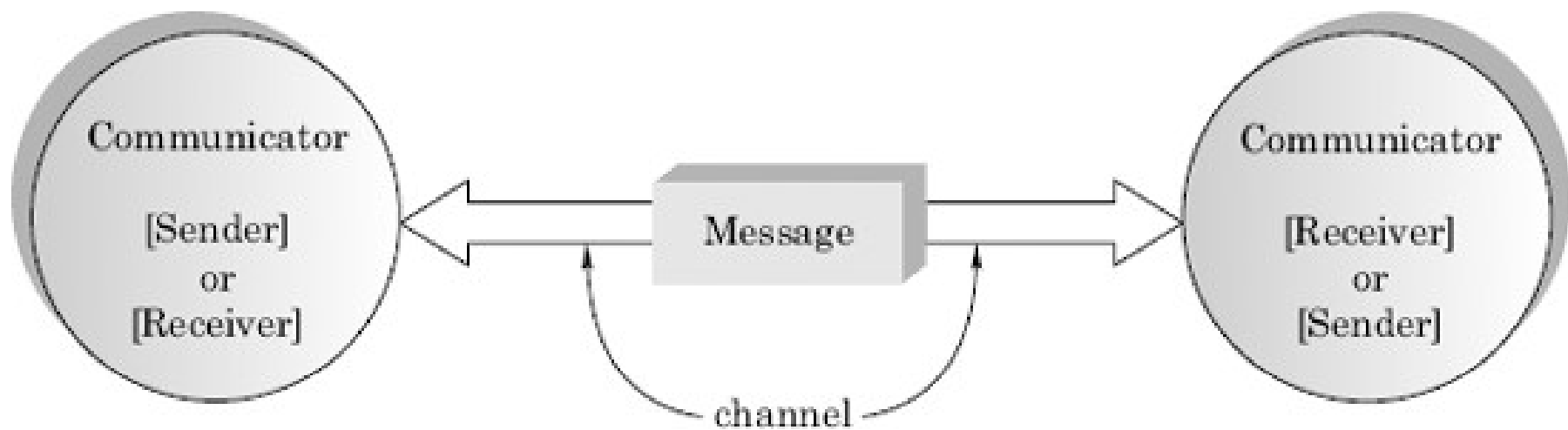# UNIT – V

UNIX SYSTEM COMMUNICATION

Dr.T.Logeswari

- Electronic mail or email is easiest way of communication on unix.

- Fast and cheap

- Used to exchange graphics , sound and video files

Communicator

[Sender]
or
[Receiver]

Message

channel

Communicator

[Receiver]
or
[Sender]

Elements of a communication process

1. sender

2. receiver

3.message

4.channel

The mesg command

- Unix facilitates users to send messages to other user's terminals who are logged in.

- This is possible only if other terminal has given a write permission.

- The mesg command is used to change the write permission of a user.

Options:
- y for yes
- n for no
- example:
- $mesg y   #grants write permission
- $mesg n   #denies write permission
- $mesg is n   #displays current status of write permission of the terminal.

Write command

- Allows a two-way communication between two users who are currently logged in and who have given write permission.

- Example:

  $write prathiba

    Going on a tour?happy journey.

    -rama

    <ctrl d>   #indicates end of message

- Message from rama@maharani on pts/2 at 14:43………

going on a tour? Happy journey.

Rama

EOF

- Conversation continues until one or both users decide to end it.

- Both users must be logged in else error message appears.

The finger command

- Similar to who command.
- It lists the details of users who have logged in and given permission to accept messages.

Example:

$finger

Login Name Tty Idle Login time office office ph.

Rama rama pts/1   feb28 13:57

Uma   uma.k pts/2   feb 28 14:21

- In this example
- Login shows login name of users
- Name shows full name of the users
- Tty shows device number of the terminals
- Idle shows idle time since user logged in
- Login time shows time of logging in of the users
- Office and office ph ->shows address and phone numberof the user

The wall command

- Wall stands for write all

- This command can be used only by super user

- Used to send message to all users on the system , known as broadcasting a message to all users .irrespective of whether users have given write permission or not.

