1. VIRTUALIZATION

"In computing, virtualization is a broad term that refers to the abstraction of computer resources.

Virtualization hides the physical characteristics of computing resources from their users, be they applications, or end users. This includes making a single physical resource (such as a server, an operating system, an application, or storage device) appear to function as multiple virtual resources; it can also include making multiple physical resources (such as storage devices or servers) appear as a single virtual resource..."

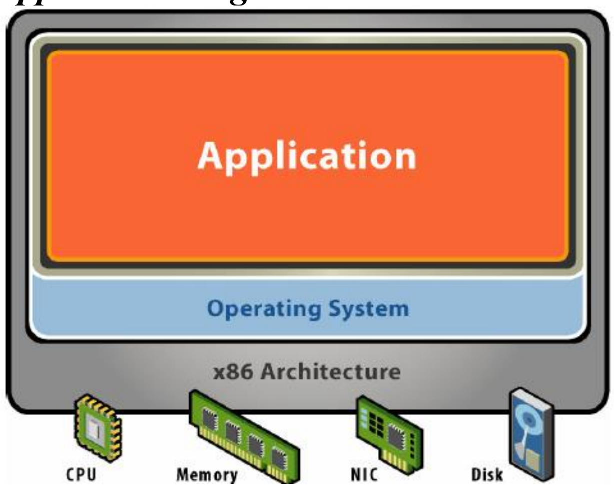


Fig: Traditional Stack

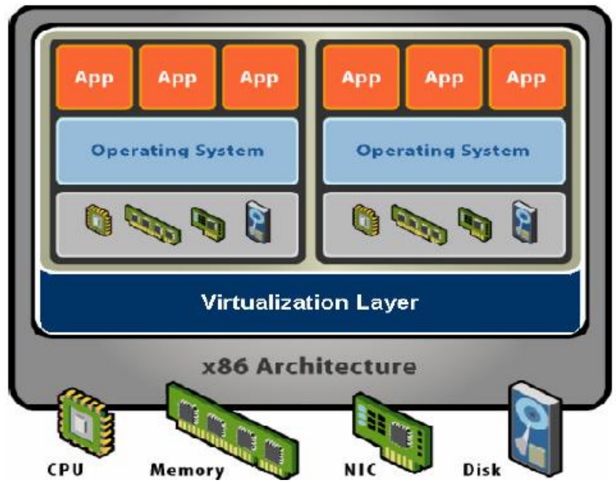


Fig: Virtualized Stack

Types of Virtualization

Today the term virtualization is widely applied to a number of concepts including:

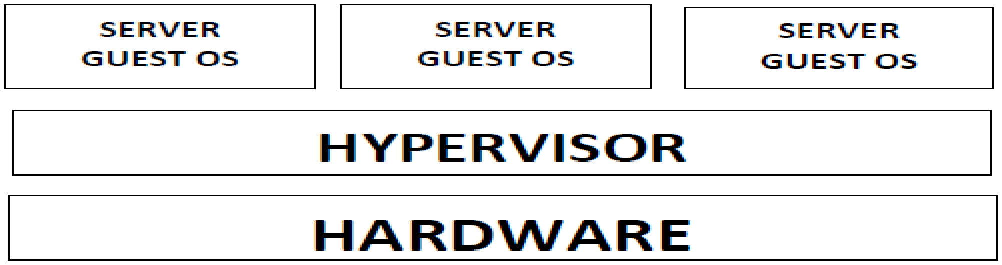
1. **Server Virtualization**
2. **Client / Desktop / Application Virtualization**
3. **Network Virtualization**
4. **Storage Virtualization**
5. **Service / Application Infrastructure Virtualization**

In most of these cases, either virtualizing one physical resource into many virtual resources or turning many physical resources into one virtual resource is occurring.

Server Virtualization

Server virtualization is the most active segment of the virtualization industry featuring established companies such as VMware, Microsoft, and Citrix. **With server virtualization one physical machine is divided many virtual servers.** At the core of such virtualization is the concept of a hypervisor (virtual machine monitor).

A hypervisor is a thin software layer that intercepts operating system calls to hardware. Hypervisors typically provide a virtualized CPU and memory for the guests running on top of them. The term was first used in conjunction with the IBM CP-370.



Hypervisors are classified as one of two types:

Type 1 – This type of hypervisor is also known as native or bare-metal. They run directly on the hardware with guest operating systems running on top of them. Examples include VMware ESX, Citrix XenServer, and Microsoft'sHyper-V.

Type 2 – This type of hypervisor runs on top of an existing operating system with guests running at a third level above hardware. Examples include VMware Workstation and SWSoft's Parallels Desktop.

Related to type 1 hypervisors is the concept of paravirtualization. Paravirtualization is a technique in which a software interface that is similar but not identical to the underlying hardware is presented. Operating systems must be ported to run on top of a paravirtualized hypervisor. Modified operating systems use the "hyper calls" supported by the paravirtualized hypervisor to interface directly with the hardware. The popular Xen project makes use of this type of virtualization. Starting with version 3.0 however Xen is also able to make use of the hardware assisted virtualization technologies of Intel (VT-x) and AMD (AMD-V). These extensions allow Xen to run unmodified operating systems such as Microsoft Windows.

Advantages/Benefits:

- **Increased Hardware Utilization** – This results in hardware saving, reduced administration overhead, and energy savings.
- **Security** – Clean images can be used to restore compromised systems. Virtual machines can also provide sandboxing and isolation to limit attacks.
- **Development** – Debugging and performance monitoring scenarios can be easily setup in a repeatable fashion. Developers also have easy access to

operating systems they might not otherwise be able to install on their desktops.

Disadvantages/Drawbacks/Downsides:

- **Security** – There are now more entry points such as the hypervisor and virtual networking layer to monitor. A compromised image can also be propagated easily with virtualization technology.
- **Administration** – While there are less physical machines to maintain there may be more machines in aggregate. Such maintenance may require new skills and familiarity with software that administrators otherwise would not need.
- **Licensing/Cost Accounting** – Many software-licensing schemes do not take virtualization into account. **For example** running 4 copies of Windows on one box may require 4 separate licenses.
- **Performance** – Virtualization effectively partitions resources such as RAM and CPU on a physical machine. This combined with hypervisor overhead does not result in an environment that focuses on maximizing performance.

Application/Desktop Virtualization

Virtualization offers a number of uses on the client side at both the desktop and application level. Such virtualization can be broken out into four categories:

- Local Application Virtualization/Streaming
- Hosted Application Virtualization
- Hosted Desktop Virtualization
- Local Desktop Virtualization

Application virtualization is an umbrella term that describes software technologies that improve manageability and compatibility of legacy applications by encapsulating applications from the underlying operating system on which they are executed. Application virtualization differs from operating system virtualization in that in the latter case, the whole operating system is virtualized rather than only specific applications.

With streamed and local application virtualization an application can be installed on demand as needed. If streaming is enabled then the portions of the application needed for startup are sent first optimizing startup time. Locally virtualized applications also frequently make use of virtual registries and file systems to maintain separation and cleanness from the user's physical machine. Examples of local application virtualization solutions include Citrix Presentation Server and Microsoft SoftGrid.

Hosted application virtualization allows the user to access applications from their local computer that are physically running on a server somewhere else on the network. Technologies such as Microsoft's RemoteApp allow for the user experience to be relatively seamless include the ability for the remote application to be a file handler for local file types.

Benefits of application virtualization include:

- **Security** – Virtual applications often run in user mode isolating them from OS level functions.
- **Management** – Virtual applications can be managed and patched from a central location.
- **Legacy Support** – Through virtualization technologies legacy applications can be run on modern operating systems they were not originally designed for.
- **Access** – Virtual applications can be installed on demand from central locations that provide failover and replication.

Disadvantages include:

- **Packaging** – Applications must first be packaged before they can be used.
- **Resources** – Virtual applications may require more resources in terms of storage and CPU.
- **Compatibility** – Not all applications can be virtualized easily.

