Course Contents:
Operating System: 150 Marks paper   100 T 50 P

Part 1   General Operating System
Part 2   Windows 2008
Part 3   Linux

Part 1 General Operating System

Q   What is an Operating System?

Ans: **An operating system is a layer of interface between user and computer that is used to manage computer resources.**

OR

           An operating system is a collection of programs that controls and coordinates the overall operation of a computer system.
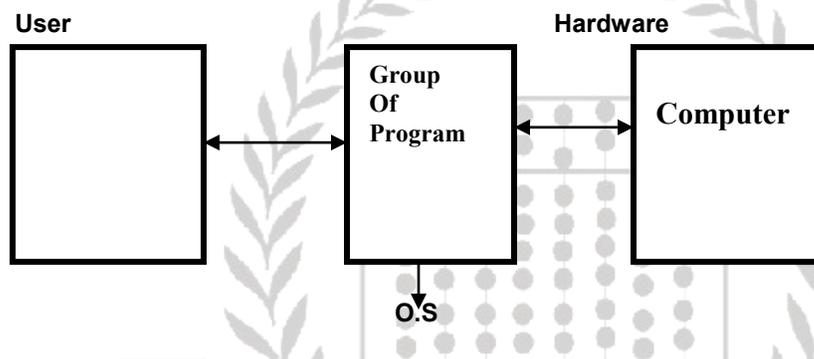
           Operating system is the most basic program within the compute system .These programs act as an interface between the hardware, application programs, files and user. In other words we can say that an operating system is a communication link between user and computer and help the user to run the application programs. The operating system manages the computer resources such as CPU, memory and I/O   devices.

Operating system loaded automatically in RAM when computer is turned on.

Commonly used operating system are Unix, DOS and Windows (Windows 95,98, ME, NT, 2000, XP).

COMPONENTS OF OPERATING SYSTEM:-

           Operating system is not a single program but It is a group of programs that make it a complete software.
Following are the main components of operating system:

  1.   Control Programs
  2.   System Service Programs
  3.   Utilities

  1.   Control Program:-
           This group contains the most basic routines that are essential for the initialization and control of computer operations.
 This group consists of three major modules:
  1.   IPL(Initial Program Loader)
  2.   Supervisor
  3.   Job Controller

  2.   System Service Programs:-

This group includes modules that support supervisor in performing different tasks like I/O management ,loading of programs and secondary storage media management. It is divided into further three modules:

1.   **Librarian**
2.   **I/O Programs**
3.   **Linkage Editor**

    3.   <u>**Utility Programs:-**</u>

This group contains the different external utilities supplied with the Operating system to enhance its capabilities. These are not the integral part of operating system.

Q   What are the different functions of operating system?

Ans   Operating System not only manages all resources of computer but also successfully executes application programs. In this regard operating system performs following different management functions.

Convenient I/O Management:-
                I/O unit consists of mechanical components and electronic components. Operating system must have routines to access, manage and handle these I/O devices.

Process Management:-
                A program in execution is called process. It is one of the important duties of operating system to run and execute the program.

- ✓ The operating system is responsible for the following activities in connection with process management:
- ✓ Creating and deleting both user and system processes
- ✓ Suspending and resuming processes
- ✓ Providing mechanisms for process synchronization
- ✓ Providing mechanisms for process communication
- ✓ Provide mechanism for Deadlock handling.

3. Multi-access System:-
      Allowing several users to use the computer simultaneously is called multi-access system. This gives the facility to programmers that the some CPU can be used by more than one user at the same time.
      The operating system processes the job one by one according to the priority.

4. Memory Management:-
      Memory means primary memory. Memory is an important resource that must be carefully managed. The way through which memory be allocated organized and reallocated from each process is called memory management.
    It is the responsibility of operating system to load programs in memory successfully.

- ✓ Keeping track of which parts of memory are currently being used and by whom
- ✓ Deciding which processes (or parts thereof) and data to move into and out of memory.
- ✓ Allocating and De allocating memory space as and when needed.
- ✓ OS provides uniform, logical view of information storage
- ✓ Abstracts physical properties to logical storage unit - File
- ✓ Each medium is controlled by device (i. e. disk drive,tape drive)

5. Storage Management:-
      In storage management we deals with secondary storage i-e Hard disk etc. An operating system is said to be more efficient one if it uses computer storage resources more efficiently and provide speedy processing.

- ✓ Free- space management
- ✓ Storage allocation
- ✓ Disk scheduling
- ✓ Some storage need not be fast
- ✓ Tertiary storage includes optical storage,
- ✓ magnetic tape Still must be managed
- ✓ Varies between WORM (write-once, read- many- times) and RW (read- write)

6.   File Management:-
     File management is most important issue because the date is the most important resource from the user point of view. The modules of operating system are responsible for efficient management of life.

1.   Communication Management:-

     Communication means method of Transmission of data when data is send from one to another. Operating system is responsible for:

- ✓ **Protocol Management**
- ✓ **Administration Management**
- ✓ **User Management**

8. Network Management:-
          Network is the environment in which two or more computers are connected to each other with communication media. The typical functions of operating system in network management are to guarantee successful transmission of data.

9. Security:

- ✓ **Defense of the system against internal and external attacks Huge range, including denial- of-service, worms, viruses, identity theft, theft of service.**
- ✓ **Systems generally first distinguish among users, to determine who can do what**
- ✓ **User identities (user Ids , security IDs) include name and associated number, one per user User ID then associated with all files, processes of that user to determine access control.**
- ✓ **Group identifier (group ID) allows set of users to be defined and controls managed, then also associated with each process, file**

Q What are different types of operating system?

          The operating system is classified as:

1.   **General Purpose Operating System**
2.   **Special Purpose Operating System**

General Purpose Operating System:-

          The general purpose operating system may be further Classified into the following types:
Single User Operating System
Multi User Operating System

i.   Single User Operating System:-

    The single user operating system usually a single processor and only one user can utilize their resources for processing.e.g: Ms Dos this operating system can run only one program at a time and hence also called single task system. These systems run on micro computer.

ii.   Multi User Operating System:-
               The systems in which several users are allowed to use the   Computer simultaneously are called multi user operating system. Thus   this system supports a number of users simultaneously. These systems are usually designed for mini and main frames computers.

- ▪ **Multi user operating system includes:**
- ▪ **Multi Tasking Operating System**
- ▪ **Time Sharing Operating System**
- ▪ **Multi Processing Operating System**

2. Special Purpose Operating System:-

The system used for special purposes are called special Purpose operating system.

1. **Batch Operating System**
2. **Interactive Processing System**
3. **Real Time Operating System**
4. **Database Operating System**
5. **Transaction Operating System**
6. **Network Operating System**
7. **On line Operating System**
8. **Graphical Operating System**

Q. 4 Define and explain the following terms:

1.   **Multitasking**
2.   **Multiprogramming**
3.   **Multiprocessing**
4.   **Multithreading**
5.   **Multi-user.**

MULTITASKING:-

Multitasking means executing more than one program concurrently. Earlier microcomputer could do only single tasking, whereby an OS could run only one application program at a time. Thus users could have to shutdown the application program they were working in before they opened another application. Today, multitasking operating system are used.

Multitasking is the execution of two or more programs by one user concurrently on the same computer with one central processor.

DOS is a mono tasking operating system as compared to Windows which can handle multiple tasks at the same time.

MULTIPROGRAMMING:-

Multiprogramming means concurrent execution different users programs. Multiprogramming is the execution of two or more programs on a multi user operating system. Multiprogramming improves the efficiency of computer system.

MULTIPROCESSING:-

Multiprocessing means simultaneous processing of two or more programs by multiple processors. In multiprocessing, processing is done by two or more processors.

Multiprocessing is can be done in severed ways. One way to perform multiprocessing is by parallel processing. Multiprocessing systems are more reliable and efficient in work as compared to single processor operating system. Windows and Linux are the examples of multiprocessing systems.

Multi-Threading:

Multi-Threading is the ability of a CPU to execute several threads of execution apparently at the same time. CPUs are very fast at executing instructions. Modern PCs can execute nearly a billion instructions every second. Instead of running the same program for one second, the CPU will run one program for perhaps a few hundred microseconds then switch to another and run it for a short while and so on.

It's also possible for a program to have multiple parts that run at the same time (or appear to!). For example a background task could be responding to mouse input while a file is loaded into RAM and another task updates a progress bar on screen.

Multi-User Operating System:

A multi-user Operating system is a system with an operating system that supports multiple users at once and/or different times. There is also a single user operating system like DOS, only one user can work on this system at the same time. On the other hand system likes windows and Linux, UNIX multiple users can work on the same system by using network clients.

Q5. What is Scheduling and what are the types of Scheduling?

SCHEDULING:-

Scheduling is a purpose of assigning priorities to all active processes. The objective of scheduling is to allocate all resources efficiently. Scheduler is subprogram of operating which perform the function of scheduling.

Scheduler specifically performs two jobs.
1. It assigns priorities to jobs.
2. It allocates resources to active jobs.

In timesharing environment, we use a single CPU and different jobs are then processed on the same CPU one by one. Every job is given some CPU time for their processing. This sharing of CPU time is called scheduling.

We can thus explain scheduling by considering the multiprogramming computer system, where several will be competing for the use of processor. At any instant only one process will be running while the others will be ready waiting for the processor. Operating system has the task of assigning priorities to all active jobs. This activity is called scheduling.

Non-Preemptive Vs Preemptive Scheduling

- ***Non-Preemptive:***

Non-preemptive algorithms are designed so that once a process enters the running state (is allowed a process), it is not removed from the processor until it has completed its service time (or it explicitly yields the processor).

- ***Preemptive:***

Preemptive algorithms are driven by the notion of prioritized computation. The process with the highest priority should always be the one currently using the processor. If a process is currently using the processor and a new process with a higher priority enters, the ready list, the process on the processor should be removed and returned to the ready list until it is once again the highest-priority process in the system.

Goals for Scheduling:

Make sure your scheduling strategy is good enough with the following criteria:

- Utilization/Efficiency: keep the CPU busy 100% of the time with useful work
- Throughput: maximize the number of jobs processed per hour.
- Turnaround time: from the time of submission to the time of completion, minimize the time batch users must wait for output
- Waiting time: Sum of times spent in ready queue - Minimize this
- Response Time: time from submission till the first response is produced, minimize response time for interactive users
- Fairness: make sure each process gets a fair share of the CPU

Types of Scheduling Algorithms:

1. FCFS (First Come First Serve)
2. LCFS (Last Come First Serve)
3. SJF (Shortest Job First)

4. SJN (Shortest Job Next)
5. Priority
6. Round Robin

Scheduling algorithms deals with the problem of deciding which of the processes in ready queue is to be allocated CPU. Following are different scheduling algorithms.
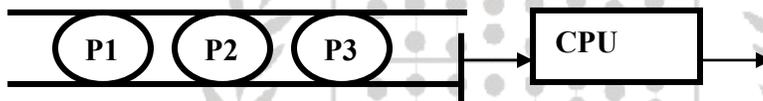
1 . FCFS:-

FIFO stands for first in first out.
In this algorithm all the coming jobs are put into a sequence on the basis of first come first served. The jobs are then taken to CPU one by one. The last coming job is then processed last.