- Wall executable file is stored in /etc directory .

- Example:

  $wall   #message send by super user
   There may be power failure.
    please save your files.
     <ctrl d>

Broadcast message from root(pts/3)(sat 09 14:37:28 2016):   #DISPLAYED ON ALL LOGGED

IN USERS.

There may be power failure.

Please save your files.

Electronic mail

- Sending and receiving messages using computer and communication tools is known as e-mail.

    Sending a mail

- The mail command is the basic e-mail program

- Contains text editor to compose mail.

- Can be used to send as well as receive mails.

- Syntax:

  $mail <options> addresses

   message text

   Example:

$mail user1 user2

Subject :seminar

…………………………

Rama <ctrl d>

- User1 and user2 are login names.
- If the receiver is not busy running a program , the following message is displayed on his screen.

➢   you have new mail.

- If the user is not logged in when mail is sent to him ,then message is displayed

➢   You have mail

Receiving a mail

- The mail command without argument is used to receive mails.

- Example:

    $mail

Mail version………

"/var/spool/mail/rama" :2 messages 1 new 1 unread

u 1. <uma> mon mar 03 10:40 labs

>N 2.<std1> mon mar 04 12:32 projects

&

- Received mails of a user are stored in a mailbox.

- Name of this will be his/her login name.

- Mailbox is found in /var/spool/mail directory.

- First line displays version of mail program

- Second line gives a summary of messages , with their status such as unread and new also indicates mail directory used and number of messages in it .

- Next list of mails are shown.

- First character on each line on gives status of each mail. Like new(N),unread(U),(>) character indicates that message as current message

-

- The "& " character in the list line is the mail prompt.
- Actions like reading,saving,deleting,forwarding and quitting the mail program.
- Personal mailbox called 'mbox' is located in user'sdirectory.
- Any message not deleted ,but read ,will be saved in this filewhen user quits mail program.

Internal mail commands

- <Enter> =>displays current mail

- N   =>displays mail numbered N.

- d   =>deletes the current mail.

-   d n   =>deletes mail n.

-   u   =>undeletes current mail

-    w filename =>saves current message in filename.

-   r   =>reply to current mail

- r n =>reply to sender of mail n.

- m user =>forwards the mail to user.

- q   =>quits the mail program.

- -   => print previous message.

-   +   => print next message.

System Administration

Dr.T.Logeswari

Introduction

- It is the installation and maintenance of the unix computer system.

- He is to maintain hardware and software of the system

- It include hardware configuration, software installation, reconfiguration of the kernel, networking etc

- So that the system admin can call as super user or root

- A super user on a unix system is one, who has unrestricted access to all files and command

- The login name is root

Super user status

- There are two ways to acquire super user status
  - To log into console directory as root
  - To execute the su command after logging in under a different username

Root the super user login

- Unix provide a special login name called root for system admin

- This account need not be created since it is in built in every unix system

- The password is set at the time of installation

        login : root

     password :   # not displayed

      #

The su command

- By executing the su command any user can acquire the status of super user if she knows the root password

        $/bin/su-

        password :

        #

- After the # pound sign showing the user now become super user

- The (-) after su changes the shell environment to super user environment ie home directory is changed to root

- It is also known as substitute user

Role of system Administrator

- Starting and shutting down the system
- User management (account adding)
- Disk space management
- Backup and restore
- Management of file system, Devices and Network services
- Monitoring system activity and security
- Responsibility of the user
- Hardware responsibilities
- Providing assistance to user whenever required

Super user privilege

- The super user is the most powerful user on the system.
- He has complete control over the entire system
- He can change the attribute of any file (permission)
- He can remove any command using rm command
- He can change the password
- He can set the system date
- He can sent message using wall command to all the user
- He can limit the size of the file using ulimit command

Security concern

- Preventing unauthorized assess to the system
- Maintaining integrity of the system
- Allow access of user files to, only user group and owner group
- Maintaining tape backup, disk backup, secure network connection
- Some important feature of unix system are
- Password security (/etc/passwd, /etc/group, /etc/shadow)
- The passwd and group files
  - The /etc/passwd file conatin complete information about the user which is recorded when user open the account
  - The three files must be writable only by the root user

