
| USB memory stick | 60 to 90 MB/s | 4 GB. . . 256 GB | 0.69. . . 2.00 |
| digital versatile disk | 61.7 MB/s (16x) | 4.7 GB (1s, 1l) | 0.69. . . 2.00 |

```
http://en.wikipedia.org/wiki/Hard_disk_drive
http://www.intel.com/content/www/us/en/
       solid-state-drives/solid-state-drives-ssd.html
http://www.tomshardware.com/charts/-usb-3.0-card-reader-charts-2014/
       -01-Compact-Flash-Sequential-Read-MB-s,3542.html
http://www.tomshardware.com/reviews/DVD-Burner,2447-8.html
```

## Logical Layering



no chance to cross boun-daries in this direc-tion

STOP

Filesystem

Partition

Partition Table

Device

Affects

## Partition Mess on Intel Systems

- first ,,OS" for Intel-based system was MS-DOS
- fundamental design error: four partitions on a hard disk named C:, D:, E:, F: (restriction 32 MB in MS-DOS 3.3 in 1987)
- disks grew bigger ⇝more ,,logical" partitions G:, H:. . .
- disks grew still bigger ⇝larger partitions
- MBR: still four *primary* partitions
- MBR: ,,extended" partition contains *logical* partitions
- MBR: disk limit 2 TB,
- MBR: no backup
- MBR: no error correcting code

## UEFI Unified Extensible Firmware Interface

EFI: Itanium platform 1998 (Intel)

UEFI: April 2011 (Intel, AMD, Microsoft, Apple,. . . )

- GPT = GUID Partition Table
- pre-OS environment, including network capability
- 8 ZiB = 8000 EiB

SI-Prefixes: kilo-mega-giga-tera-peta-exa-zetta-yotta-. . .

IEEE1541: kibi-mebi-gibi-tebi-pebi-ebi-zebi-yobi-. . .

Linux / Windows 64-bit / HP-UX / HP-OpenVMS / Apple(Intel) / FreeBSD(GPT)

GUID = Globally Unique Identifier

## What is a File System?

A file system is a *logical* unit of (background) memory.

Inodes are local to a file system.

A file system can live on

- a hard disk
- a floppy disk
- a CDROM
- a DVD
- a memory stick
- a part of RAM (RAMDISK)
- . . .

## FreeBSD Device Naming

The name determines what type of driver handles the storage device:

| device name | drive type |
|---|---|
| ad | IDE (ATA, SATA) hard drives |
| da | USB mass storage, SCSI hard drives |
| acd | IDE CDROM drives |
| cd | SCSI CDROM drives |
| scd,mcd | non–standard CDROM drives |
| sa | SCSI tape drives |
| ast | IDE tape drives |
| fla | flash drives |
| aacd,mlxd,mlyd,idad,twed | RAID drives |

## Linux Device Naming

- /dev/hda first drive, first IDE controller
- /dev/sda first drive, first SATA/SCSI controller
  - first partition /dev/sda1.
  - second partition /dev/sda2.
- /dev/sdb 2nd drive
  - first partition /dev/sdb1.
  - second partition /dev/sdb2.

Type of device is irrelevant (HDD/CDROM).

## Which devices are found?

Look at the boot messages.

Example:

```
# dmesg

ada0 at ata0 bus 0 scbus2 target 0 lun 0
ada0: <ST3250310AS 3.AAB> ATA-7 SATA 2.x device
ada0: 238475MB (488397168 512 byte sectors: 16H 63S/T 16383C)

ada1 at ata1 bus 0 scbus3 target 1 lun 0
ada1: <ST3500418AS CC38> ATA8-ACS SATA 2.x device
ada1: 476940MB (976773168 512 byte sectors: 16H 63S/T 16383C)

acd0: DVDROM <TSSTcorpDVD-ROM SH-D162C/TS04> at ata1-master UDMA33
acd1: CDRW <CW088D ATAPI CD-R/RW/V110F> at ata1-slave UDMA33
```

## FreeBSD GPT Device and Partition Naming

/dev/ada0 is the first drive

Its first partition is /dev/ada0p1 (boot).

Its second partition is /dev/ada0p2 (usually / ).

```
# gpart show ada0
=>        34  488397101  ada0  GPT  (233G)
          34       1024     1  freebsd-boot  (512K)
        1058   10485760     2  freebsd-ufs  (5.0G)
    10486818  209715200     3  freebsd-ufs  (100G)
   220202018   25165824     4  freebsd-ufs  (12G)
   245367842    8388608     5  freebsd-ufs  (4.0G)
   253756450  125829120     6  freebsd-ufs  (60G)
   379585570    8388608     7  freebsd-swap  (4.0G)
   387974178  100422957     8  freebsd-ufs  (48G)
```

## Example: booting different partition

```
gpart unset -a bootme -i 2 ada0

gpart set -a bootme -i 6 ada0
```

## File System (FS)

- lives within a partition
- maps directory-tree structure and files to disk
- inodes (meta–data) and directories/files (data)
- faetures: max FS size, max file size, crash recovery. . .

⇝several file system types

http://linux-xfs.sgi.com
/projects/xfs/papers/xfs_white/xfs_white_paper.html

## File System Types

- FreeBSD
  - ufs (UNIX filesystem), FFS (Berkeley Fast Filesystem)
  - ext2fs
  - cd9660 – CD–ROM file system
  - new: ZFS (Sun Microsystems)
  - . . .
- Linux
  - ext2 – standard linux FS
  - ext3 – journaling extension of ext2
  - ext4 – extension of ext3 (performance/features)
  - reiserfs – file system based on balanced trees

  - jfs – IBM's journaled FS
  - xfs – journaled FS
  - iso9660 – CD–ROM file system
  - . . .

http://www.tech-analyser.com/2011/10/
understanding-file-systemsntfs-fat.html

http://www.enterprisestorageforum.com/technology/features/
article.php/3849556/10-Reasons-Why-ZFS-Rocks.htm

## Show supported FS types

```
$ ls -l /sbin/mount_*
-r-xr-xr-x  /sbin/mount_cd9660
-r-xr-xr-x  /sbin/mount_fusefs
-r-xr-xr-x  /sbin/mount_mfs
-r-xr-xr-x  /sbin/mount_msdosfs
-r-xr-xr-x  /sbin/mount_nfs
-r-xr-xr-x  /sbin/mount_nullfs
-r-xr-xr-x  /sbin/mount_oldnfs
-r-xr-xr-x  /sbin/mount_udf
-r-xr-xr-x  /sbin/mount_unionfs
```

## Partitioning/FS/Mounting

| action | GPT |
|---|---|
| partition disk | `gpart` |
| init filesystem | `newfs/mkfs` |
| dev ⇝ dir tree | `mount` |

| command | parameters |
|---|---|
| `gpart` | disk |
| `newfs` | partition, FS type |
| `mount` | partition, directory |

## Partitioning (1)

concept: additional layer between disk and FS

advantage:

- separated file storage
- controlled subsystems

disadvantage:

- fixed size (though `growfs` may resize)
- each partition to be configured

## Partitioning (2)

Should be done carefully (fixed sizes).

The system core should not be affected by file I/O of users.

⇝`/`, `/home`, `/var`, `/tmp` should be on different file systems

swap at least as big as RAM

/var at least as big as RAM