Suppose

P1   enters   at   2:15am
P2   enters   at   2:25am
P3   enters   at   2:50am

So, the process will be arranged as:

Smaller processes arrived later than longer process will wait for very long time.

2. LCFS:-

LIFO stands for last in first out.
In this scheduling strategy, the priority list of jobs is made on the basis of last in first served.
When the job list is made, the job lying at the last of priority list sent to CPU for processing.

Suppose,

P1 enters at 2:15 am
        P2 enters at 2:25 am
        P3 enters at 2:50 am

So, the process will be arranged as:

3. SJF:-

SJF stands for shortest job first.
The scheduling is based upon the memory requirement of process. In this strategy all the incoming jobs are arranged according to their size from smaller to larger. The process having smallest size is assigned higher priority.

Suppose

The size of P1 is 4 kb
The size of P2 is 2 kb
The size of P3 is 1 kb
The size of P4 is 3 kb

so, the process are arranged as:

```
P1  P4  P2  P3          → CPU    t →
```

4. SJN:-

SJN stands for shortest job next.
In this scheduling strategy, process is arranged on the basis of short job first. The first job is then taken to CPU for processing. Now, if a new process comes during the processing of a job the execution of the current job is stopped and it is checked whether the execution time of just coming job is less then the remaining execution time of the currently processing job. If it is so, the currently processing job is placed in a register incompletely and the new coming job is processed first.

On the other hand, if the execution time of the new job is greater than the remaining execution time of the current process, then the new coming job will be placed in the priority queue. The newly coming job is placed in the queue on the basis of shortest job first.

5. Priority:

In Priority scheduling each process is assigned a priority, and whether process comes first or last, it will be processed according to its priority given.

6. RR:-

RR stands for Round Robin.
 In this scheduling processes are dispatched to CPU in FIFO manner but are given a limited CPU time called a time slice. If a process is not completed in this time slice, the CPU is pre empted and given to the next waiting process. The pre empted process then placed at the back of the ready queue.

```
A  C  B  A       → CPU  → Exit
   Time Out
```

What is a Deadlock?

A deadlock is a situation in which two or more competing actions are each waiting for the other to finish, and thus neither ever does.

In an operating system, a deadlock is a situation which occurs when a process enters a waiting state because a resource requested by it is being held by another waiting process, which in turn is waiting for another resource. If a process is unable to change its state indefinitely because the resources requested by it are being used by other waiting process, then the system is said to be in a deadlock.

Deadlock is a common problem in multiprocessing systems, parallel computing and distributed systems, where software and hardware locks are used to handle shared resources and implement process synchronization.

NECESSARY CONDITIONS:

ALL of these four **must** happen simultaneously for a deadlock to occur:

DEADLOCK CHARACTERISATION

Mutual exclusion

One or more than one resource must be held by a process in a non-sharable (Exclusive) mode.

Hold and Wait

A process holds a resource while waiting for another resource.

No Preemption

There is only voluntary release of a resource - nobody else can make a process give up a resource.

Circular Wait

Process A waits for Process B waits for Process C .... waits for Process A.

What is Memory Management Unit in operating system?

Memory management is the process of managing the computer memory which consist of primary memory or secondary memory. In this, we allocate the memory portions to programs and software's after freeing the space of the computer memory. Basically, memory management is of critical importance for operating system because the multi-tasking can take place in the system which switches the memory space from one process to another. Moreover, the concept of the virtual memory is used in the system according to which programs from main memory are loaded to the secondary memory when the space is not large enough to hold the programs.
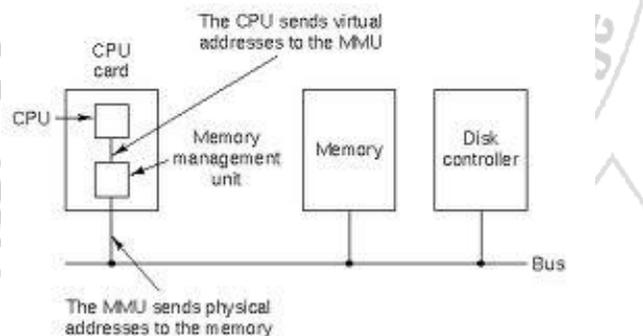
The Disk swapping is used in which virtual memory separates the memory addresses using the physical addresses. The management of the virtual memory is carried out in computer system which will enhance the performance of the system by collecting the garbage database which is meant for allocation and deallocation of resources. As this garbage collection table is implemented in the programming structures that uses the region based management for the objects.

What is the role of the operating system in memory management unit?

The concept of virtual memory is derived from this memory management unit because it provides the loader tool which loads the data from the secondary memory in main memory when required. There are so many benefits provided by this memory management system like multi-tasking of the programs in memory and many more. Many of the features of memory management unit are given below that describes the role of it in operating system.

Every program for its execution requires some space in computer memory which is provided by memory management unit using virtual memory that provides the external storage addressing location for the Programs that does not have too much space in main memory for their execution and saved them in secondary memory but when required loaded them again in main memory. This deallocation and reallocation of programs in main memory deals with concurrency. At last, we say that loading capabilities of programs with the memory addressing is there in it.

The data which we are using in our computer is kept in the secondary storage medium that stores the data permanently in computer memory because it is non volatile in nature and protection of the stored data in memory is provided by the memory management unit such that it will automatically repair and fix the errors there in the bad tracks and sectors. Moreover, as far as the data security is concerned then certain programs are protected with the master password that cannot allow the access of the data without the administrator confirmation. Moreover, certain programs are provided with the shell that protects them from malicious matter.

The data is organized in the well defined manner that provides the easier access of data to the user because sharing is used in which various processes shares the memory with each other using the inter process communication that allows the inter communication between the shared processes and the data stored in memory uses the logical and physical organization in which data are divided into modules that leads to internal and external fragmentation of the main memory such that main memory frames are divided into modules for the programs allocation that is known segmentation.

What is difference between process and thread?

Process:

1. An executing instance of a program is called a process.
2. Some operating systems use the term 'task' to refer to a program that is being executed.
3. A process is always stored in the main memory also termed as the primary memory or random access memory.
4. Therefore, a process is termed as an active entity. It disappears if the machine is rebooted.
5. Several process may be associated with a same program.
6. On a multiprocessor system, multiple processes can be executed in parallel.
7. On a uni-processor system, though true parallelism is not achieved, a process scheduling algorithm is applied and the processor is scheduled to execute each process one at a time yielding an illusion of concurrency.
8. Example: Executing multiple instances of the 'Calculator' program. Each of the instances are termed as a process.

Thread:

1. A thread is a subset of the process.
2. It is termed as a 'lightweight process', since it is similar to a real process but executes within the context of a process and shares the same resources allotted to the process by the kernel (See kquest.co.cc/2010/03/operating-system for more info on the term 'kernel').
3. Usually, a process has only one thread of control – one set of machine instructions executing at a time.
4. A process may also be made up of multiple threads of execution that execute instructions concurrently.
5. Multiple threads of control can exploit the true parallelism possible on multiprocessor systems.
6. On a uni-processor system, a thread scheduling algorithm is applied and the processor is scheduled to run each thread one at a time.
7. All the threads running within a process share the same address space, file descriptor, stack and other process related attributes.
8. Since the threads of a process share the same memory, synchronizing the access to the shared data within the process gains unprecedented importance.

Part-2 Windows 2008 Server

Types of Operating system according to role in a network.

1. **Server Side Operating System**
2. **Client Side Operating System (Desktop operating systems)**

1. Server Side Operating System

All those operating systems which act like a server in a network. Examples are Windows NT server.

1) **Windows 2000 Server**
2) **Windows 2003 Server**
3) **Windows 2008 Server**
4) **Linux Server**
5) **Unix Server**

2. Client Side Operating System:

These are the operating systems which act like a client in a network.

Examples are.

1) **Windows 95**
2) **Windows 98**
3) **Windows ME**
4) **Windows NT workstation**
5) **Windows 2000 professional**
6) **Windows XP**
7) **Windows Vista**
8) **Linux Client**
9) **Unix Client**

Windows 2008:

 Windows 2008 is a multipurpose operating system with integrated support for client / server and peer to peer networks. The windows 2000 family of product has been designed to increase reliability deliver higher levels of system availability and provide for scalability. Windows 2000 incorporates comprehensive internet and application support. Windows 2008 platform provide administrators with more control over their networks and client / server infrastructure**.**

Microsoft is releasing four editions of windows 2008.

1) windows 2000 professional
2) windows 2008 server
3) windows 2008 advanced server
4) windows 2008 data centre server

Windows 2000 professional:-

Windows 2000 professional is the main Microsoft desktop operating system for business of all sizes.
 It incorporates the best business features of windows 98 and build the traditional strengths of windows NT.

Windows 2008 server:-

Windows 2008 server is a file, print and application server as well as web based platform and contains all the features of windows 2008 professional plus many new server specific features, windows 2008 server is ideal for small to medium sized enterprise application development.

Windows 2008 Advanced server:-

Windows 2008 advanced server is a powerful departmental and application server operating system that includes the full features of windows 2008 server and adds the advanced high availability and improved scalability.

Windows data centre server:-

Windows 2008 data centre server is a specialized high end version of windows 2008 server, designed for large scale enterprise. Windows 2008 data centre server is optimized for large data warehouse. It is also ideal for large seal internet server providers (ISPs) and website hosting.

FEATURES OF WINDOWS 2008

Following are the some important features of windows 2008

1. Virtualization

Although it will not be available with the initial launch of Server 2008, Microsoft's Hyper-V hypervisor-based virtualization technology promises to be a star attraction of Server 2008 for many organizations.

Although some 75 percent of large businesses have started using virtualization, only an estimated 10 percent of servers out are running virtual machines. This means the market is still immature. For Windows shops, virtualization using Server 2008 will be a relatively low-cost and low-risk way to dip a toe in the water.

At the moment, Hyper-V lacks the virtualized infrastructure support virtualization market leader VMware can provide. Roy Illsley, senior research analyst at U.K.-based Butler Group, noted that Microsoft is not as far behind as many people seem to think, however. "Don't forget Microsoft's System Center, which is a fully integrated management suite and which includes VM Manager. Obviously it only works in a Wintel environment, but if you have Server 2008 and System Center, you have a pretty compelling proposition.