Login-id:password:user-id#:group-id#:userinfo:home-dir:shell

- The password file contain one row, for every user. Each row is made up of 7 files separated by colon

The /etc/shadow files

- For every row in /etc/passwd file there is a corresponding entry in /etc/shadow file

- The encrypted password can be easily decrypted with some effort

- So storing the password directly on passwd file is not secure. So they used a separate file to keep called /etc/shadow which can be read and edited only by the system admin

- Username:coded_password:last_change:min_days:max_days: warn_days:disable_in:expire_date

The restricted shell rbash

- A standard shell allows user to move around in the file system, execute commands change environment variables and so on.

- Normal privileges to the user need to be restricted

- So rbash is allotted to him. It is executable program similar to sh but minimum privileges

- The user allowed to work only in home directory

- The user cannot change the PATH variable

- The user cannot allowed to create new files or append to existing files

File Encryption using crypt

- Crypt command is used to protect individual files from other including super user

- It relies on simple substitution

- ~A changed to ^A

- It is used for both encryption and decryption

    $crypt xyz <test> test.crypt

The above command encrypt the file test using key xyz

    $crypt xyz < test.crypt> test   (decrypt)

    $crypt < test > test.crypt

    key

User Management

- The normal duties of the system administrator includes adding or deleting a user or a group from the system

- There are three types of account on a unix system
  - Root account
  - System account
  - User account

managing user and groups

- There are three main user administration files
  - /etc/passwd = keep user account and password information
  - /etc/shadow = hold the encrypted password of the corresponding account
  - /etc/group = group information of each account
  - /etc/gshadow = secure group account information

Adding a user Account

- The addition of a new user account can be done either through a shell script or by editing the /etc/passwd file

- To add a new user called dept the steps are

- Edit the file/etc/passwd using any editor such as vi

- Add the line:

        Dept::105:2Dept of cse : /home/dept:/bin/sh

Dept = is the login name   :: = no password

105 = user id   2 = group id

- Next the home directory of the user is created using mkdir command

    #mkdir / home/ dept

- Since super user created this directory, the owner and the group of this directory will be root

    #chown dept dept

- Similarly the group must be changed from root to csc as below

    # chgrp csc dept

- Now the user can login dept

Create an account through shell script

- Syntax

  Useradd –d homedir –g groupname-m-s shell –u userid accountname

-d homedir = specifies home directory for the account

-g groupname = specifies group account for this account

-m = create home directory if doesnot exist

-s shell =specifies default shell

-u userid = specify user id for the account

$useradd –d/home/mohini –g developer -2/bin/sh mohini

Modify a user account

- The usermod command enables you to make changes to an existing account from the line

- It uses the same argument as the useradd command, plus the -1 argument which allow you to change the account name

- You can change account mohini to mohini20

    $usermod –d/home/mohini20 –m –l mohini mohini20

Removing a user account

- Userdel command is used to delete an existing user

- There is only one argument or option available for the command –r for removing the account home directory and mail file

    $userdel –r mohini20

Startup and shutdown

- Startup
- As soon as the power on the system look all peripherals and next to complete boot cycle
- First important thing is loading into kernel
- -/kerenl/genunix in solar is and /boot/vmlinux in linux into memory
- The kernel known spawn the init(PID1)daemon
- A unix system can be booted to a specific mode which is represented by a number or a letter called runlevel
- Two modes possible single , multiple
- Single user is system admin to perform important task
- Multiuser individual file system to be mounted and system daemeon started

Shutdown

- The system admin shutdown the system at the end of the day
- Abrupt switching off the system may lead to problem
- So shutdown command is used for this purpose
  - Inform the user with wall command about shutting system
  - Send signal to all running process
  - Log off all user and kill remaining processes
  - Unmount all secondary file system
  - Shutdown finally shut down the system successfully

Backup and restore

- The process of saving all important files at regular intervals of time is known as backup or making archive

- The system admin has to decide which file to backup

- The process of restoring all required files from an archives is called extraction

