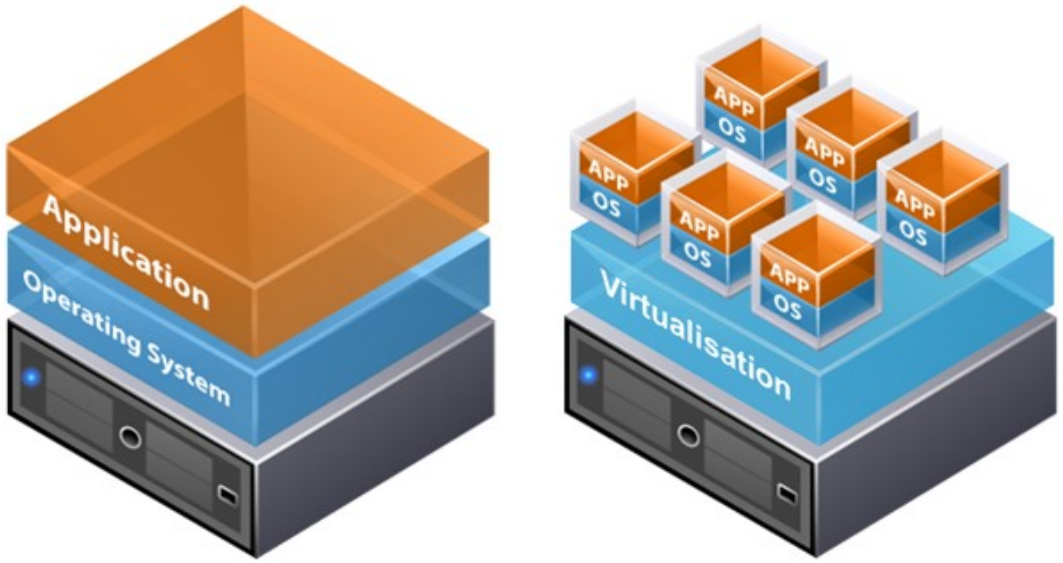
Virtualisation and the Cloud

Platform Technologies

Based on Tanenbaum, Modern Operating Systems

Virtualisation

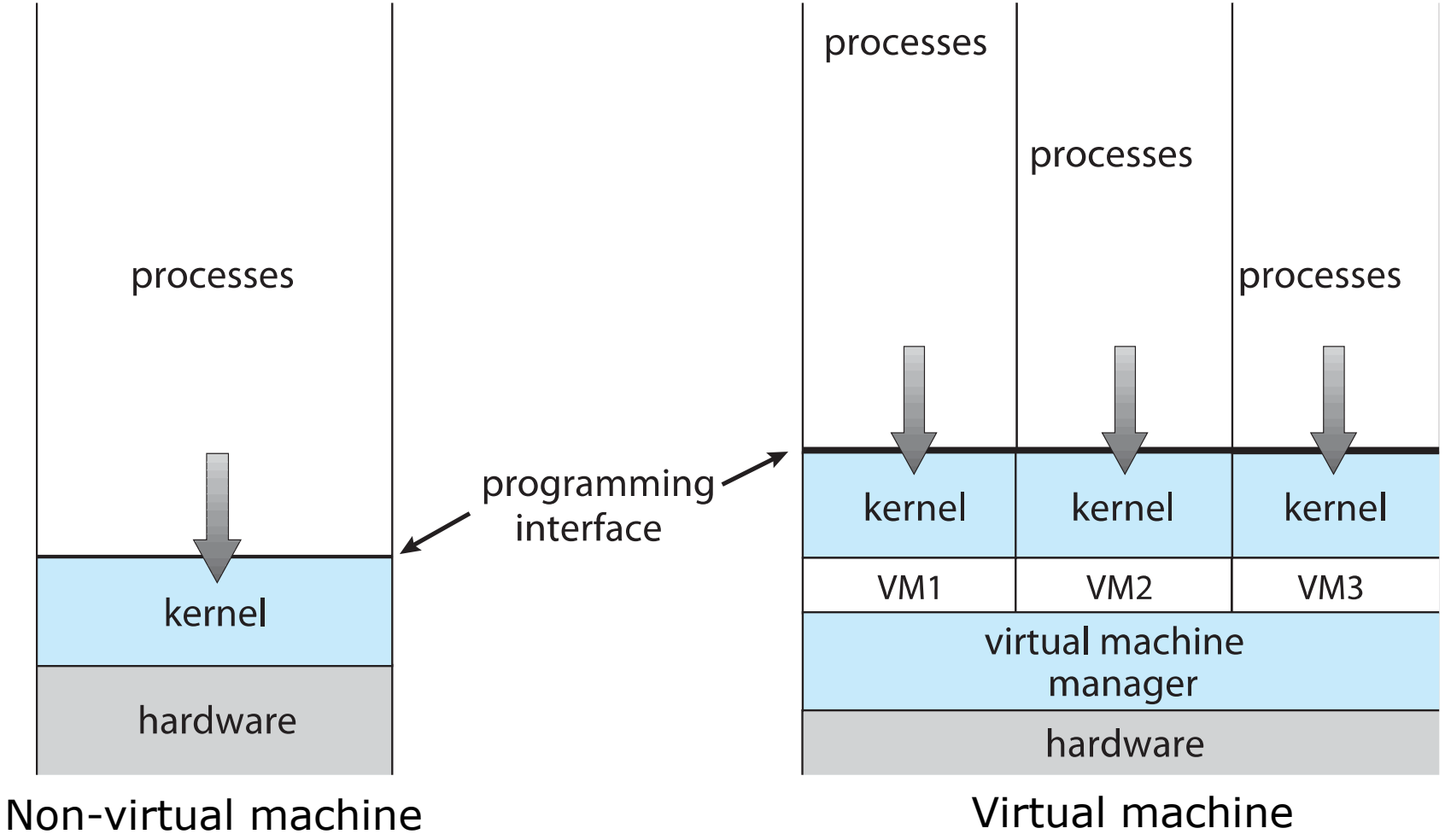
- Fundamental idea – abstract hardware of a single computer into several different execution environments
- Single physical machine can run multiple operating systems **concurrently**, each in its own isolated virtual machine environment