"What Microsoft is doing by embedding virtualization technology in Server 2008 is a bit like embedding Internet Explorer into Windows," said Illsley. "This is an obvious attempt to get a foothold into the virtualization market."

At launch, Microsoft is unlikely to have a similar product to VMware's highly popular VMotion (which enables administrators to move virtual machines from one physical server to another while they are running), but such a product is bound to available soon after.

2. Server Core

Many server administrators, especially those used to working in a Linux environment, instinctively dislike having to install a large, feature-packed operating system to run a particular specialized server. Server 2008 offers a Server Core installation, which provides the minimum installation required to carry out a specific server role, such as for a DHCP, DNS or print server. From a security standpoint, this is attractive. Fewer applications and services on the sever make for a smaller attack surface. In theory, there should also be less maintenance and management with fewer patches to install, and the whole server could take up as little as 3Gb of disk space according to Microsoft. This comes at a price — there's no upgrade path back to a "normal" version of Server 2008 short of a reinstall. In fact there is no GUI at all — everything is done from the command line.

3. IIS

IIS 7, the Web server bundled with Server 2008, is a big upgrade from the previous version. "There are significant changes in terms of security and the overall implementation which make this version very attractive," said Barb Goldworm, president and chief analyst at Boulder, Colorado-based Focus Consulting. One new feature getting a lot of attention is the ability to delegate administration of servers (and sites) to site admins while restricting their privileges.

4. Role-based installation

Role-based installation is a less extreme version of Server Core. Although it was included in 2003, it is far more comprehensive in this version. The concept is that rather than configuring a full server install for a particular role by uninstalling unnecessary components (and installing needed extras), you simply specify the role the server is to play, and Windows will install what's necessary — nothing more. This makes it easy for anyone to provision a particular server without increasing the attack surface by including unwanted components that will not do anything except present a security risk.

5. Read Only Domain Controllers (RODC)

It's hardly news that branch offices often lack skilled IT staff to administer their servers, but they also face another, less talked about problem. While corporate data centers are often physically secured, servers at branch offices rarely have the same physical security protecting them. This makes them a convenient launch pad for attacks back to the main corporate servers. RODC provides a way to make an Active Directory database read-only. Thus, any mischief carried out at the branch office cannot propagate its way back to poison the Active Directory system as a whole. It also reduces traffic on WAN links.

Recent Windows Coverage

IIS Takes Modular Approach with Windows Server 2008
Win 2003 High Availability Solutions Series

6. Enhanced terminal services

 Terminal services have been beefed up in Server 2008 in a number of ways. TS RemoteApp enables remote users to access a centralized application (rather than an entire desktop) that appears to be running on the local computer's hard drive. These apps can be accessed via a Web portal or directly by double-clicking on a correctly configured icon on the local machine. TS Gateway secures sessions, which are then tunnelled over https, so users don't need to use a VPN to use Remote Apps securely over the Internet. Local printing has also been made significantly easier.

7. Network Access Protection

Microsoft's system for ensuring that clients connecting to Server 2008 are patched, running a firewall and in compliance with corporate security policies — and that those that are not can be remediated — is useful. However, similar functionality has been and remains available from third parties.

8. Bitlocker

System drive encryption can be a sensible security measure for servers located in remote branch offices or anywhere where the physical security of the server is sub-optimal. Bitlocker encryption protects data if the server is physically removed or booted from removable media into a different operating system that might otherwise give an intruder access to data which is protected in a Windows environment. Again, similar functionality is available from third-party vendors.

9. Windows PowerShell

Microsoft's new(ish) command line shell and scripting language has proved popular with some server administrators, especially those used to working in Linux environments. Included in Server 2008, PowerShell can make some jobs quicker and easier to perform than going through the GUI. Although it might seem like a step backward in terms of user friendly operation, it's one of those features that once you've gotten used to it, you'll never want to give up.

10. Better security

We've already mentioned various security features built into Server 2008, such as the ability to reduce attack surfaces by running minimal installations, and specific features like BitLocker and NAP. Numerous other little touches make Server 2008 more secure than its predecessors. An example is Address Space Load Randomization — a feature also present in Vista — which makes it more difficult for attackers to carry out buffer overflow attacks on a system by

changing the location of various system services each time a system is run. Since many attacks rely on the ability to call particular services by jumping to particular locations, address space randomization can make these attacks much less likely to succeed.

It's clear that with Server 2008 Microsoft is treading the familiar path of adding features to the operating system that third parties have previously been providing as separate products. As far as the core server product is concerned, much is new. Just because some technologies have been available elsewhere doesn't mean they've actually been implemented. Having them as part of the operating system can be very convenient, indeed.

If you're running Server 2003 then, now is the time to start making plans to test Server 2008 — you're almost bound to find something you like. Whether you decide to implement it, and when, is up to you**.**

Architecture of Windows 2008:

The Windows 2008 operating system architecture is a hybrid architecture that is comprised of client/server, layered, object-oriented, and symmetric multiprocessing architecture principles.
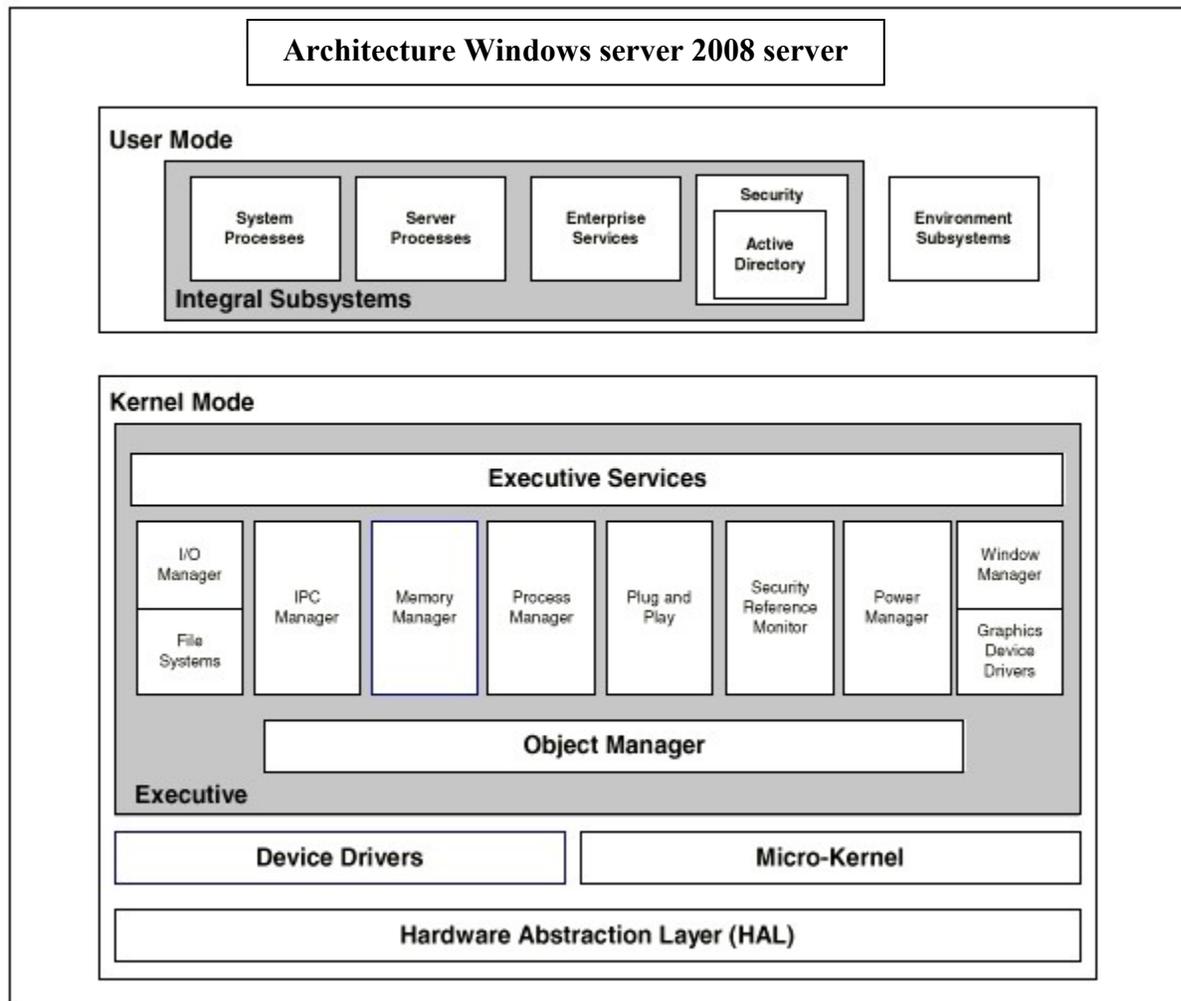
- **Executive:**

Contains components that implement memory management, process and thread management, security, I/O, interprocess communication, and other base operating system services. For the most part, these components interact with one another in a modular, layered fashion.

- **Microkernel:**

The Microkernel's primary functions are to provide multiprocessor synchronization, thread and interrupt scheduling and dispatching, and trap handling and exception dispatching. During system startup, it extracts information from the Registry, such as which device drivers to load and in what order.

- **Hardware Abstraction Layer (HAL):**

The HAL is the code associated with Windows 2008 that changes with the hardware the operating system is being run on. Thus, it becomes compatible with multiple processor platforms. The HAL manipulates the hardware directly.

- **Device drivers:**

Device drivers send and receive load parameters and configuration data from the Registry.

- **Windowing and graphics system:**

This system implements the graphical user interface (GUI).

File System:

What's FAT?
What About VFAT?
FAT32
What's NTFS?
　　Compatibility
　　Volume Size
　　Fault Tolerance
　　Security
　　File Compression
The System Partition
Converting to NTFS
Converting to FAT32

What's FAT?

　　FAT may sound like a strange name for a file system, but it's actually an acronym for File Allocation Table. Introduced in 1981, FAT is ancient in computer terms. Because of its age, most operating systems, including Microsoft Windows NT®, Windows 98, the Macintosh OS, and some versions of UNIX, offer support for FAT.

The FAT file system limits filenames to the 8.3 naming convention, meaning that a filename can have no more than eight characters before the period and no more than three after. Filenames in a FAT file system must also begin with a letter or number, and they can't contain spaces. Filenames aren't case sensitive.

What about VFAT?

VFAT is an extension of the FAT file system and was introduced with Windows 95. VFAT maintains backward compatibility with FAT but relaxes the rules. For example, VFAT filenames can contain up to 255 characters, spaces, and multiple periods. Although VFAT preserves the case of filenames, it's not considered case sensitive.