- Backup
  - Tar
  - Cpio
  - dump

The tar command

- The tar command is used for taking backup and restoring those files
- Tar stand for tape archive
- Tar work with filename and directory names as argument
- It operate recursively
- The copies are placed at the end of the archive
- The key option used are

      -c create   -x extract   -t display

      -f device name   -v to display the progress of backup

Creating an archive

- To create an archive the option –cvf is used

  $tar –cvf prgs.tar c_prgs java _prgs sh_script

  -c copy or write

  -f name of the archive prgs.tar

  -v to display the progress of tar command

- In the above example tar command fills the archive prgs.tar with 3 directory

Extracting files from archive

- To extract file from the archive tar uses x-option

$tar –xvf prgs.tar

Viewing the archive

- The content of the file can be viewed by –t option

$tar –tvf prgs.tar

Cpio command

- The cpio command copy input and output is used to copy files to and from backup device

Option

- -o output

- To copy the current directory to 1.44 mb floppy

- #ls | cpio –ov > /dev/fdoh1440

- In above eg the files in current directory are piped to cpio through ls command and redirected to 1.44 mb floppy

Dump Command

- It is not widely preferred when compared to tar command

- It can be used with local file system

- Operate at a lower level when it comes to accessing file system

- The dump command can only backup file in a local system

Checking UNIX file system with fsck

- Fsck is a unix utility for checking and preparing file system inconsistencies
- Reason behind
  - Abnormal shutdown
  - Power failure or switch off the system
- **Fsck – mode of operatio**n
  - **Interactive – error occur stop user correct**
  - **Non interactive – without stopping correct the error**

Running fsck

- Fsck should always be run in a single user mode Which ensure proper repair of system

Command syntax

- Fsck [-F fstype] [-V][-yY]

- -F fstype of file system to be repaired

- -V verify the command line syntax

- -y or –Y run the command in non interactive mode repair

Fsck phases

- Fsck check the file system in a series of 5 pages and check a specific functionality of file system in each phases
  - Phase 1 – check block and size
  - Phase 2 – check pathnames
  - Phase 3 – check connectivity
  - Phase 4 – check reference counts
  - Phase 4 – check cylinder Group