Traditional Architecture

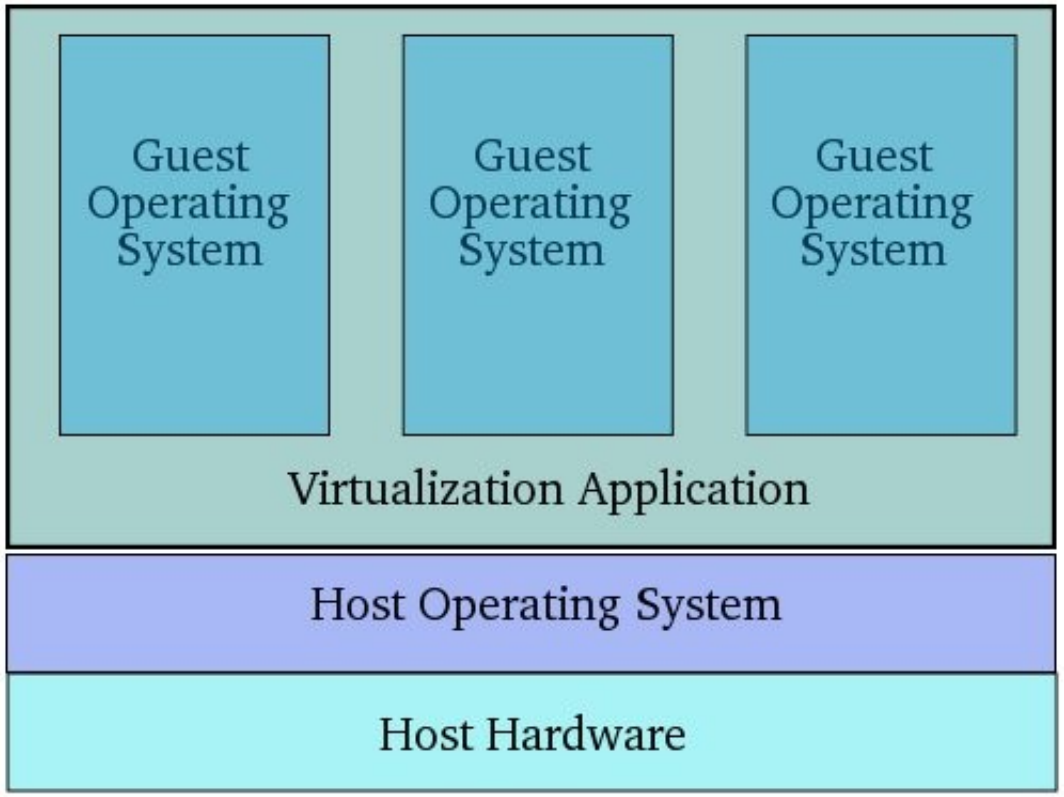
Virtual Architecture

Virtualisation



Virtualisation Components

- **Host**
  - Underlying hardware system
- **Virtual machine manager** (**VMM**) or **hypervisor**
  - Creates and runs virtual machines by providing interface to share available hardware resources from the host to the guest
- **Guest**
  - Operating system running on VMM



History

- First appeared in IBM mainframes in 1972
- Allowed multiple users to share a batch-oriented system
- Formal definition of virtualisation helped move it beyond IBM
  1. A VMM provides an environment for programs that is essentially identical to the original machine
  2. Programs running within that environment show only minor performance decreases
  3. The VMM is in complete control of system resources
- In late 1990s, Intel CPUs became fast enough for researchers to try virtualizing on general purpose PCs
  - **Xen** and **VMware** created technologies, still used today
  - Virtualisation has expanded to many OSes, CPUs, VMMs

Benefits and Features

- Creates independent user environments
  - Host system protected from VMs, VMs protected from each other
  - Sharing is provided though via shared file system volume, network communication