When you create a long filename (longer than 8.3) with VFAT, the file system actually creates two different filenames. One is the actual long filename. This name is visible to Windows 95, Windows 98, and Windows NT (4.0 and later). The second filename is called an MS-DOS® alias. An MS-DOS alias is an abbreviated form of the long filename. The file system creates the MS-DOS alias by taking the first six characters of the long filename (not counting spaces), followed by the tilde [~] and a numeric trailer. For example, the filename Brien's Document.txt would have an alias of BRIEN'~1.txt.

FAT32

FAT32 is actually an extension of FAT and VFAT, first introduced with Windows 95 OEM Service Release 2 (OSR2). FAT32 greatly enhances the VFAT file system but it does have its drawbacks.

The greatest advantage to FAT32 is that it dramatically increases the amount of free hard disk space. To illustrate this point, consider that a FAT partition (also known as a FAT16 partition) allows only a certain number of clusters per partition. Therefore, as your partition size increases, the cluster size must also increase. For example, a 512-MB FAT partition has a cluster size of 8K, while a 2-GB partition has a cluster size of 32K.

This may not sound like a big deal until you consider that the FAT file system only works in single cluster increments. For example, on a 2-GB partition, a 1-byte file will occupy the entire cluster, thereby consuming 32K, or roughly 32,000 times the amount of space that the file should consume. This rule applies to every file on your hard disk, so you can see how much space can be wasted.

Converting a partition to FAT32 reduces the cluster size (and overcomes the 2-GB partition size limit). For partitions 8 GB and smaller, the cluster size is reduced to a mere 4K. As you can imagine, it's not uncommon to gain back hundreds of megabytes by converting a partition to FAT32, especially if the partition contains a lot of small files.

As I mentioned, FAT32 does have limitations. Unfortunately, it isn't compatible with any operating system other than Windows 98 and the OSR2 version of Windows 95. However, Windows 2008 will be able to read FAT32 partitions. The other disadvantage is that your disk utilities and antivirus software must be FAT32-aware. Otherwise, they could interpret the new file structure as an error and try to correct it, thus destroying data in the process.

Note: FAT32 can't be converted to FAT16 file system.

What's NTFS?

Now that I've discussed the FAT, VFAT, and FAT32 file systems, let's examine the NTFS file system. NTFS stands for New Technology File System. Microsoft created NTFS to compensate for the features it felt FAT was lacking. These features include such things as increased fault tolerance and enhanced security. Now that you know a little about these file systems, let's compare how each performs in various situations.

Compatibility

Before you decide what type of file system to use on a partition, you should consider compatibility. If multiple operating systems will access the partition, you must use a file system that all operating systems can read. Usually, this means using FAT because of its universal compatibility. Only Windows NT supports NTFS partitions.

Keep in mind, however, that this limitation only applies to the local machine. For example, if you have Windows NT and Windows 98 loaded on the same machine and both operating systems require access to a common partition, you must format that partition as FAT. However, if Windows NT is the only operating system on the PC, you can format the partition as NTFS, even if computers running other operating systems will access the partition across the network.

Volume Size

Another determining factor in your decision is the physical size of your partition. FAT only supports partition sizes up to 2 GB. If your partition size is larger than 2 GB, you must format it as FAT32 or NTFS, or you must break it into smaller partitions. You should also keep in mind that because of the enhanced features associated with NTFS, NTFS has more overhead than FAT. If your partition size is smaller than 200 MB, you should use FAT to avoid losing a large amount of disk space to the overhead associated with NTFS. The maximum size of an NTFS partition is 16 exabytes.

Comparison between NTFS and FAT

NTFS	FAT 16/32
• Default File system In Windows XP, 2k and NT	• Fat 16 not compatible with XP, FAT is more compatible with other operating Systems (Windows 95, etc)
• Support For Drives over 40gb, Files over GB	
• Allows extended file names, foreign characters	• FAT 16 has 8.3 character limitation
• Has a severely crippled maintenance system in chkdsk	• Has better, more and interactive recovery utilities (scandisk)
• Chkdsk is notoriously slow	• Scandisk is very quick
• Increased security with file encryption	• Just a space for the OS to read files
• Smaller file clusters, 4kb	• Faster on drives less than 10gb
• Compression to reduce disk space	• FAT 16 cluster size is 32kb
• User permissions for files and folders	• Cluster chains containing data from interrupted copies are marked as damaged
• File copies are "undone" if interrupted, cluster chains is cleaned	• Master File Table are separate from files
• Small files are kept in Master File Table at the beginning of the drive	
• Not compatible with different operating systems on the same computer	

Some Random Facts

1. Fat 16 was developed in 1981 for dos
2. Fat 16 was designed to handle floppies
3. Fat 32 is an extension of Fat 16
4. Fat 32 introduced in service pack 2 of Windows 95
5. Operating systems may recognize Fat16, but not Fat 32 (Win NT)
6. You can go from FAT to NTFS but not the other way around
7. FAT = File Allocation Table
8. NTFS = New Technology File System

Well, Which One Should I Choose?

1. If you really only want to choose one way or another, here are two very important considerations:
2. For files above 4gb, and hard disks above 32gb, go for NTFS
3. For smaller drives, files and better recovery tools go for FAT
4. But why not go for both, which is the best option in my opinion.
5. Set aside some FAT so that you can run recovery tools, especially scandisk, so that you have something usable when things go awry, instead of the awful Windows System Tools.
6. Then set the rest to NTFS so that you have better security on personal files, support for large files and drive.

Fault Tolerance

Once you've considered your partition size and compatibility issues, you've got some flexibility in determining which file system is right for you. One issue to consider when making this decision is fault tolerance. Windows NT offers software support for several alternate disk access methods that increase speed and/or fault tolerance. These options include things such as disk striping and disk striping with parity. Many of these options require NTFS. If you're planning on using a hardware-based stripe set, you can use either file system.

Even without these advanced fault-tolerant options, NTFS includes built-in fault-tolerant capabilities well beyond the capabilities of FAT or FAT32. For example, when NTFS writes a change to the hard disk, it makes a record of the change in a log file. In the event of a power failure or a disk error, Windows NT can use these log files to repair your data.

NTFS also repairs hard disk errors automatically without displaying an error message. When Windows NT writes a file to an NTFS partition, it keeps a copy of the file in memory. It then reads back the file to make sure it matches the copy stored in memory. If the copies don't match, Windows NT marks that section of the hard disk as bad and won't try to use it again. It then uses the copy of the file stored in memory to rewrite the file to an alternate location on the hard disk.

The FAT and FAT32 file systems don't offer any of these safety features. While FAT and FAT32 do maintain two different copies of the file allocation table in case one copy is damaged, these systems are incapable of automatically fixing errors. Instead, you must run a utility such as ScanDisk.

Security

As I mentioned before, NTFS has its own built-in security system. You can grant various permissions to directories and to individual files. These permissions protect files and directories locally and remotely. For example, if someone were to try to access the restricted files, NTFS would protect those files.

If you're using FAT or FAT32, you depend on share permissions for security. Share permissions will protect a file across the network, but they offer no local protection. A person trying to access restricted files could simply sit at the local PC and gain full access to these files. Another disadvantage to share permissions is that they can be messy to manage. If you have hundreds of users on a server, each with his or her own directories, you could potentially end up with hundreds of shares, some of which may overlap, thus creating additional complications.

File Compression

Another advantage to NTFS is native support for file compression. If you ever used the compression program that came with MS-DOS 6.22, you may be groaning right now. As you may recall, the MS-DOS compression utility required you to compress your entire partition. The compression process took a long time and, when completed, drastically slowed your PC's file access. Another disadvantage was that a minor disk problem could potentially trash the entire partition. FAT32, on the other hand, offers no compression capabilities at all.

The NTFS compression is much better than its predecessors. It offers you the chance to compress individual files and directories of your choice. Because it compresses individual files, if you have a minor hard disk problem, it won't screw up your compression scheme and make you lose everything. Another advantage to compressing individual files and directories is that you can compress only seldom-used files. By doing so, you won't slow down your operating system by making it decompress files each time it needs to access them.

The System Partition

After reading this article, you may have decided that NTFS is far superior to FAT and FAT32. In most cases, if you're using Windows NT, you should use NTFS. However, this isn't always the case.

As I mentioned, NTFS partitions are only accessible via Windows NT. If you have a fatal error with Windows NT, you can't simply boot a system disk to a command prompt and fix a problem on an NTFS partition. To get around this problem, Microsoft recommends installing a second copy of Windows NT on your hard disk and using this copy to repair problems that occur on NTFS partitions.

Unfortunately, this method has some serious drawbacks. For starters, a second copy of Windows NT could consume up to 150 MB depending on which options you choose to load. Second, during the boot process, both copies share common files. Therefore, if your system partition (the partition your PC boots from) is formatted as NTFS and has a problem, you may not be able to boot either copy of Windows NT to fix the problem. While you may think the odds of a system partition error may be slim, just remember that many of the changes you may make to your disk partitions result in having to manually update the Boot.ini file. If you incorrectly update this file, Windows NT will become unbootable. Because this is an initial boot file on the system partition, every installed copy of Windows NT would share this file.

A better solution is to format your system partition as FAT. If you're concerned about security, simply make the system partition small and don't place anything other than the Windows NT system files on **it.**

Remember: a FAT partition is safe from a security standpoint, as long as no unauthorized person has physical access to the machine.

Converting to NTFS

If you're running Windows NT and want to use NTFS on some of your partitions that already contain data, you can easily convert a partition to NTFS. To do so, open an MS-DOS prompt window and type the following command:

CONVERT drive: /FS:NTFS

For example, if you wanted to convert your D drive to NTFS, you'd replace the word drive with the letter D, as shown below:

CONVERT D: /FS:NTFS

Converting to FAT32

Converting to FAT32 is even easier than converting to NTFS. To convert a FAT partition to FAT32 (within Windows 98), simply click **Start** and go to **Program Files**, **Accessories**, **System Tools**, **Drive Converter (FAT32)**. When you do, you'll see a wizard that will allow you to select the partition you wish to convert and begin the conversion process. Before you convert a partition, however, remember that on older systems or systems with very full drives, this process can take several hours.

WINDOWS 2008 NETWORKS:-

Windows 2008 supports secure network environment in which use users are able to share common resources, regardless of network size.

There are two types of network that windows 2008 supports.
  a. Workgroup
  b. Domain

A) windows 2008 workgroup:-

A windows 2008 workgroup is referred to as peer to peer network because all computer in the workgroup can share resources as equals with out a dedicated server. Each computer in the workgroup maintains a local security database. A local security database is a list of user accounts and resource security information. Therefore the administration of user accounts and resources security is a workgroup is decentralized.

Advantages:-

  a. it does require a computer running windows 2008 server to hold centralized security information.
  b. It is simple to design and implement a workgroup

B)   windows 2008 domain:-

 A windows 2008 domain is logical grouping of network computer that share a central directory database. A directory database contains user accounts and the security information for the domain.