Desktop virtualization (or Virtual Desktop Infrastructure) is a server-centric computing model that borrows from the traditional thin-client model but is designed to give administrators and end users the best of both worlds: the ability to host and centrally manage desktop virtual machines in the data center while giving end users a full PC desktop experience.

Hosted desktop virtualization is similar to hosted application virtualization, expanding the user experience to be the entire desktop. Commercial products include Microsoft's Terminal Services, Citrix's XenDesktop, and VMware's VDI.

Benefits of desktop virtualization include most of those with application virtualization as well as:

- **High Availability** – Downtime can be minimized with replication and fault tolerant hosted configurations.
- **Extended Refresh Cycles** – Larger capacity servers as well as limited demands on the client PCs can extend their lifespan.
- **Multiple Desktops** – Users can access multiple desktops suited for various tasks from the same client PC.

Disadvantages/Drawbacks/Downsides:

Disadvantages of desktop virtualization are **similar to server virtualization**. There is also the added disadvantage that clients must have network connectivity to access their virtual desktops.

The final segment of **client virtualization** is local desktop virtualization. It could be said that this is where the recent resurgence of virtualization began with VMware's introduction of VMware Workstation in the late 90's. Today the market includes competitors such as Microsoft Virtual PC and Parallels Desktop. Local desktop virtualization has also played a key part in the increasing success of Apple's move to Intel processors since products like VMware Fusion and Parallels allow easy access to Windows applications. Some the benefits of local desktop virtualization include:

- **Security** – With local virtualization organizations can lock down and encrypt just the valuable contents of the virtual machine/disk. This can be more performant than encrypting a user's entire disk or operating system.
- **Isolation** – Related to security is isolation. Virtual machines allow corporations to isolate corporate assets from third party machines they do not control. This allows employees to use personal computers for corporate use in some instances.
- **Development/Legacy Support** – Local virtualization allows a users computer to support many configurations and environments it would otherwise not be able to support without different hardware or host operating system. Examples of this include running Windows in a virtualized environment on OS X and legacy testing Windows 98 support on a machine that's primary OS is Vista.

Network Virtualization

Up to this point the types of virtualization covered have centered on applications or entire machines. Other computing concepts also lend themselves to being software virtualized as well. Network virtualization is one such concept.

***Network Virtualization* is the process of combining hardware and software network resources and network functionality into a single, software-based administrative entity, a virtual network.** Network virtualization involves platform virtualization, often combined with resource virtualization.

Network virtualization is categorized as either **external**, combining many networks, or parts of networks, into a virtual unit, or **internal**, providing network-like functionality to the software containers on a single system…

Using the internal definition of the term, desktop and server virtualization solutions provide networking access between both the host and guest as well as between many guests. On the server side virtual switches are gaining acceptance as a part of the virtualization stack. The external definition of network virtualization is probably the more used version of the term however. Virtual Private Networks (VPNs) have been a common component of the network administrators' toolbox for years with most companies allowing VPN use. Virtual LANs (VLANs) are another commonly used network virtualization concept.

Advantages/Benefits:

- **Customization of Access** – Administrators can quickly customize access and network options such as bandwidth throttling and quality of service.
- **Consolidation** – Physical networks can be combined into one virtual network for overall simplification of management.

Disadvantages/Drawbacks/Downsides:

- **Increased complexity**
- **Performance overhead**
- **Need for administrators to have a larger skill set.**

Storage Virtualization

Storage virtualization **refers to the process of abstracting logical storage from physical storage.**

The term storage virtualization typically includes additional concepts such as **data migration and caching**. Storage virtualization is hard to define in a fixed manner due to the variety of ways that the functionality can be provided. Typically, it is provided as a feature of:

- Host Based with Special Device Drivers
- Array Controllers
- Network Switches
- Stand Alone Network Appliances

Another primary way that storage virtualization is classified is whether it is in-band or out-of-band**. In-band (often called symmetric) virtualization** sits between the host and the storage device allowing caching. **Out-of-band (often called asymmetric) virtualization** makes use of special host based device drivers that first lookup the meta data (indicating where a file resides) and then allows the host to directly retrieve the file from the storage location. Caching at the virtualization level is not possible with this approach.

Advantages/Benefits:

- **Migration** – Data can be easily migrated between storage locations without interrupting live access to the virtual partition with most technologies.
- **Utilization** – Similar to server virtualization, utilization of storage devices can be balanced to address over and underutilization.
- **Management** – Many hosts can leverage storage on one physical device that can be centrally managed.

Disadvantages/Drawbacks/Downsides:

- **Lack of Standards and Interoperability** – Storage virtualization is a concept and not a standard. As a result vendors frequently do not easily interoperate.
- **Metadata** – Since there is a mapping between logical and physical location, the storage metadata and its management becomes key to a working reliable system.
- **Backout** – The mapping between local and physical locations also makes the backout of virtualization technology from a system a less than trivial process.

Service / Application Infrastructure Virtualization

Application infrastructure virtualization (sometimes referred to as application fabrics) unbundle an application from a physical OS and hardware. Application developers can then write to a virtualization layer. The fabric can then handle features such as deployment and scaling. In essence this process is the evolution of grid computing into a fabric form that provides virtualization level features. Companies such as Appistry and DataSynapse provides features including:

- Virtualized Distribution
- Virtualized Processing
- Dynamic Resource Discovery

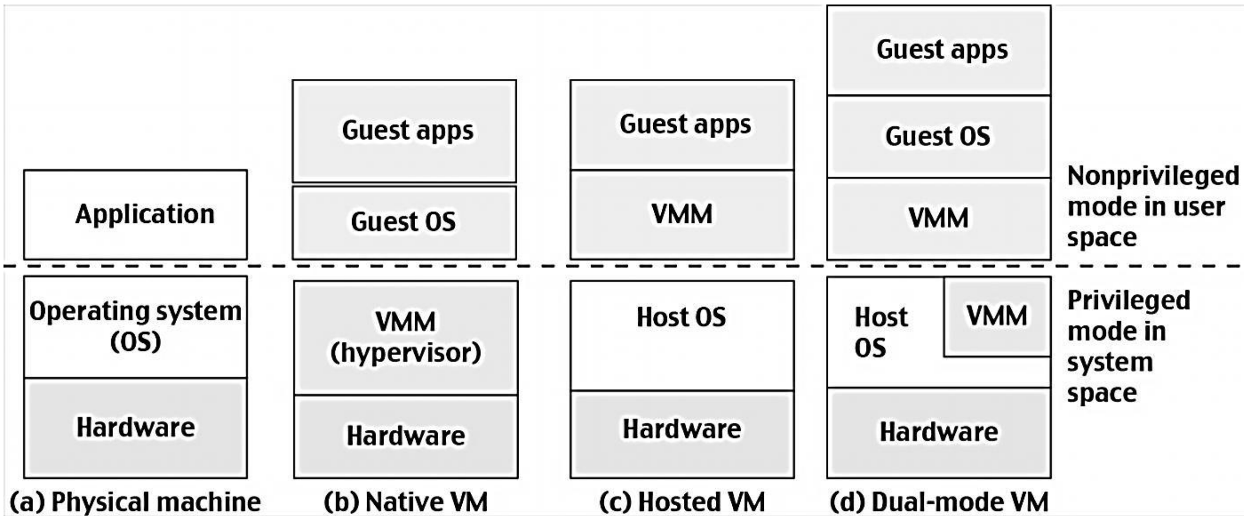
IBM has also embraced the virtualization concept at the application infrastructure level with the rebranding and continued of enhancement of Websphere XD as Websphere Virtual Enterprise. The product provides features such as service level management, performance monitoring, and fault tolerance. The software runs on a variety of Windows, Unix, and Linux based operating systems and works with popular application servers such as WebSphere, Apache, BEA, JBoss, and PHP application servers. This lets administrators deploy and move application servers at a virtualization layer level instead of at the physical machine level.