- Reduce downtime and enhance resiliency
  - Freeze and **suspend** a currently running VM
  - Then can move or copy somewhere else and **resume**
  - Snapshot of a given state, able to restore back to that state
  - Some VMMs allow multiple snapshots per VM

Benefits and Features

- **Consolidation**
  - Run multiple, different OSes on a single machine, for different purposes such as app dev, testing, etc. on different platforms
- **Templating**
  - Create an OS + application VM, provide it to customers, use it to create multiple instances of that combination
- **Live migration**
  - Move a running VM from one host to another without interruption to users

Benefits and Features

- All those features taken together -> **cloud computing**
  - Using APIs, programs tell cloud infrastructure (servers, networking, storage) to create new guests, VMs, virtual desktops
- Great for OS research, better system development efficiency

Types of VMs and Implementations

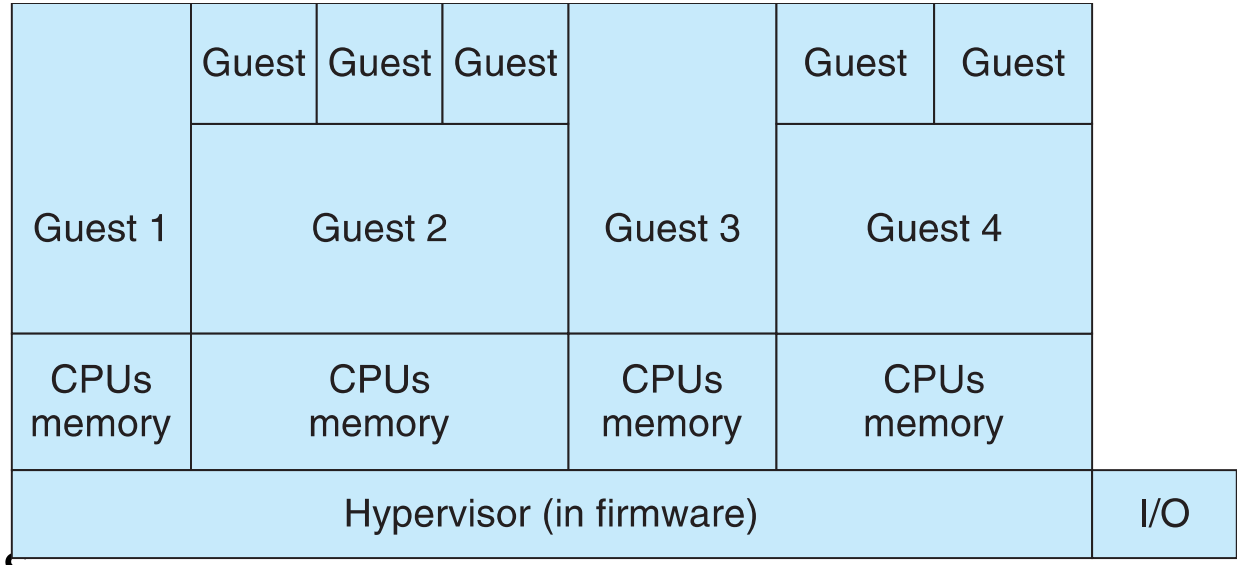
- Many variations as well as HW details
  - Assume VMMs take advantage of HW features
- Steps simpler, faster than with a physical machine install
  - Can lead to **virtual machine sprawl** with lots of VMs, history and state difficult to track