In a domain the directory resides on computer that are configured as domain controllers. A domain controller is a server that manages all security related to aspects of domain interaction. Security and information are centralized.

USER ACCOUNTS:-

Windows 2008 provides three different types of user account.
1.   Local user account.
2.   Domain user account.
3.   Built in user account.

1.   Local User Account.

 A local user account allows a user to log on to a specific computer to gain access to resources on that computer.

2.   Domain User Account.

A domain user account allows a user to log on to a domain to gain access to network resources. This account is created on the domain controller and placed on the domain computer.

3.   Built In User Account

A built in user account allows a user to perform administrative task or gain access to local or network resources.

 Two commonly used built in accounts are:
        a) Administrator
        b) Guest

A) Administrator

Use the administrator account to manage the overall computer. If your computer is the part of a domain, use the built in administrator account to manage configuration. Task done by the administrator account include orating and modifying user accounts and groups manage security policies creating printers etc. you can not delete the administrator account.

B) Guest

Use the built in guest account to give occasional user the ability to log on and give access to the resources. The guest account is disabled by default. Enable the guest account only in low security networks and always assign it a password. You can rename the guest account but you can not delete it.

CREATE USER ACCOUNTS:-

You can create the local user account by doing the following step.

1.   Click Start Menu
2.   Go To programs
3.   Select Administrative Tools
4.   Select "Active Directory user and accounts"
5.   Select Domain name in left side tree
6.   Select User and Right Click on it
7.   Select New User from Popup menu
8.   Enter user name and password

9. Click ok
10. User is created

GROUPS:-

A group is a collection of user account.
Group simplifies administration by allowing you to assign permission and rights to a group of user rather having to assign permission to each individual user account. User can be a member of multiple groups. Groups can be a member of other groups.

LOCAL GROUPS:-

A local group is a collection of user account on a computer. A use local group to assign permission to the resources residing on the computer on which the local group is created windows 2008 creates local groups in the local security database. You can not create local groups on domain controller.

CREATING LOCAL GROUPS:-

You can create the local user account by doing the following step.

1. Click Start Menu
2. Go To programs
3. Select Administrative Tools
4. Select "Active Directory user and accounts"
5. Select Domain name in left side tree
6. Select Group and Right Click on it
7. Select New Group from Popup menu
8. Click ok
9. Group is created

Built in local groups:-

Built in local group give rights to perform system tasks on a single computer, such as backing up and restoring files, changing the system time and administering resources.

Following are some built in local groups:

1. Administrator:-

Member can perform all administrator tasks on the computer.

2. Backup Operator:-

Member can use windows backup to back to back up and restore the computer.

3. Guests:

Member can perform only task for which you have specifically granted rights and can gain access only to resources for which you have assigned permission.

4. Power User:-

Member can create and modify local user account on the computer and share resources.

5. Replicator:-

Supports file replication in a domain.

6. User:-

Member can perform only tasks for which you have specifically granted rights and can gain access only to the resources for which you have assigned permission.

7. Auditing:-

Auditing allows you to track both user activities and windows 2008 activities ,which are called events, on a computer. Through auditing you can specify that windows 2008 write a record of an event to the security log:

An audit entry in the security log contains the following information
   a. The action that was performed.
   b. The user who perform the action.
   c. The success or failure of the event and when the event occurred.

8. Audit Policy:

In audit policy defines the types of security events that windows 2008 records in security log on each computer. The security log allows you to track the events that you specify.

The types of events that you can audit include the following:

   a) Accessing files and folders.
   b) Logging on and off.
   c) Shutting down and restarting a computer.
   d) Changing user account and group.
   e) Attempts to make changes to objects in directory services.
   f) After you have determined the types of events to audit, you must also determine whether to audit the success or failure or both.

Making Windows XP/ win 7 Client or adding a client node in Windows 2008 or 2003 Server

   1. Attach Cables to both server and client
   2. Assign valid IP address to both the computers
   3. Create user on the server side
   4. on the client side in win XP Select Properties from my computer
   5. Select "Computer Name tab"
   6. Click on "Change Button"
   7. Select Domain
   8. Enter domain name in text box, like "abacus.com"
   9. Restart computer and login from the user created on server
   10. Client is ready to work with the server machine

PROTOCOL IN WINDOWS 2008:-

TCP/ IP

TCP/IP was developed by the Advanced Research Project Agency (ARPA) of the U.S. Department of Defense. TCP/IP runs on a wide variety of platforms, it is an ideal choice for a routing protocol.

TCP/IP consists of two distinct protocols, the Transmission Control Protocol (TCP) and Internet Protocol) (IP). The TCP operates at the transport layer and the IP operates at the network layer. The IP provide two basic services; breaking the message up into transmission packets and addressing. The IP is also responsible for packet routing. On occasions this requires that the responsible for packet routing. On occasions this requires that the IP to break a message into smaller packets of the appropriate size. To do this, the IP must determine the address of the next node on the path to the messages destination.

The IP is not responsible for guaranteeing end-to-end message delivery. The TCP protocol is held accountable for a message delivery. If a packet is lost during transmission, the TCP is responsible for re-sending the message. Also

the IP does not guarantee that individual packet will arrive in the correct order, a function that is provided by the TCP. Thus the primary functions of the TCP are to provide message integrity, to provide acknowledgement that a complete message had been received by a destination node, and to regulate the flow of message between source and destination nodes.

NetBEUI (NetBIOS Extended User Interface) Protocol.

It is a transport protocol commonly found in smaller networks. NetBEUI is not commonly used in large networks and will become less used in the future because it is not routable protocol with little overhead because of its inability to route packets.

FTP (File Transfer Protocol)

It is a standardized method of transferring files between files between two machines. FTP is a connection-Oriented protocol, which means that the protocol verifies that packets successfully reach their destination.

IPX (Inter-Packet Exchange) Protocol

IPX is the basic protocol used on a NetWare Network. IPX is an externally fast streamlined protocol that is not connection oriented. IPX can be used for Windows NT and Windows 2008 and is fairly common. The Primary responsibility for IPX is the handling of broadcast issues. IPX is a routable protocol that is located in the network layer of the OSI Model.

<u>Administering Volume Sets and RAID Arrays</u>

When you work with Microsoft Windows 2008 servers, you'll often need to perform advanced disk setup procedures, such as creating a volume set or setting up a RAID array. The following are some of the tasks that you can perform with Disk Manager.

- With a *volume set*, you can create a single volume that spans multiple drives. Users can access this volume as if it were a single drive, regardless of how many drives the actual volume is spread over. A volume that is on a single drive is referred to as a *simple* volume. A volume that spans multiple drives is referred to as a *spanned* volume.

- With *RAID arrays*, you can protect important business data and, sometimes, improve the performance of drives. RAID is an acronym for redundant array of independent disks. Windows 2008 supports three different levels of RAID: 0, 1, and 5. you implement RAID arrays as mirrored, striped, and striped with parity volumes.

In Windows 2008, volumes are designed to be used with dynamic disks. If you created volumes under Microsoft Windows NT 4.0, you'll need to upgrade the basic drives containing the volumes to dynamic drives and then manage the volumes as you would any other Windows 2008 volume. If you don't do this, your management options for the volumes are limited.

Volume sets and RAID arrays are created on dynamic drives and are only accessible to Windows 2008 and later. Because of this, if you dual boot a computer to a previous version of Windows, the dynamic drives are unavailable.

However, computers running previous versions of Windows can access the drives over the network—just like any other network drive.

Using Volumes and Volume Sets

You create and manage volumes in much the same way as partitions. A volume is a drive section that can be used to store data directly.

Volume Basics

As Figure 11-1 shows, Disk Management color codes volumes by type, much like partitions. Volumes also have a specific

- Layout Volume layouts include simple, spanned, mirrored, striped, and striped with parity.

- Type Volumes always have the type dynamic.

- File system as with partitions, each volume can have a different file system type, such as FAT (file allocation table), FAT 32, or NTFS (Windows NT file system).

Figure 11-1: Disk Management displays volumes much like partitions.

- Status The state of the drive. For details on drive state, see the section of Chapter 10 entitled "Understanding Drive Status."

- Capacity The total storage size of the drive.

An important advantage of dynamic volumes over basic volumes is your ability to make changes to volumes and drives without having to restart the system (in most cases). Volumes also let you take advantage of the fault tolerance enhancements of Windows 2008. While you can't use dynamic drives with previous versions of Windows, you can install other operating systems and dual boot a Windows 2008 system. To do this, you must create a separate volume for the other operating system. For example, you could install Windows 2008 on volume C and Linux on volume D.

With volumes, you can

- Assign drive letters, as discussed in the section of Chapter 10 entitled "Assigning Drive Letters."

- Assign drive paths, as discussed in the section of Chapter 10 entitled "Assigning Drive Paths."

- Create any number of volumes on a disk as long as you have free space.

- Create volumes that span two or more disks and, if necessary, configure fault tolerance.

- Extend volumes to increase the capacity of the volume.

- Designate Active, System, and Boot volumes, as described in the section of Chapter 10 entitled "Special Considerations for Basic and Dynamic Disks."

Understanding Volume Sets

With volume sets, you can create volumes that span several drives. To do this, you use free space on different drives to create what users see as a single volume. Files are stored on the volume set segment by segment, with the first segment of free space being used first to store files. When this segment fills up, the second segment is used, and so on.

You can create a volume set using free space on up to 32 hard disk drives. The key advantage to volume sets is that they let you tap into unused free space and create a usable file system. The key disadvantage is that if any hard disk drive in the volume set fails, the volume set can no longer be used—which means that essentially all the data on the volume set is lost.

Creating Volumes and Volume Sets

You create volumes and volume sets by completing the following steps:

1. In the Disk Management Graphical view, right-click an area marked Unallocated on a dynamic disk and then chooses Create Volume. This starts the Create Volume Wizard. Read the welcome dialog box and then click Next.

2. As shown in Figure 11-2, select Simple Volume to create a volume on a single disk or Spanned Volume to create a volume set on multiple disks. Simple volumes can be formatted as FAT, FAT 32, or NTFS. To make management easier, you should format volumes that span multiple disks as NTFS. NTFS formatting allows you to expand the volume set, if necessary.

   Note: If you find that you need more space on a volume, you can extend simple and spanned volumes. You do this by selecting an area of free space and adding it to the volume. You can extend a simple volume within the same disk. You can also extend a simple volume onto other disks. When you do this, you create a spanned volume, which must be formatted as NTFS.

3. You should see the Select Disks dialog box shown in Figure 11-3. Use this dialog box to select dynamic disks that are a part of the volume and to size the volume segments on those disks.

4. Available dynamic disks are shown in the All Available Dynamic Disks list box. Select a disk in this list box, and then click Add >> to add the disk to the Selected Dynamic Disks list box. If you make a mistake, you can remove disks from the Selected Dynamic Disks list box by selecting the disk and then clicking <<Remove.