2. VIRTUAL MACHINES & VIRTUALIZATION MIDDLEWARE

A conventional computer has a single OS (Operating System) image. Single OS image offers a rigid architecture that tightly couples application software to a specific hardware platform.

Some software running well on one machine may not be executable on another platform with a different instruction set under a fixed OS.

The below diagram shows the comparison between physical machine and three VM architectures



In **FIG-A: -** X-86 architecture desktop running its installed windows OS.

FIG-B: - shows a native VM installed with the use of VMM called Hypervisor in privileged mode.

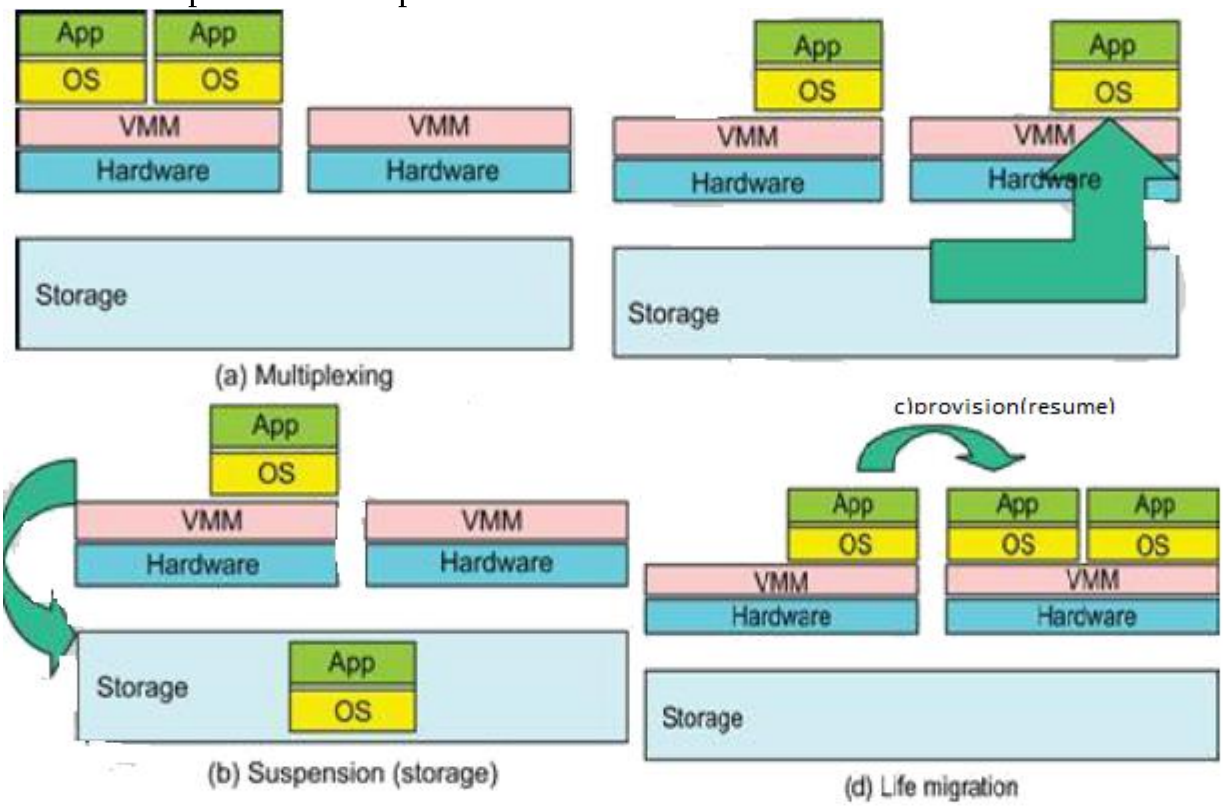
Virtual machines (VM's) offer solutions to

1. Underutilized resources,
2. Application inflexibility,
3. Software manageability
4. Security concerns in existing physical machines.

Hypervisor approach is also called Bare-Metal VM because the hypervisor handle bare hardware (CPU, Memory, and I/O) devices directly. The VM can be provisioned for any hardware system, the VM is built with virtual resources managed by guest OS to run a specific application.

The VM is built with virtual resources managed by guest OS to run a specific application. Between VM's and host platform one need s to deploy a middleware layer called VMM (Virtual Machine Monitor).

In FIG-C, VMM runs in non-privileged mode. The host OS need not be modified.
In FIG-D, the VM is implemented in dual mode. Part of VMM runs at user level and another part runs at supervisor level.



In this case the host OS may have to be modified to some extent. The VM approach offers hardware independence of OS and applications. The user application running on its dedicated OS could be bundled together as a virtual appliance that can be ported to any hardware platform

VM Primitive Operations

The VMM provides VM abstraction to the guest OS. With full virtualization, the VMM exports a VM abstraction identical to physical machine so that a standard OS (windows 2000 or Linux) can run just as it would on the physical hardware.

The following are the low level VMM operations

1. Multiplexing 2. Suspension
3. Provision 4. Life migration.

First VM's can be multiplexed between hardware machines

Second a VM can be suspended and stored in stable storage.

Third a suspended VM can be resumed or provisioned to a new hardware platform.

Finally a VM can be migrated from one hardware platform to another. These VM operations enable a VM to be provisioned to any available hardware platforms.

The VM approach will significantly enhance the utilization of server resources. Multiple server functions can be consolidated on the same hardware platform to achieve higher system efficiency.

3. GRID FRAMEWORK

- Grid computing is the integration of computer resources for achieving similar objective.
- The grid may be a dispersed system along with non-interactive workloads which comprise a huge number of files.
- Grids are frequently created with middleware software libraries of a common grid.
- Grids are a type of dispersed computing system, whereas a virtualized super computer is made from various networked.
- Grids focus on two different but associated objectives—supplying isolated access to IT resources and building up processing control.
- The grid is a technology which controls two factors—allocation and trust.
- Grid computing is a versatile technology which has its base in e-science and has progressed from previous expansions in parallel and high-performance computing (HPC).

The main resources that can be shared in a grid are:

1. Processing and computing power
2. Networked file and data storage systems
3. Bandwidth and communications
4. Application software
5. Tools used for scientific purpose

The distinct definitions for grid and grid computing are:

- **Grid middleware** is exclusive software that offers the essential functionality needed to facilitate sharing of various resources and setting up of virtual businesses. Grid middleware is exclusive software that is incorporated into the infrastructure of the concerned corporation. Grid middleware offers a unique virtualization and sharing layer which is positioned among the various infrastructures and the particular user applications using it.
- **Grid computing** is fundamentally the installed Grid middleware or the computing permitted by grid middleware based on synchronized, safe,

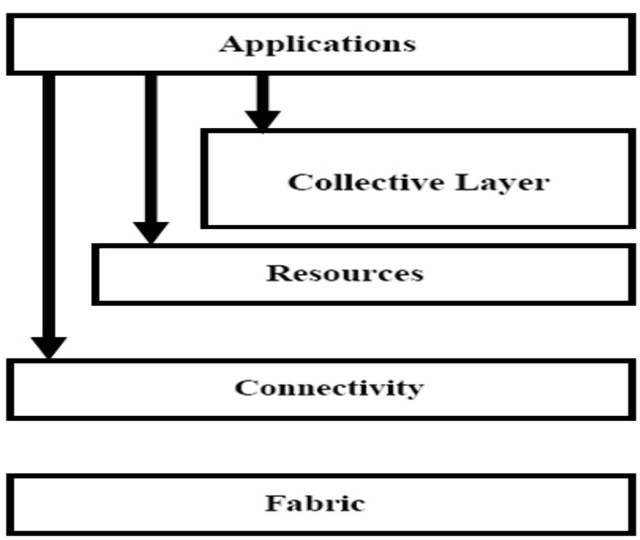
flexible resource sharing among a collection of resources, people, and organizations.