DNS

Figure 25.1 *Example of using the DNS service*
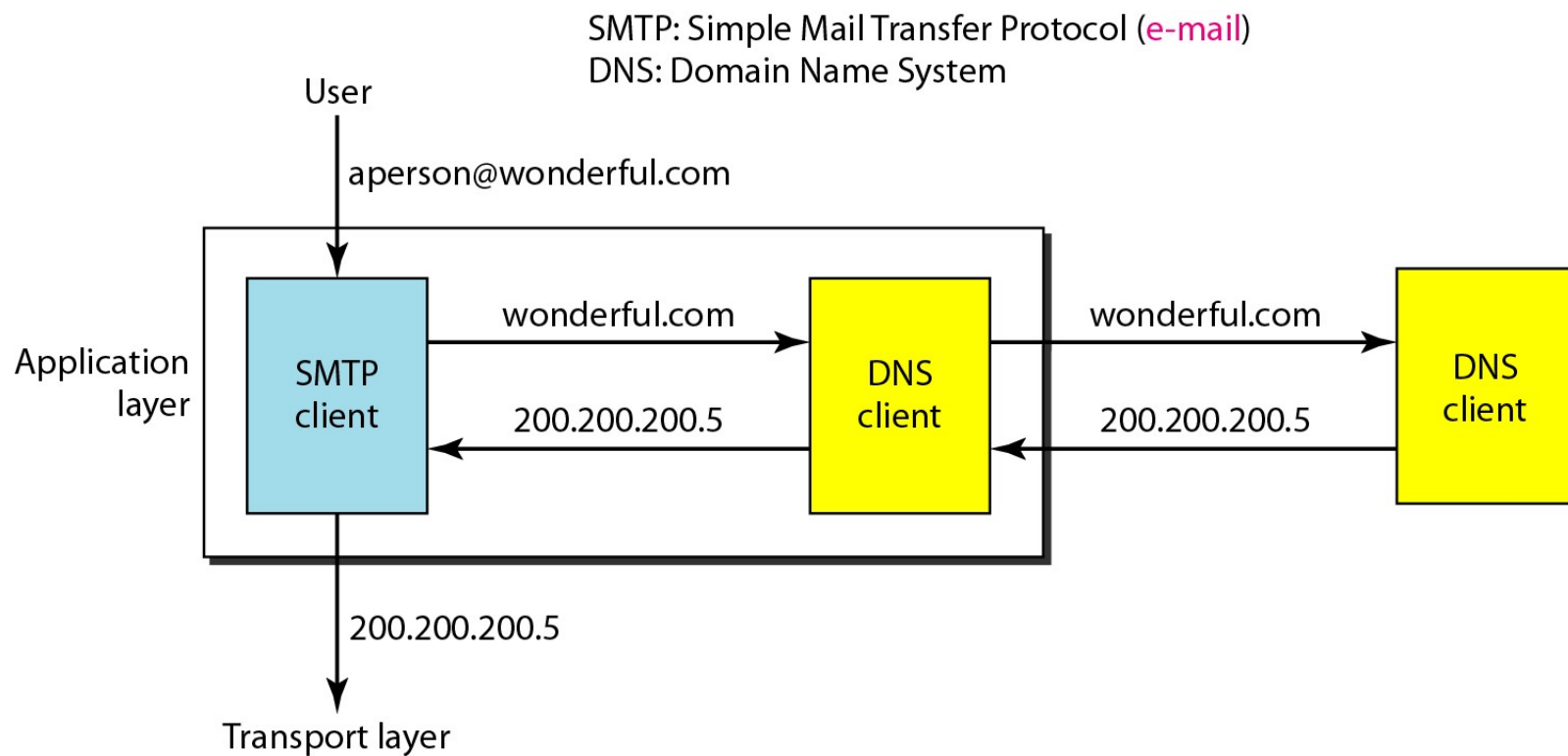
DFS
Definition:

Implement a common file system that can be shared by all autonomous computers in a distributed system

Goals:

Network transparency
High availability

Network File System (NSF)

- Developed by Sun Microsystems to provide a distributed file system independent of the hardware and operating system

- Architecture
  - Virtual File System (VFS):

    File system interface that allows NSF to support different file systems
  - Requests for operation on remote files are routed by VFS to NFS
  - Requests are sent to the VFS on the remote using
    - The remote procedure call (RPC), and
    - The external data representation (XDR)
  - VFS on the remote server initiates files system operation locally
  - *Vnode* (Virtual Node):
    - There is a network-wide *vnode* for every object in the file system (file or directory)- equivalent of UNIX *inode*
    - *vnode* has a mount table, allowing any node to be a mount node