5. Select a disk in the Selected Dynamic Disks list box, and then use the For Selected Disk … MB combo box to specify the size of the volume on the selected disk. The Maximum field shows you the largest area of free space available on the selected disk. The Total Volume Size field shows you the total disk space selected for use with the volume.

Although you can size the volume set any way you want, you may want to take a moment to consider how you'll use volume sets on the current workstation or server. Simple and spanned volumes aren't fault tolerant. Rather than creating one monstrous volume with all the available free space, you may want to create several smaller volumes.

Specify whether you want to assign a drive letter or path. These options are used as follows:

- Assign a Drive Letter to assign a drive letter, choose this option and then select an available drive letter in the selection list provided.

- Mount This Volume to an Empty Folder Those Supports Drive Paths to assign a drive path, choose this option and then type the path to an existing folder or click Browse to search for or create a folder.

- Do Not Assign a Drive Letter or Drive Path to create the volume without assigning a drive letter or path, choose this option. You can assign a drive letter or path later, if necessary.

6. As shown in Figure 11-4, determine whether the volume should be formatted. If you elect to format the volume, follow the steps described in the section of Chapter 10 entitled "Formatting Partitions."

7. Click next, and then click Finish. If you add volumes to a physical drive that contains the Windows 2008 operating system, you may inadvertently change the number of the boot volume. Read the warning prompts and then make any necessary changes to the BOOT.INI file as described in Chapter 10 under "Updating the Boot Disk."

Managing Volumes

You manage volumes much like you manage partitions. You can

- Assign drive letters and paths
- Change or delete volume labels
- Convert a volume to NTFS
- Check a drive for errors and bad sectors
- Defragment disks
- Compress drives and data
- Encrypt drives and data

Follow the techniques outlined in the section of Chapter 10 entitled "Managing Existing Partitions and Drives."

Improved Performance and Fault Tolerance with RAIDs

You'll often want to give important data increased protection from drive failures. To do this, you can use RAID technology to add fault tolerance to your file systems. With RAID 1 you increase data integrity and availability by creating copies of the data. With RAID 5, you increase data integrity by creating a volume with data and parity striped intermittently

across three or more physical disks. You can also use RAID to improve the performance of your disks. However, the data integrity feature is not available with RAID 0.

Different implementations of RAID technology are available. These implementations are described in terms of levels. Currently, the most widely implemented RAID levels are 0, 1, 2, 3, 4, 5, 6, 7, 10, and 53. Each RAID level offers different features. Windows 2008 supports RAID levels 0, 1, and 5.

- Use RAID 0 to improve the performance of your drives. You can also use RAID 0 to gain more space by combining leftover sections on two or more physical drives.

- Use RAID 1 and 5 to provide fault tolerance for data.

Table 11-1 provides a brief overview of the supported RAID levels. This support is completely software-based and is only available on Windows 2008 servers.

Table Windows 2008 Server Support for RAID

RAID Level	RAID Type	Description	Major Advantages
0	Disk striping	Two or more volumes, each on a separate drive, are configured as a stripe set. Data is broken into blocks, called stripes, and then written sequentially to all drives in the stripe set.	Speed/Performance
1	Disk mirroring	Two volumes on two drives are configured identically. Data is written to both drives. If one drive fails, there's no data loss because the other drive contains the data. (Doesn't include disk striping.)	Redundancy. Better write performance than disk striping with parity.
5	Disk striping with parity	Uses three or more volumes, each on a separate drive, to create a stripe set with parity error checking. In the case of failure, data can be recovered.	Fault tolerance with less overhead than mirroring. Better read performance than disk mirroring.

The most common RAID levels in use on Windows 2008 servers are level 1 disk mirroring and level 5 disk striping with parity. Disk mirroring is the least expensive way to increase data protection with redundancy. Here you use two identically sized volumes on two different drives to create a redundant data set. If one of the drives fails, you can still obtain the data from the other drive.

On the other hand, disk striping with parity requires more disks—a minimum of three—but offers fault tolerance with less overhead than disk mirroring. If any of the drives fail, the data can automatically be recovered by combining blocks of data on the remaining disks with a parity record. Parity is a method of error checking that uses a special algorithm to create a value that could be used to recover lost data. You use this parity sector to recover data in case of hard drive failure.

Implementing RAID on Windows 2008 Servers

For server systems, Windows 2008 supports disk mirroring, disk striping, and disk striping with parity. How to implement these RAID techniques is discussed in the sections that follow.

Note: Some operating systems, such as MS-DOS, don't support RAID. If you dual boot your system to one of these noncompliant operating systems, your RAID-configured drives will be unusable.

Implementing RAID 0: Disk Striping

RAID level 0 is disk striping. With disk striping, two or more volumes—each on a separate drive—are configured as a stripe set. Data written to the stripe set is broken into blocks that are called *stripes*. These stripes are written sequentially to all drives in the stripe set. You can place volumes for a stripe set on up to 32 drives, but in most circumstances sets with two to five volumes offer the best performance improvements over non-RAID volumes because data from multiple drives is simultaneously accessed. Beyond this, the performance improvement decreases significantly.

The major advantage of disk striping is speed. Data can be accessed on multiple disks using multiple drive heads, which improves performance considerably. However, this performance boost comes with a price tag. As with volume sets, if any hard disk drive in the stripe set fails, the stripe set can no longer be used, which means that essentially all data in the stripe set is lost. You'll need to recreate the stripe set and restore the data from backups. Data backup and recovery are discussed in Chapter 14.

Note: The boot and system volumes can't be part of a striped set. Don't use disk striping with these volumes.

When you create stripe sets, you'll want to use volumes that are approximately the same size. Disk Management bases the overall size of the stripe set on the smallest volume size. Specifically, the maximum size of the stripe set is a multiple of the smallest volume size. For example, if you have three physical drives and if the smallest volume is 50 MB, the maximum size for the stripe set is 150 MB.

To maximize performance of the stripe set, there are several things you can do:

- Use disks that are on separate disk controllers. This allows the system to simultaneously access the drives.

- Don't use the disks containing the stripe set for other purposes. This allows each disk to dedicate its time to the stripe set.

You create a stripe set by completing the following steps:

1. In the Disk Management Graphical view, right-click an area marked Unallocated on a dynamic disk and then chooses Create Volume. This starts the Create Volume Wizard. Read the welcome dialog box, and then click next.

2. Select Striped Volume as the volume type. Create the volume as described previously in this chapter in the section entitled "Creating Volumes and Volume Sets." The key difference is that you need at least two dynamic disks to create a striped volume.

3. Once you create a striped volume, you can use the volume just like any other volume. You can't expand a stripe set once it's created. Because of this, you should carefully consider the setup before you implement it.

Removing a Mirrored Set

In Disk Management, you can remove one of the volumes from a mirrored set. When you do this, all data on the removed mirror is deleted and the space it used is marked as Unallocated.

To remove a mirror, complete the following steps:

1. In Disk Management, right-click one of the volumes in the mirrored set and then choose Remove Mirror.
2. Confirm the action when prompted. All data on the removed mirror is deleted.

Repairing a Stripe Set without Parity

A stripe set without parity doesn't have fault tolerance. If a drive that is part of a stripe set fails, the entire stripe set is unusable. Before you try to restore the stripe set, you should repair or replace the failed drive. Afterward, you need to re-create the stripe set and then recover the data contained on the stripe set from backup.

Regenerating a Stripe Set with Parity

With RAID 5 you can recover the stripe set if a single drive fails. You'll know that a stripe set with parity drive has failed because the status of the set changes to Failed Redundancy and the status of the individual volume changes to Missing, Offline, or Online (Errors).

You can repair RAID 5 on basic and dynamic disks, but you must rebuild the set using the same disk type. To resolve problems with the RAID 5 set, complete the following steps:

1. You need to get all drives in the RAID 5 set online. The status of the set should read Failed Redundancy. The corrective action you take depends on the status of the failed volume.

   Note: If possible, you should back up the data before you perform this procedure. This ensures that if you have problems, you can recover your data.

2. If the status is Missing or Offline, make sure that the drive has power and is connected properly. Afterward, start Disk Management, right-click the failed volume, and select Reactivate Disk. The drive's status should change to Regenerating and then to Healthy. If the status of the drive doesn't return to Healthy, right-click the volume and select Regenerate Parity.

3. If the status is Online (Errors), right-click the failed volume and select Reactivate Disk. The drive's status should change to Regenerating and then to Healthy. If the status of the drive doesn't return to Healthy, right-click the volume and select Regenerate Parity.

4. If one of the drives shows as Unreadable, you may need to rescan the drives on the system by selecting Rescan Disks from Disk Management's Action menu. If the drive status doesn't change, you may need to reboot the computer.

5. If one of the drives still won't come back online, you need to repair the failed region of the RAID 5 set. Right-click the failed volume and then select Remove Volume. You now need to select an unallocated space on a separate dynamic disk for the RAID 5 set. This space must be at least as large as the region to repair, and it can't be on a drive that's already being used by the RAID 5 set. If you don't have enough space, the Repair Volume command is unavailable, and you'll need to free space by deleting other volumes or replacing the failed drive.

Part-iii

<u>Linux</u>

<u>WHAT IS LINUX:-</u>

Linux is an operating system that was first created at the University of Helsinki in Finland by a young student named Linux Torvalds. At this time the student was working on a UNIX system that was running on an expensive platform. Because of his low budget and his need to work at home, he decided to create a copy of the UNIX system in order to run it on a less expensive platform. He began his work in 1991 when he released version 0.02 and work steadily until 1994 when version 1.0 of Linux Kernel was released. The current full featured version at this time is 2.2.x (released January 25, 1999) and development continues. The Linux operating system is developed under the GNU General Public license and its source code is freely available to everyone who downloads it via the internet.

The CD ROM version of Linux is also available in many stores and computer that provide it. Linux may be used for a wide variety of purposes including networking, software development and as end user platform. Linux is often considering an excellent, low cost alternative to other more expensive operating system because you can install it on multiple computers without paying more.

<u>WHAT IS DISTRIBUTION:-</u>

The concept of a distribution can be a little hard to understand in a world of commercial operating system such as windows 98 and NT and even commercial UNIX system such as Solaris.
After all in all these cases the name of operating system denotes a very specific product. For instance windows 98 define the complete set of windows utilities, applications and drivers that Microsoft chips runs. There is no room for variation. Any application driver or utility that user adds to their systems is not considered part of windows 98 and windows 98 does not technically exists as a product with less than its complete set of software and tools.

In the Linux world however this definition becomes blared. The term Linux can refer to every thing from kernel to any collection of Linux based application put together with a kernel to produce a functioning system running Linux.