- **Grid infrastructure** refers to the union of grid middleware and hardware which converts single portions of data resources and hardware into an incorporated virtualized infrastructure that is displayed to the user as the only computer in spite of heterogeneity of the fundamental infrastructure.
- **Utility computing** is a type of computing that provides customized applications of grid and computing as a service. It is based on pay-as-per-utilization business modules.

4. GRID ARCHITECTURE

Various layers of the grid architecture are:

- **Fabric layer:** It Includes Physical resources that are shared inside the grid. It comprises Network resources, Computational resources, storage systems, sensors, software modules and additional system resources.
- **Connectivity layer:** It switch of data among fabric layer resources. It Comprises identification, transfer, navigation and support for safe conversation
- **Resource layer**: It provides protection and interaction activity as distinguished by connectivity layer, which is used for many applications such as accounting and scrutinizing etc. It incorporates mainly information and management practices



- **Collective layer:** It is liable for resource management and for interaction with collection of resources. The most facilities are directory services, co-allotment, scrutinizing, investigative services, data imitation services and setting up and collaborating services.
- **Application layer:** It involves user applications which are installed on grid. It is significant to observe that no user application s which are installed on a grid, unless it is grid permitted application, that is, an application which utilizes various processors of a grid.

The key functionalities of a grid middleware are as follows:

1. Integration and virtualization of various independent resources
2. Requirement of information concerning resources and their accessibility
3. Lively and flexible resource administration and allotment
4. Brokerage of resources based on open markets or corporation strategies
5. Safety comprising agreement and confirmation of users and accountability
6. Licenses administration
7. Expense and invoicing
8. Transport of non-insignificant ‘Quality of Service’

Advantages of Grid Computing:

- Easier to collaborate with other organizations.
- Make better use of existing hardware.
- No need to but huge servers for applications that can be split up and farmed out to smaller commodity type servers.
- Grid environments are much more modular and don’t have single points of failure. If one of the servers/desktops within the grid fail there are plenty of other resources able to pick the load.
- Jobs can be executed in parallel speeding performance
- Can solve larger, more complex problems in a shorter time.

Challenges of Grid Computing:

- It is not enough to just change the prevailing spread IT infrastructure into a grid. In majority of instances, investments are required for making the existing applications to work on a grid infrastructure.
- Lack of values for grid computing make resources’ findings for grid technology difficult and risky.
- Grid computing is a versatile technology and the launching of grid computing in a corporation is characteristically a long-standing plan that needs time until the visibility of first results. The beginning of grid

computing could need consistency of physical resources. Even if grids would essentially be capable to handle heterogeneity of resources that are accessible, advanced heterogeneity of resources might need advanced savings in terms of money and time and hence increase the downfall risk.

5. CLOUD COMPUTING ARCHITECTURE

- In cloud computing environment, physical resources are made available to cloud users with the help of virtualization software in the form of virtual resources.
- Cloud computing architecture is not fixed as other computing architectures, but it is different on the basis of different jobs, resource distribution.
- Basic cloud computing environment is shown in the Fig. 3.1 in which various services such as available servers, virtual desktop, system software, application software, database, etc. are available for cloud users.
- Users can avail the services using any device such as desktop system, laptop, mobile, tablet, etc.,

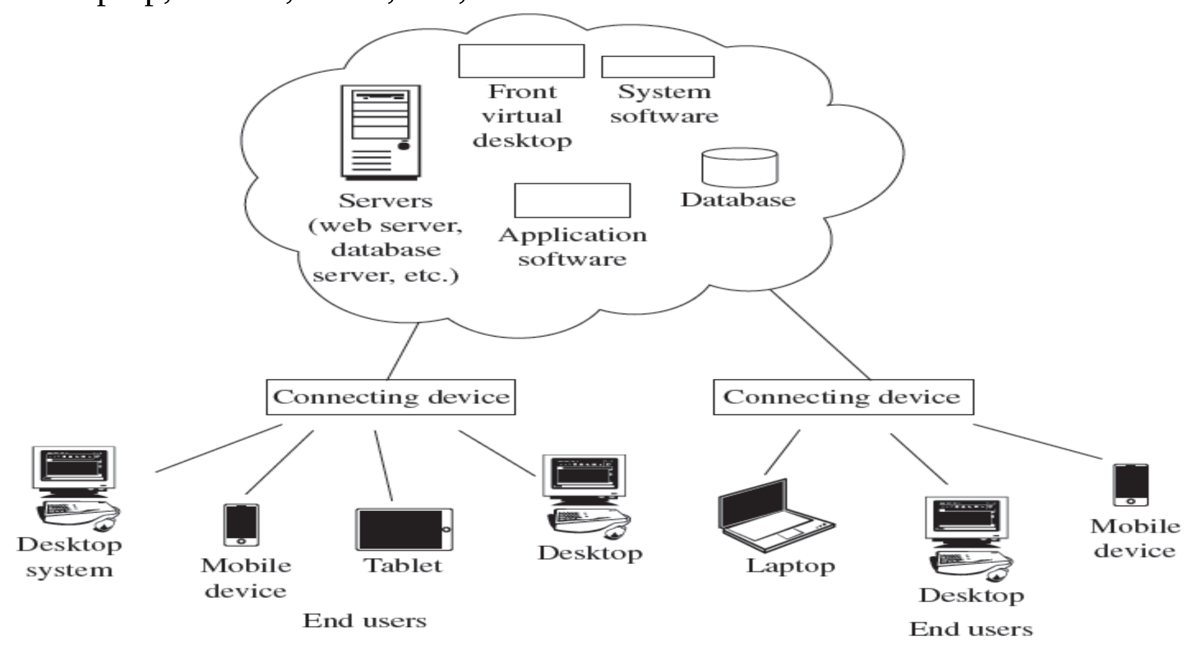


Fig. 3.1 Cloud architecture

The Cloud Computing architecture is based on different criteria:

- On the Basis of Load Balancing
- On the Basis of Disk Provisioning
- On the Basis of Storage Management

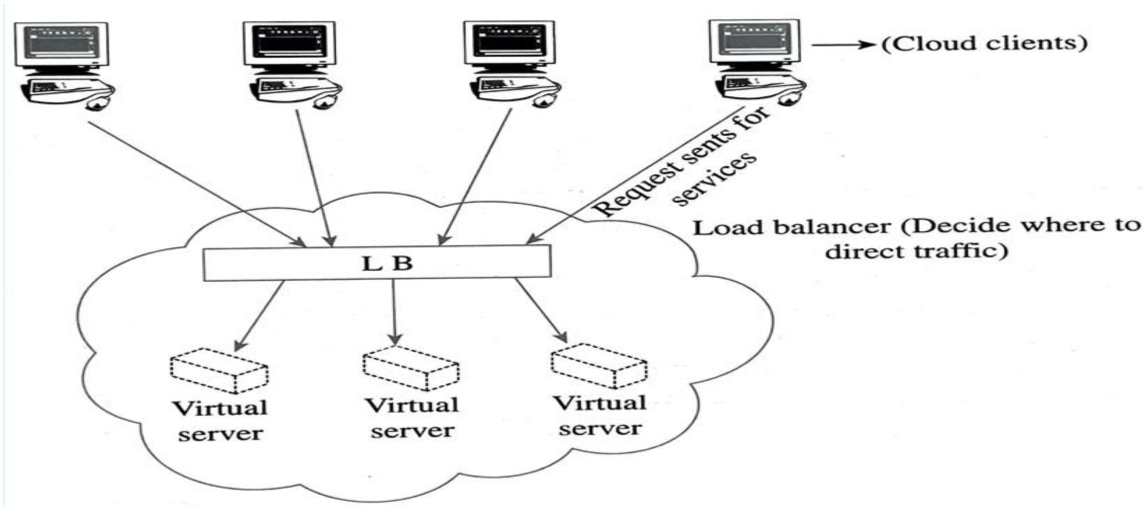
- On the Basis of Hypervisor Installed
- On the Basis of Migration
- On the Basis of Service Relocation
- On the Basis of Cloud Balancing
- On the Basis of Virtual Switches Load Balancing
- On the Basis of Failure Detection and Recovery

On the Basis of Load Balancing:

- Load balancing is the technique which is responsible to distribute the load, that is, no of requests, no of users etc. across one or additional servers, network interfaces, hard drives or other computing recourses.
- Load balancing is used to improve performance, reliability, elasticity, scalability and availability.
- Load balancing handles runtime distribution.