NFS Architecture
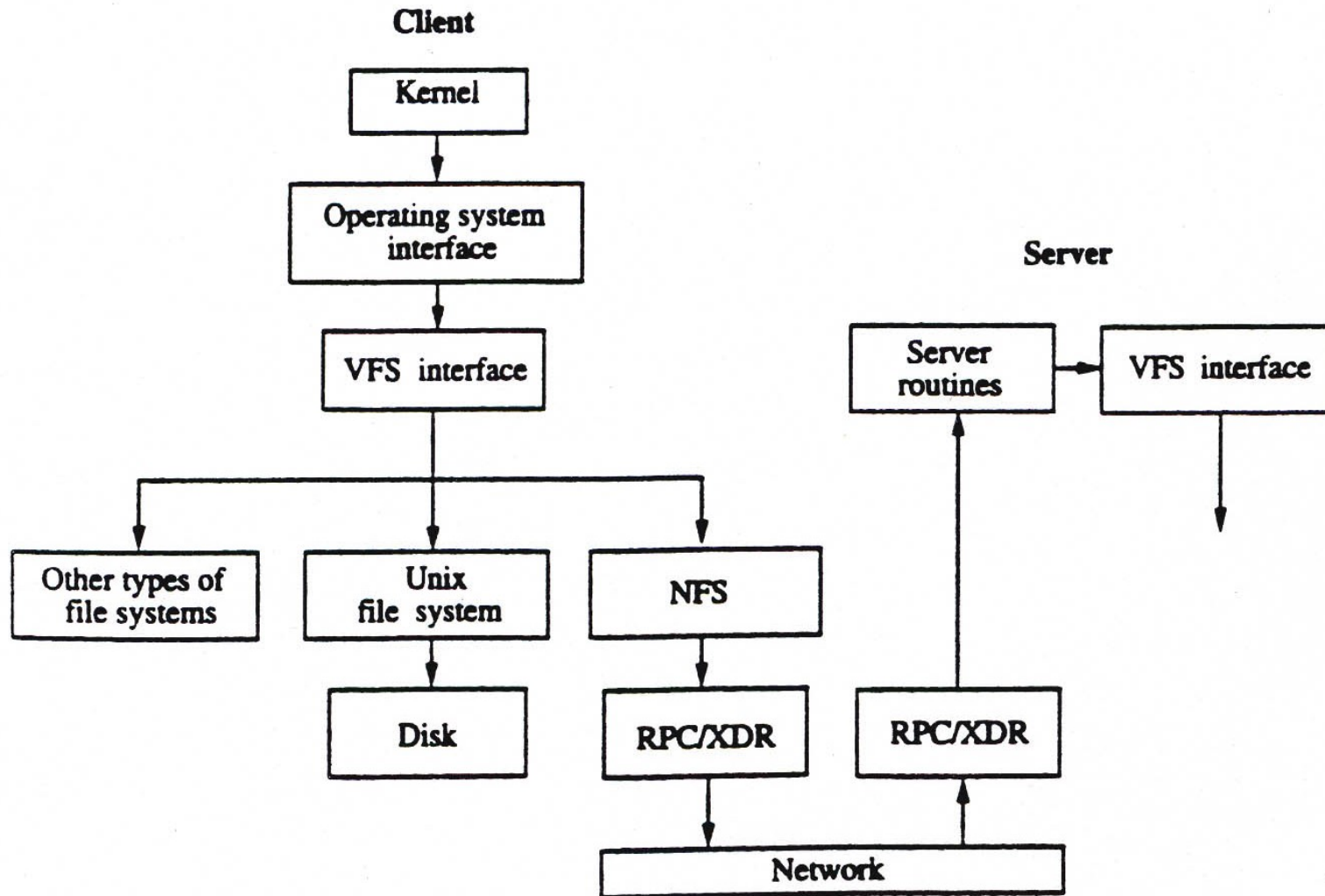
NFS (Cont.)

- Naming and location:
  - Workstations are designated as clients or file servers
  - A client defines its own private file system by mounting a subdirectory of a remote file system on its local file system
  - Each client maintains a table which maps the remote file directories to servers
  - Mapping a filename to an object is done the first time a client references the field. Example:

    Filename: */A/B/C*
    - Assume *'A'* corresponds to *'vnode1'*
    - Look up on *'vnode1/B'* returns *'vnode2'* for *'B'* where *'vnode2'* indicates that object is on server *'X'*
    - Client asks server *'X'* to lookup *'vnode2/C'*
    - *'file handle'* returned to client by server storing that file
    - Client uses *'file handle'* for all subsequent operation on that file

NFS (Cont.)

- **Caching:**
  - Caching done in main memory of clients
  - Caching done for: file blocks, translation of filenames to *vnodes*, and attributes of files and directories

(1) Caching of file blocks
  - Cached on demand with time stamp of the file (when last modified on the server)
  - Entire file cached, if under certain size, with timestamp when last modified
  - After certain age, blocks have to be validated with server
  - Delayed writing policy: Modified blocks flushed to the server after certain delay

(2) Caching of filenames to *vnodes* for remote directory names
  - Speeds up the lookup procedure

(3) Caching of file and directory attributes
  - Updated when new attributes received from the server, discarded after certain time

- **Stateless Server**
  - Servers are stateless
    - File access requests from clients contain all needed information (pointer position, etc)
    - Servers have no record of past requests
  - Simple recovery from crashes.