This lack of clear set of application utilities drivers and a kernel that together can clearly be identified exists because Linux has opened the door to different flavors of Linux that meet different needs. There are distributions. Distributions can be built on different versions of kernel can include different set of application utilities tools and drivers modules and can offer different installation and update programs to ease management of the system. There are numerous Linux distributions in recent years through five distributions have emerged as the most common.

1. Red Hat
2. Slack ware
3. Caldera
4. S.U.S.E
5. Detain

Architecture of Linux Operating System or Components

**Linux has all the components like a typical operating system as under.**

Kernel:-

The Kernel (Basically in raw binary form that is laded directly into memory at time of startup) is the central part of Linux Operating System.

The Linux Kernel includes device driver supports for a large number of PC Hardware devices (graphic cards, Network Cards, Hard Disk etc), advanced processor and memory management feature, and supports for many different types of file system including dos floppies and iso9660 standard for CD ROMs**.**

The Shell and GUIs:

The Shell Surrounds the Kernel and provides the Linux user interface. As Linux Supports two form of command input. Through textual command line shells like that Bourne shell and CSH the C shell. The second type of interface is graphical interface (GUIs) such as KDE and GNOME windows Manager.

Kernel

User Programs

Shell
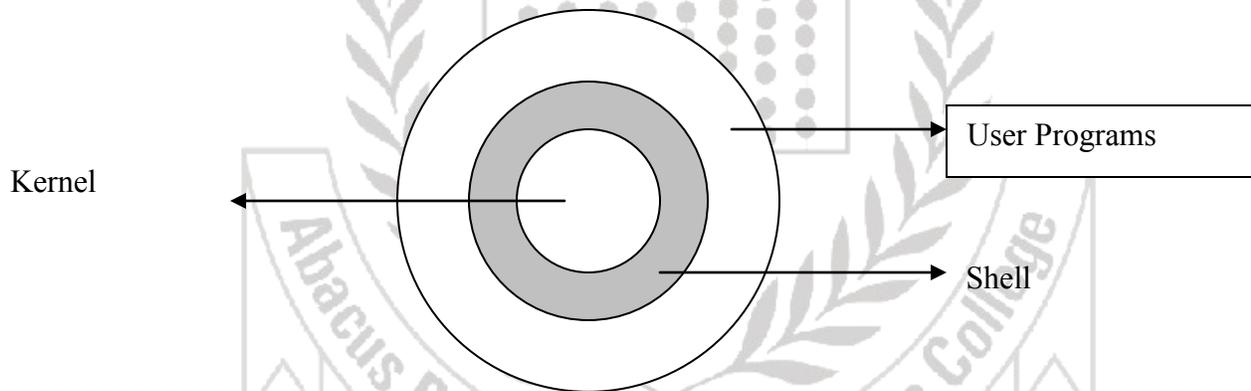
The fundamental architecture of Linux is given below:
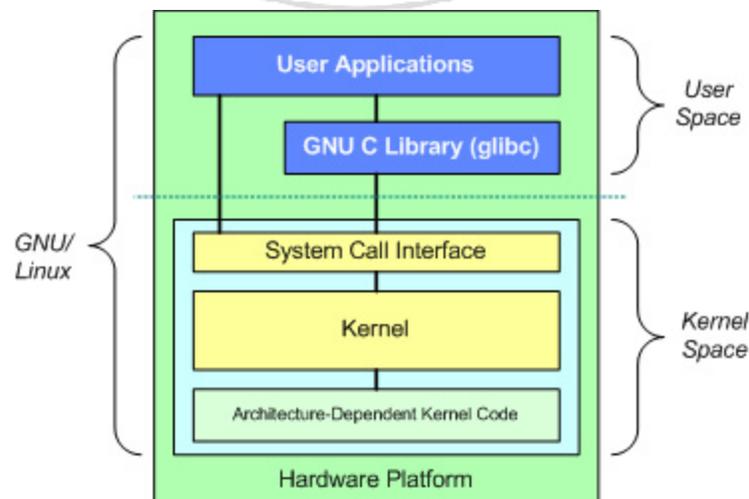
At the top is the user, or application, space. This is where the user applications are executed. Below the user space is the kernel space. Here, the Linux kernel exists.

There is also the GNU C Library (glibc). This provides the system call interface that connects to the kernel and provides the mechanism to transition between the user-space application and the kernel. This is important because the kernel and user application occupy different protected address spaces. And while each user-space process occupies its own virtual address space, the kernel occupies a single address space.

The Linux kernel can be further divided into three gross levels. At the top is the system call interface, which implements the basic functions such as read and write. Below the system call interface is the kernel code, which can be more accurately defined as the architecture-independent kernel code. This code is common to all of the processor architectures supported by Linux. Below this is the architecture-dependent code, which forms what is more commonly, called a BSP (Board Support Package). This code serves as the processor and platform-specific code for the given architecture.

FEATURES OF LINUX (Red Hat):-

The features that Red Hat Linux into popularity was its package management system. This system allows software application to be tested, configured and provided in ready to run state for Red Hat Linux. Using simple management tools, new packages can be downloaded installed and run without the some times tortuous configuration required with other packages. One benefit provided by package management is upgradeability. It is possible to upgrade versions of Red Hat without having to reinstall Linux from scratch.

Another major feature of the Red Hat distribution is that it is available not only on the Intel PC platform but also on two other platforms.

     a)   Digital Alpha based computers
     b)   Sun SPARC based computers.

Red Hat Linux offers a lot of new features not found in earlier versions and still not found in all distribution of Linux.

These features include:

     1)   improved installation
     2)   New and improved system administration tools.
     3)   the introduction of GNOME

1. Portability:

Means to modify a program from one computer system so that it works with different system. About 90% of code in current version of Linux is written in c language and remainder in assembly language. Linux is there fore a potable operating system as it can be easily modified.

♦ Multitasking:

It is an operating system that can do more than one thing at a time. Linux allows user to run as many process as it can handle. User can run several commands in background while executing another in fore ground.

♦ Multi-user:

An operating system that can be used by more than one person at a time, sharing resources, file space, printer and soon Linux support from one to 2008 users at a time.

♦ **Job control:**

It is ability to control which job is executed in fore ground, back ground or is suspended.

♦ **File system:**

It has tree like structure. It starts with one directory called root, symbolized by /, has multiples directories under it. Storage space for different user files is maintained by operating system. Files can be protected by unauthorized users**.**

♦ **Pipes:**

It is Linux File that takes output of one process and provides it as input to next process. While executing and multiple Linux command pipes may be used between command to create what is referred to as pipe line command.

♦ **Linux shell:**

User interaction with Linux is controlled by shell, a powerful command for interpreter. When user interact with shell search for program, if found, executes it.

♦ **Visual shell:**

These are menu-driven and provide command for file management, text processing and electronic mail.

♦ **Linux utilities:**

It includes 100 utility programs for function like sorting data, processing text and searching for information.

♦ **System Security**

There is several level of security in Linux. The First level is system security the standard login procedure be force Linux start running on the system which stopped the illegal user to start the windows. 2nd level security is file system security. So every user uses its own set of files and third level security allow user to encrypt the data files on the disk.

♦ **Linux Maturity**

Linux is solid and time tested operating system that has been in use over 25 years. Software is free form bugs and has high level of reliability of its capability.

Multitasking: Several programs can run at the same time.

•**Multiuser:** Several users can logon to the same machine at the same time There is no need to have separate user licenses.

• **Multiplatform:** Linux runs on many different CPUs, that mean it supports multiprocessor machine.

• **Multithreading:** Linux has native kernel support for multiple independent threads of control within a single process memory space.

•**Crash proof:** Linux has memory protection between processes, so that one program can't bring the whole system down.

•**Demand loads executables:** Linux only reads from those parts of a program that are actually used on the disk.

•**Shared copy-on-write pages among executables:** This means that multiple processes can use the same memory to run in. When one tries to write to that memory, that page (with 4KB piece of memory) is copied somewhere else. Copy-on-write has two benefits: increasing speed and decreasing memory use.

• Virtual memory uses paging (not swapping whole processes) to disk to a separate partition or a file in the file system, or both, with the possibility of adding more swapping areas during runtime (yes, they're still called swapping areas). A total of 16 of these 128 MB (2GB in recent kernels) swapping areas can be used at the same time, for a theoretical total of 2 GB of usable swap space. It is simple to increase this if necessary, by changing a few lines of source code.

•Linux has a unified memory pool for user programs and disk cache, so that all free memory can be used for caching, and the cache can be reduced when running large programs.

• Linux does core dumps for post-mortem analysis, allowing the use of a debugger on a program not only while it is running but also after it has crashed.

• Linux is mostly compatible with POSIX, System V, and BSD at the source level.

• Through an iBCS2-compliant emulation module, Linux is mostly compatible with SCO, SVR3, and SVR4 at the binary level.

• Free and Open source code for all: All source code of Linux is available, including the whole kernel and all drivers, the development tools and all user programs; also, all of it is freely distributable. Plenty of commercial programs are being provided for Linux without source, but everything that has been free, including the entire base operating system, is still free.

• Linux supports pseudoterminals (pty's) and multiple virtual consoles: By several independent login sessions through the console, you can switch between by pressing a hot-key combination (not dependent on video hardware). These are dynamically allocated; you can use up to 64.

• Linux supports several common file systems, including minix, Xenix, and all the common system V file systems, and has an advanced file system of its own, which offers file systems of up to 4 TB, and names up to 255 characters long.

• Linux has a transparent access to MS-DOS partitions (or OS/2 FAT partitions) via a special file system:.You don't need any special commands to use the MS-DOS partition, it looks just like a normal Unix file system (except for funny restrictions on file names, permissions, and so on). MS-DOS 6 compressed partitions do not work at this time without a patch (dmsdosfs). Also VFAT (WNT, Windows 95) support and FAT-32 is available in Linux 2.0

• Linux has CD-ROM file system which reads all standard formats of CD-ROMs.

• Linux performs well with TCP/IP networking, including ftp, telnet, NFS, etc.

• Linux is userfriendly as Netware client and server

• Linux also runs as Lan Manager/Windows Native (SMB) client and server

Linux Commands

MKDIR COMMAND:
Purpose:
Mkdir command is used for creating new directory (Folder). We also used some option with mkdir command.

Syntax:
        Mkdir [- option] Directory Name
Where Option are:
- p Parent directory creator. If directory, not exists.
-m Assign Permission default 755 mean Read, Write and execute Access for owner and Read and Execute Access for Other user and Group.

For example
                Mkdir   [-m]   abacus 755

CD Command OR CHDIR Command
Purpose:
Change current directory to directory which are specify in the command. We also use chdir command for this purpose.
Syntax
                Cd   Directory name
For example
                Cd   abacus

RMDIR Command
This Command is used to Delete the directory. Directory must be empty.
Syntax
        Rmdir   [-option]   Directory name
Where Option are:
-p
–s Give the message for confirmation

For Example
                Rmdir -s abacus
After typing this command delete the folder name abacus and before deleting give the confirmation message.