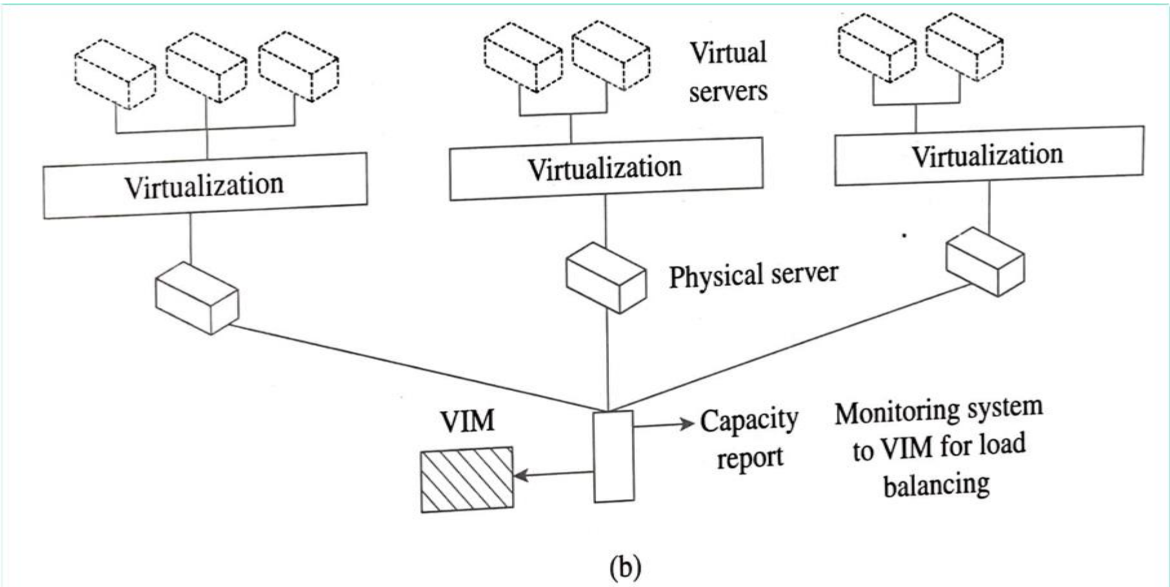
The distribution function includes:

1. A high power resource for handling workload that requires more processing power.
2. Providing services on the basis of priority.
3. Directing traffic to a particular IT resource as per the requirement by cloud users.



(a)

Load balancer is able to perform functions such as optimizing resource utilization, better throughput, maintaining QoS, etc. It can hardware or software. In the figure (a), If a cloud user requests for a server, load balancer acts as resource allocator between user and cloud service that is hidden from the user. In the figure (b), Virtual Infrastructure Manager (VIM) provides proper load balancing and runtime distribution of client demands.



On the Basis of Disk Provisioning:

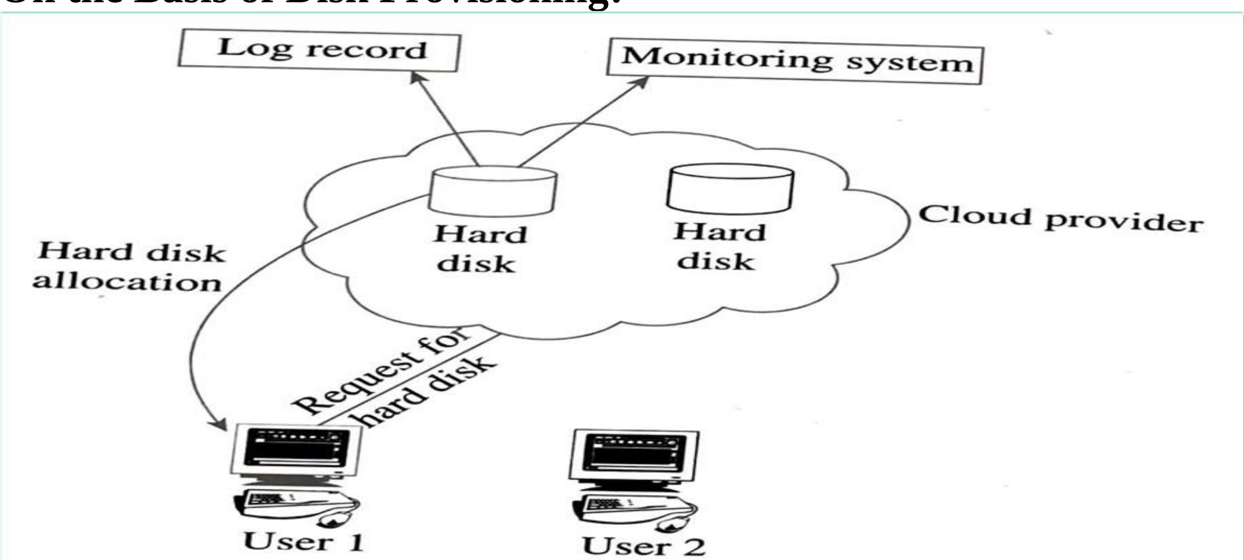


Fig. 3.3 Disk provisioning

Dynamic disk provisioning is used by cloud users for dynamic storage allocation, due to which clients have to pay extra amount of storage than what is actually used and required. For example, if a client needs four, 100 GB hard drives on virtual server, they are not billed for using 400 GB of storage space as shown in Fig. 3.3.

Software is used to actually monitor and track activity of cloud user and to generate bill. Log storage is important for monitoring cloud usage and for generating billing on the basis of fluctuations of usage. Redundant storage is also necessary for making the data safe and secure because sometimes a cloud storage device can lead to failure of the primary resource. At the time of failure of primary resource, request is directed to secondary storage device for providing smooth service to cloud consumers.

On the Basis of Storage Management:

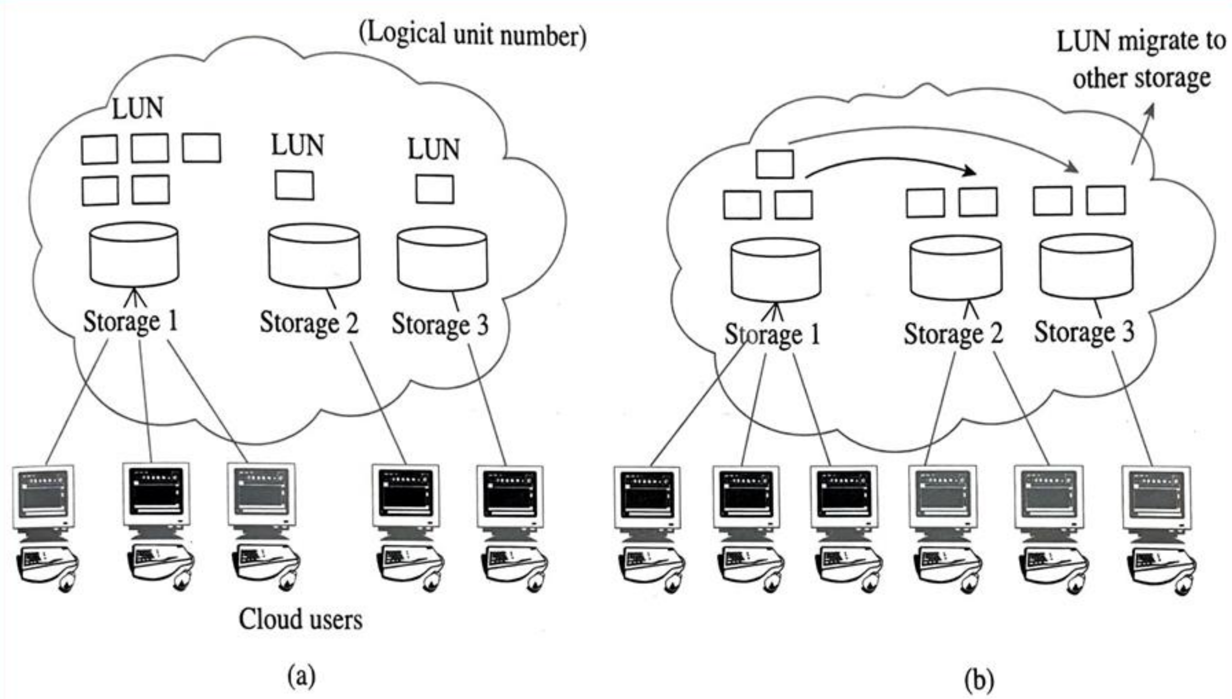


Fig. 3.4 (a) Uneven distribution of storage (b) Even distribution of storage

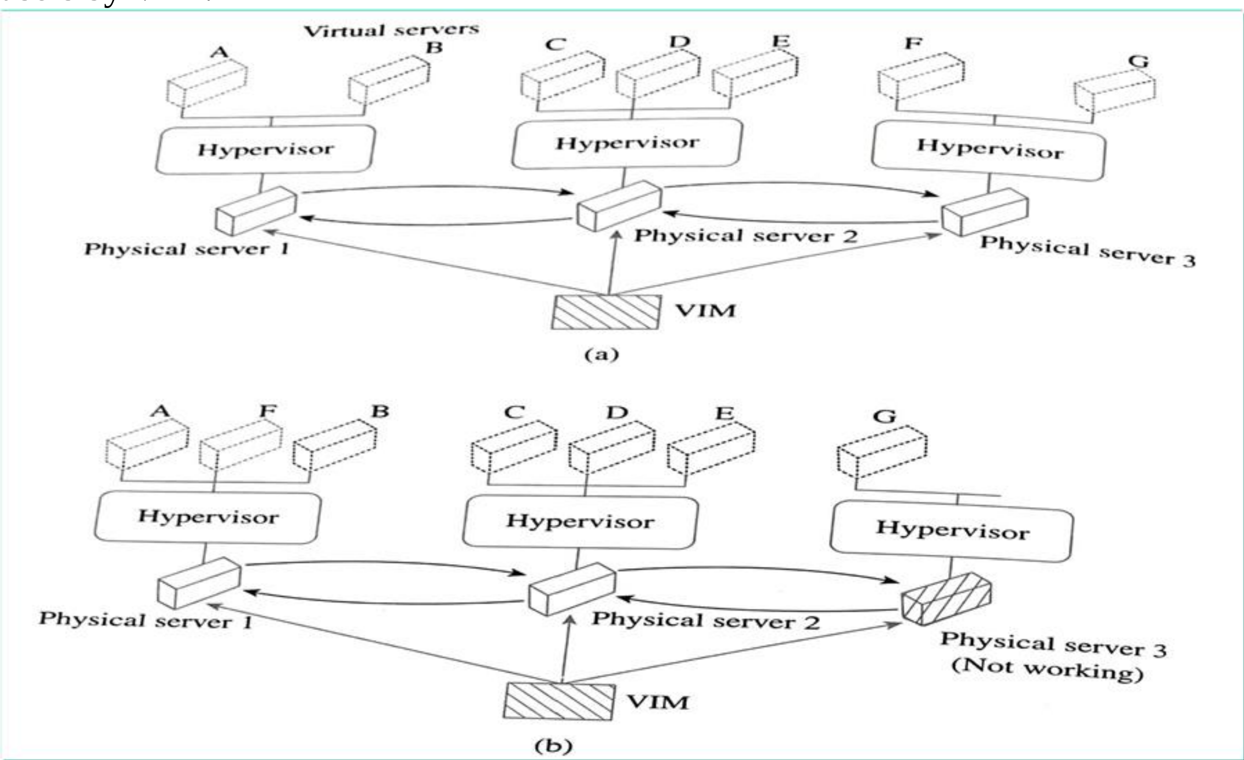
- For better data redundancy, secondary storage devices are placed at different geographical locations for making data recovery at the time of disaster.
- Over utilization of storage device causes performance degradation and underutilized resource, which storage potential not used.

- In the figure (a), Data is saved as Logical Unit Number (LUN). Various LUNs can be saved in a storage device as per the requirement.
- Storage 1 is overloaded as compared to Storage 2 and Storage 3.This is not even distribution of workload and better potential utilization of the resource is not in the distribution.
- In the figure (b), storage is redistributed among all the three storage resources.

On the Basis of Hypervisor Installed:

A hypervisor is responsible for creating many virtual servers from one physical server, but if the physical server falls due to any reason, then the virtual server fails as well. A virtual infrastructure manager (VIM) is responsible for maintaining and continuously monitoring a group of hypervisors. VIM initiates live migration of affected virtual machine in case of any failure.

Physical servers 1, 2, and 3 are working properly in Fig. 3.5(a). Here, as per the given Fig. 3.5(b), physical server 3 is not working properly and so the other server is not receiving any response. At this situation, virtual instances F and G are migrated to some other server dynamically without any disturbance to the cloud users by VIM.



On the Basis of Migration:

A mechanism that supports runtime transfer of virtual servers, from one to another is called Live Migration of a virtual machine. In Fig. 3.6, there are physical servers with name A and B. Virtualization software is used to make physical resource (server) available for the end users of cloud as virtual server.

Auto-scaling is possible in virtual server if the workload increases. If at run time there is need of migration, then the following steps have to be followed:

1. In the given Fig.3.6, work is overloaded on virtual server of physical server A, so VIM commands the hypervisor to suspend the execution of the busy physical server and migrate load to some other server.
2. The VIM instructs the instantiation of virtual server on an idle physical server. State information of busy server is getting synchronized with the idle server and now VIM instructs hypervisor to resume the virtual server processing without disturbing the cloud user data processing.

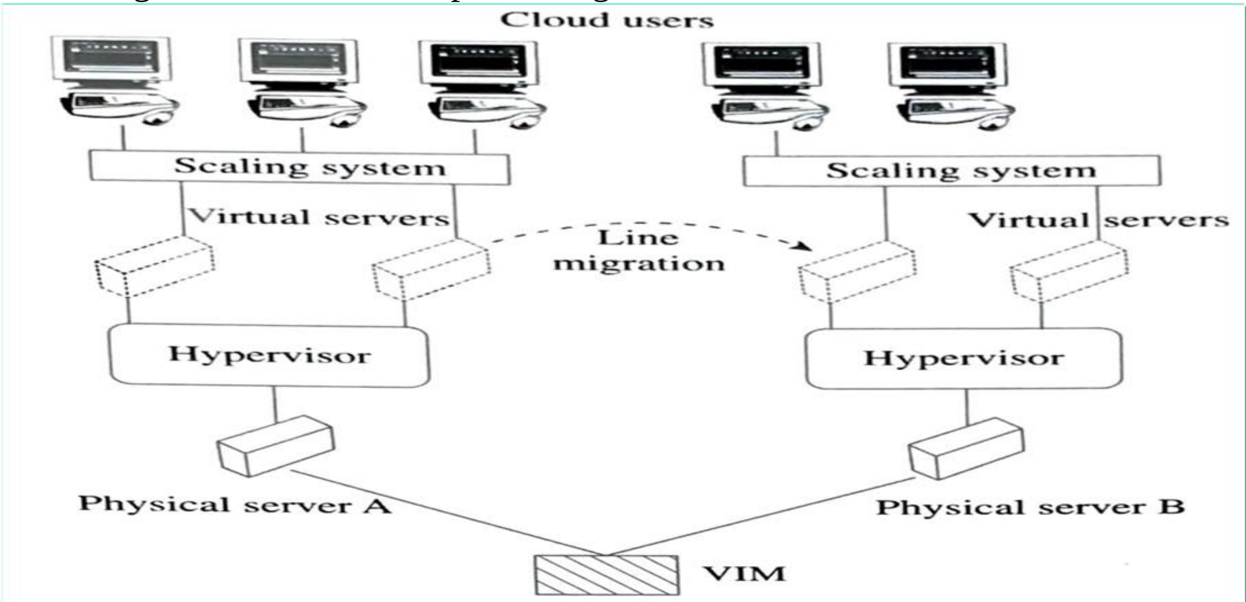


Fig. 3.6 Live Migration

For even distribution of workload, some time there is a need to migrate data from one storage device to another storage device. If the monitoring system in the cloud environment discovers uneven distribution of workload or if storage capacity of a storing device reaches to some threshold value as see in Fig.3.7(a), the LUN will be migrated to some other storage device as shown in Fig.3.7(b).