RM COMMAND:
Purpose
This command used to delete the folder and files and also sub folder if existing.
Syntax
                Rm [-r –f –I] Directory

Where –r means delete all the sub folder.
-I means give message before deleting
-f mean delete also write protected file
For Example
                Rm   -m abacus
After typing this command and pressing Enter Key the folder Abacus And All its files and subfolder deleted.

LS COMMAND
Purpose
This command displays the list of files and folder of the working directory.

Syntax
                Ls [-option]

Where option are:
-a display all the files including those files start with dot (.) means hidden files.
-A all the files including start with double dot.

-l display the long list means that all the information about files and folders.
-R in reverse order.

For Example

Ls – l

CAT COMMAND

Purpose

This command read the data form standard input and then out put in the different forms. In simple word we say that CAT command is used for three different purposes.

- ➢ First to create a new file for this purpose we use cat command in this way
Cat > file name
- ➢ Second we create a file for an other file we use cat command in this way
Cat source file name > destination file name

Where source file is file from which we create a new file. And destination file is new file name.

- ➢ if we want to merge the file contents with an other file we use cat command in this way:
Cat source file name >> destination file name

With this command Contents of source file merge with contents of Destination file.

- ➢ Cat command also display the Contents of file. For this purpose we use cat command with simple file name.
Cat File name

For Example

Cat > test.txt

After this type the contents of file and then press CTRL + D Key for save the file.

Cat Test.txt

This command Display the contents of file test.txt.

Cat test.txt > New.txt

This command Create a new file name new.txt and copy the contents of test.txt in to new.txt

Cat test.txt >> new.txt

This command add the contents of test.txt in to new.txt

CP COMMAND:

Purpose

This command copy the file form one location to other location or Copy the contents of one file to an other file

Syntax

Cp [option] (source file name) (destination / or destination file name)

Where option are:
-I Give the message if overwriting occur
-p Preserve that permission is granted.

For Example

Cp test.txt abacus

Where test.txt is file name and Abacus is folder name where we want copy test.txt.
We also use cp command in this way

Cp test.txt new.txt

In this way contents of first file copy in second file.

MV COMMAND:
Purpose

This command is used for two purposes.
- ➢ First Move the file or folder from one location to other location.
- ➢ This command also used for Renaming the file and folders.

Syntax

mv source file/folder   Destination

Or

mv old file name   new file name

For Example

mv   test.txt shah.txt

This command change the name file text.txt to shah.txt

LN COMMAND:
Purpose

This command creates the link of given file. This command same wok as we create short cut in windows.

Syntax

ln file name Link File name

For Example

Ln test.txt welcome.txt

FILE COMMAND
Purpose

This command describes the nature of file.

Syntax

File test.txt

For Example

File Test.txt

Return ASCII Text File

WC COMMAND:
Purpose

This command Count the Contents of file. For example total number of Character, Word and lines.

Syntax

Wc [-Option] File Name

Where Option are:
   -c Count the Total Character
   -l   Count The Total line
   - W Count The total Word

FOR EXAMPLE

WC [-c] Test.txt

Display the Total Character of the File Test.txt

CALENDAR COMMAND:
Purpose

This command Provide daily remainder service.

Syntax

Calendar   <message>

After This Press CTRL + D key

Now Type Calendar

FOR EXAMPLE

Calendar   MY 16 it will be Holiday
After This Press CTRL + D key
Now Type Calendar

CAL COMMAND
Purpose
This command display the calendar of the year

Syntax:
                    Cal [Month][Year]
Where month and year are optional if we type only CAL command then display the current calendar.
FOR EXAMPLE
                        Cal march 2006
After typing this command and pressing Enter Key Calendar of March 2006 is display on the screen.

PASSWD COMMAND:

PURPOSE
This Command Display the User Password.

SYNTAX
                    Passwd User Name [-d][-f]
Where –d for deleting the password
-f means that you user must be change the password.

CHMOD COMMAND

PURPOSE
This command change the mode of file or attribute of file same work as ATTRIB COMMAND work in DOS. We also say that this file give the rights to any user for a specific file.
There are two way in which we set the mode of file. First By giving OCTAL number set
Such that.
            R   W   X
            4   2   1
For every three type of user Such that Owner, Group and Other User We Give the Sum of These Combination of Number.
For example
                Chmode   755 Text.txt
Means that Owner Access all rights and other (4+1= 5)means that R + X (Read and Execute) the file.
Other Way is that we specify the Character set Like That R, W and X for three type of work Read , Write and Execute.
For Example
                    Chmod g +rwx Test.txt
Its means that give the Read , Write and Execute all access to Group User.

WHO COMMAND
PURPOSE

This Command Display The list of those users who are Currently Login.

SYNTAX
                    Who [-s][-q][-h][-i]
Where
-s means that Display the User ID
-H Column Header
-q Display quick Information consist on only user ID
-I Also send the message

WHO AM I COMMAND
PURPOSE
This tells that who ere you, Means That Log in Name of the user.
SYNTAX
Who am I

WRITE COMMAND:
Purpose
This command used to send the message to the other user right at the same time when you type the message it will be send at real time message to the online user whose name is specified in the command. In the end press CTRL+D or Z key for stop this process.
Syntax
Write User Name List
Message
Press CTRL+D or Z
For Example :
Write user01
Hello   how are You my Friend
When You press Enter key this message Transmit to User01. For end of session Press CTRL+D or CTRL+Z key.

MESSG COMMAND:
PURPOSE
Set the privileges That user Send The messages are Not to Other User.
SYNTAX
Mess Yes / Not

WALL COMMAND
Purpose
This command is used to display the message to all those users who are currently logged on to the system. wall command is differ form write command because write command send the message to specify users but wall command send the message to all user.
Syntax:
Wall   message   (Press CTRL+Z key)
For Example :
Wall message
Please Shut Down You PC
CTRL+Z

MAIL COMMAND:
This command is used to send the mail to any user in Network. If User currently not login then mail store in the mail box of that user. User can check this mail at any time when he/she login by typing mail and press enter key.

SYNTAX
Mail User ID
Write text-------

Press CTRL +D Key to save
Also you can send the file with mail command
For this purpose write command in this way
Mail User name < File Name
CLEAR COMMAND:
PURPOSE
This command clears the contents of the screen.
SYNTAX
Clear <Press Enter Key>

VI COMMAND:
This command is used to edit the file are create new file.
SYNTAX
             Vi file name
For Example:
             vi   test.txt

PICO COMMAND:
PURPOSE
             This command is used for creating a new file are edit the previous store file.
SYNTAX
             Pico < File name>
For Example:
             Pico Test.txt

LESS COMMAND:
PURPOSE
             This command Write The Contents of file on the screen. You can not edit the file with this command. Jus like Type command in DOS.
SYNTAX
             Less < File Name>
For Example:
             Less test.txt

TAR COMMAND:
PURPOSE
             This command Create a backup of file.
 SYNTAX:
             Tar File name Backup filename

DELUSER COMMAND:
PURPOSE
         This command deletes the user from Linux Server. Or Remove the Login Name.
SYNTAX
             Deluser User Name
For Example:
             Deluser   user01

TOUCH COMMAND:
This command is used to create a new file or edit the existing file.
SYNTAX
             Touch File name

CHGRP COMMAND:
PURPOSE
         This command is used to changing the group of file.
             Chgrp Group Name File name
For Example:
             Chgrp Friend Test.txt

MORE COMMAND:
Purpose:
         The more command is used to display the contents of file page by page. The more command pauses at the end of each page and by pressing Space Bar key Next page is display.
Syntax:
             More [+ Line Number] File name
Where Line number is optional which specify the Starting Line Number.
For Example
             More Test.txt

OR

     More +20 test.txt

TAIL COMMAND:

Purpose:

     Display the contents of file from one specific point to an other specific point. (Top to Tail)

Syntax:

     Tail +Start Line number   test.txt   [+ End Line Number] File Name

Last Line Number is optional

For Example:

     Tail +17 Test.txt

Display from line number 17 to end

HEAD COMMAND:

Purpose:

     This command display the contents of file form top to Specific Number Of line.

Syntax:

     Head   [- Number]   file Name

For Example:

     Head   -3 test.txt

Display the first 3 line on the screen

FINGER COMMAND:

Purpose:

     Display the detail of Information of the user. If we specify the user name then information about that user is display other wise information of all currently login is display.

Syntax:

     Finger [user name]

Where user name is optional.

For Example:

     Finger (Press Enter Key)

AT COMMAND:

Purpose:

     This command is used to send the message or execute any command at specific time.

Syntax:

     At Time

     Message OR Command

For Example:

     At 04:00

     This is Class Time

     (Press CTRL + D)

SHUTDOWN COMMAND:

Purpose:

     This command disconnects the other user from server. We also say that this command change the system status multi user to single user.

Syntax:

     Shutdown –g –y

Where –g give the 60 second to user save work and log out and –y means that disconnect the user with out confirmation

For Example:

     Shutdown - g

Disconnect the user in 60 second

     Shutdown - g 30

Disconnect the user in 30 second

ADDUSER COMMAND:
Purpose:
        This command add the new user to the system.
Syntax:
                Adduser Login name [Login ID] [Login Directory]
Where
Login ID is User Identification number
Login Directory is root Directory of that user. By default same as user name
For Example:

                Adduser abacus
PS COMMAND:
Purpose:
        This command is used to display the running process.
Syntax:
                Ps
For Example:
                PS <Press Enter Key>
Display the Current Process ID and Terminal And Time.

KILL COMMAND :
This command Stopped the running process in background.
SYNTAX
                Kill [-Signal] [Process ID]
FOR EXAMPLE
                    Kill -15 223

GREP:-

The grep command is used to search a word in a file or directory.
Syntax:-
 # grep word
example:-
 # grep islamia.

FIND:-

The find command is used to find a file or directory.
Syntax:-
 # find 1 name directory file
example:-
 # find 1 name akhtar

MAN:-

The man command is used to get information about a command.
Syntax:-
 # man command name
example:-
 # man ls

ZIP:-

The zip command creates a zip archive from

UNZIP:-

The unzip command manipulates and extracts zip archives.
Syntax:-
 # unzip [file name]
 # unzip abacus

BG:-

The bg command is used to set the background color of your screen.
Syntax:-
 # color name
example:-
 # bg yellow

FG:-

The fg command is used to set the foreground color of your screen.
Syntax :-
 # fg color name
example:-
 # fg green

AT:-

The at command is used to schedule commands to be executed at a specific time.
Syntax :-

 # at shutdown 12:30