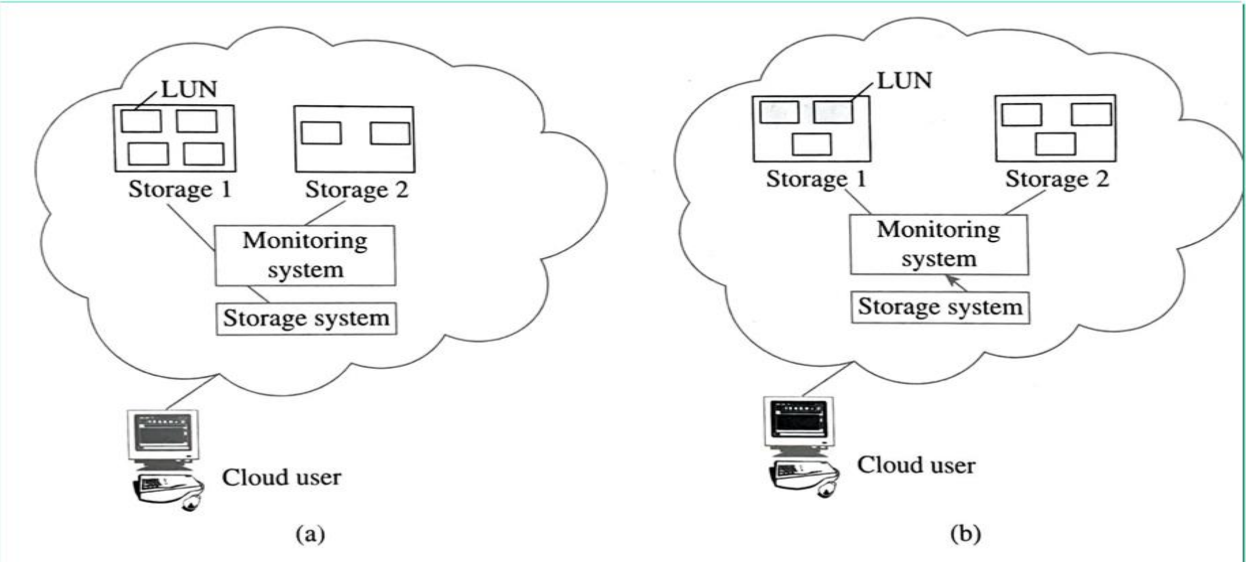


Fig. 3.7 (a) Uneven distribution of workload (b) Even distribution of workload

On the Basis of Service Relocation:

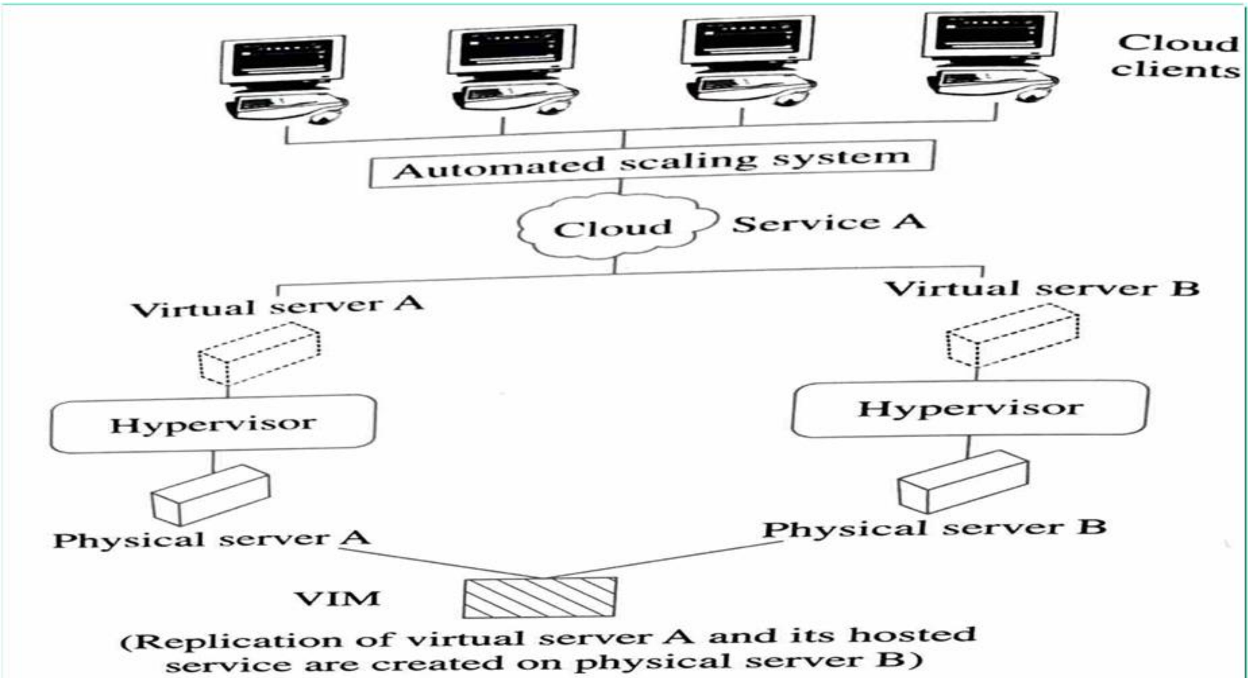


Fig. 3.8 Service relocation

Due to many reasons, some time for a particular instance of time, services of cloud are made unavailable to the cloud user. Some of the reasons are as follows:

1. Maintenance required due to any problem such as hardware failure, updating required, etc.

2. Migration of data and services from one machine to another
3. Processing capacity required by the cloud user exceeds the threshold value.

As in the given Fig.3.8 virtual servers A and its various hosted services of physical server A are initiated and migrated on physical server B.

On the Basis of Cloud Balancing:

This architecture is as per the cloud consumer request and to provide various services to cloud users. Such as:

1. Improved reliability and availability of resources
2. Proper load balancing of the resources for optimal utilization
3. Enhanced performance of the various IT resources.

Two Components in the figure. Those are

- Automated Scaling listener-> Aware of all redundant array of resources.
- Failover System-> Works at the time of failure in the cloud environment or IT resource

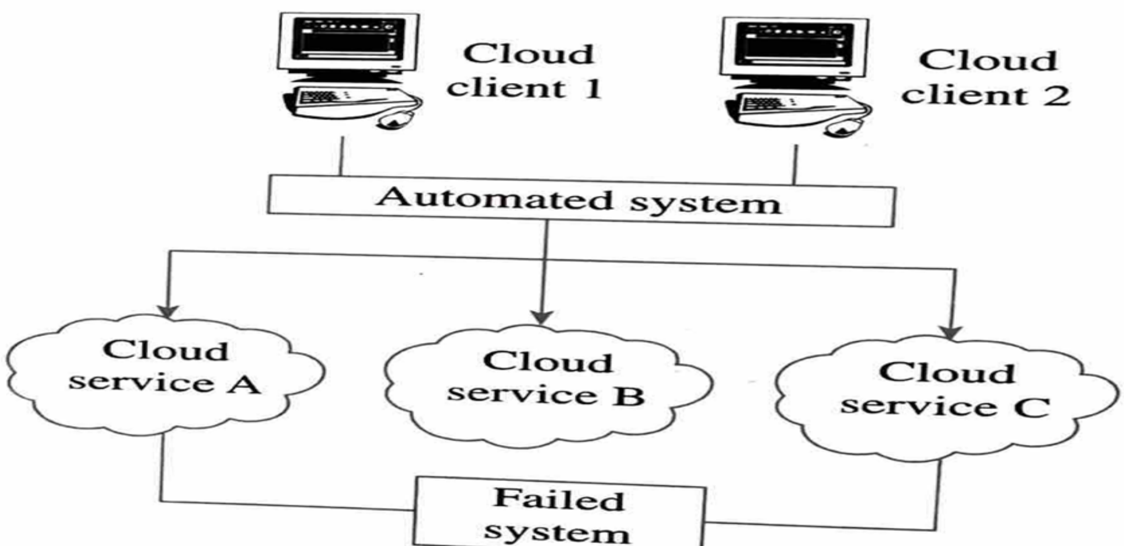


Fig. 3.9 Cloud balancing

On the Basis of Virtual Switches Load Balancing:

A physical uplink acts as an interface for cloud consumers and virtual resources. Physical uplink monitors the traffic in the cloud networks and all clients send requests through this link. As the number of users and service requests increases after crossing a threshold value, performance of the network goes down causing sensitive packet loss and many other problems in the network.

To overcome the above problem, multiple uplinks are added for proper balancing. Multiple and redundant path with multiple uplinks can easily handle network traffic and improve performance of the network

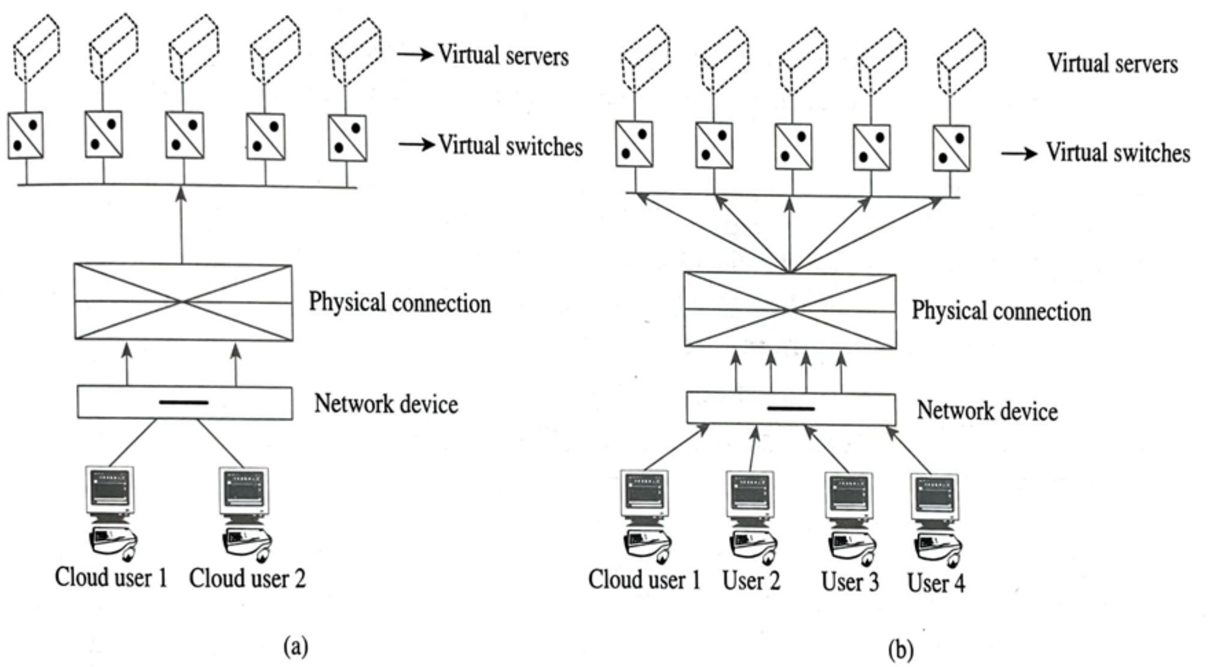


Fig. 3.10 (a) Single connection between network device and switches (b) Multiple connection between network device and switches

On the Basis of Failure Detection and Recovery:

A monitoring system works in the network to monitor activities in the network and it has some predefined functions that have to run at the time of particular events. Recovery policies are also defined in the system when automatic recovery occurs due to any failure of data center, new instances will be made available at another data center for proper cloud management and virtual images of resources are kept in the physical storage device.

6. KEY DESIGN ASPECTS OF CLOUD ARCHITECTURE, CLOUD SERVICES AND CLOUD APPLICATIONS

Apart from the various advantages of cloud computing, it also has various issues related to the architecture.

Issues at Design Level:

The key issue related to create an open architecture and the development of heterogeneous platforms.

Issues of Architectural of Cloud Computing:

Cloud computing architecture needs to support essential features such as separation, scalability, and reusability with flexibility. However, for the development of this type of architecture, developers face many challenges due to the new technologies and various industries requirement.

Platform related issues: With the increasing demand of cloud computing, there are various issues related to platform and infrastructure's development of cloud computing as per the user requirements.

Issues Related to the Implementation:

At the time of implementation of cloud service there are still some issues, such as

Issues related to Business: Organizations are sometimes interested to adopt cloud services for their various needs of IT industry but the cost but saves energy as well

Technical Issues: cloud environment also faces various issues related to technical specification that need to be solved at various levels but do not affect performance. These also include issues related to security.

7. SIMILARITIES AND DIFFERENCES BETWEEN GRID AND CLOUD COMPUTING

Difficult could understand the contrast between two kinds of computing as they are not dependent on one another. They are used for augmenting the consumption of the accessible resources.

A cloud computing design is planned to facilitate users to utilize distinct services without investing in the original design. Although grid proposes similar provision for computing control, cloud computing is not limited to merely that since cloud users may gain different services like website hosting.

Cloud computing:

Cloud computing is of specific advantage to small and medium-sized companies which desire to entirely outsource their data-center infrastructure or big corporations which desire to acquire peak load ability bearing the charge of constructing big data center. In both cases, service customers who's what they require on the internet and spend only for what they utilize.

Grid Computing:

Cloud computing develops from Grid computing and offers on-demand resource provisioning. Grid computing might or might not belong to the cloud, depending on the kinds of users using it. If the users are systems' integrators and managers,

they are concerned about how things are sustained in the cloud. They promote, virtualize, and deploy applications and servers.

Grid computing needs the use of software which may separate and pass on parts of a program as single big system picture to numerous computers. One worry regarding grid is that if single part of the software on a joint crashes, other parts of the software other joints might crash too. This is relaxed in case that constituent has a failover constituent on another joint. But trouble may yet take place if constituents rely on their parts of software to achieve one or more grid computing responsibilities. Big system pictures and related hardware to run and sustain them can donate to huge assets and functioning costs.

Similarities and Differences:

Similarities:

- Grid computing and cloud computing are scalable.
- Grid and cloud computing offer service-level agreements (SLAs) for uptime accessibility of around 99 per cent. If the service slides below the definite uptime service level, the service credit for receiving data to the customer gets delayed.
- The Amazon S3 offers a web services' interface for the recovery and storage of data in the cloud.

Differences:

- Cloud computing offers SaaS applications, whereas grid computing is used when the processing authority of service or an application is distributed across multiple systems.
- With cloud computing, the corporation acquires feasibility and expense savings, whereas with grid computing the corporation acquires suppleness and authority.
- By separating the logical from the physical resources, virtualization determines a few of the challenges met by grid computing. While grid computing attains high consumption via the allotment of numerous servers on a particular job or assignment, the virtualization of servers in cloud computing attains high consumption by permitting single server or compute numerous responsibilities concurrently.