Types of VMs and Implementations

- Whatever the type, a VM has a lifecycle
  - Created by VMM
  - Resources assigned to it (number of cores, amount of memory, networking details, storage details)
  - In type 0 hypervisor, resources usually dedicated
  - Other types dedicate or share resources, or a mix
  - When no longer needed, VM can be deleted, freeing resources

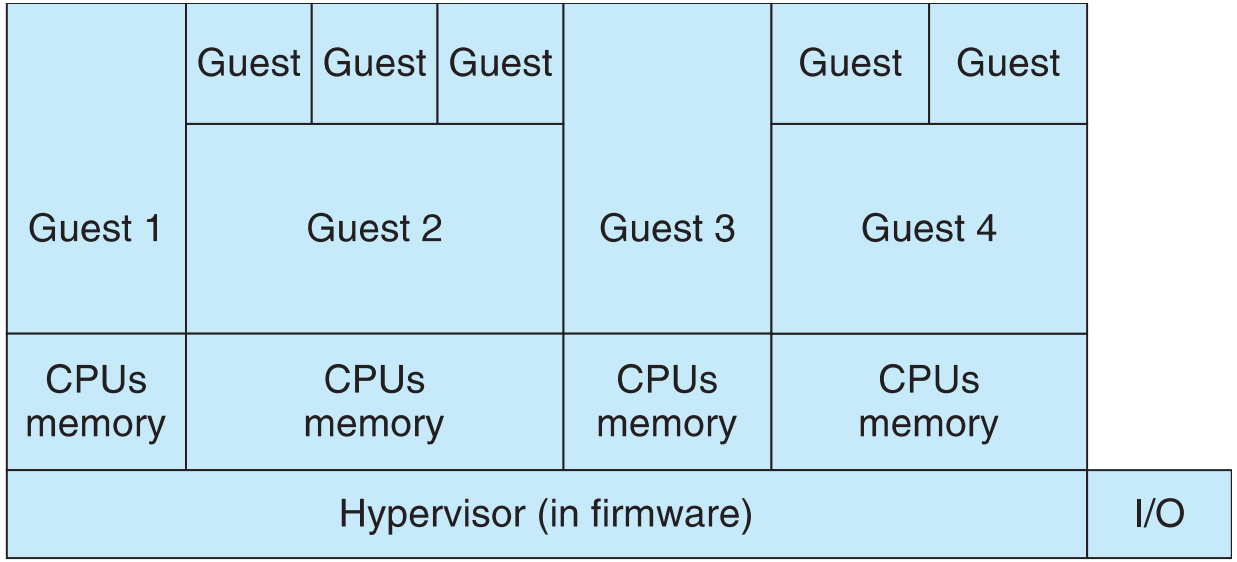
Types of VMs – Type 0 Hypervisor

- Oldest VM idea
- From different HW manufacturers
- VMM is a HW feature
- Implemented by firmware
- OS need to nothing special
- Smaller feature set than other types
- “Partitions”, “Domains”
- Each guest has dedicated HW



Types of VMs – Type 0 Hypervisor

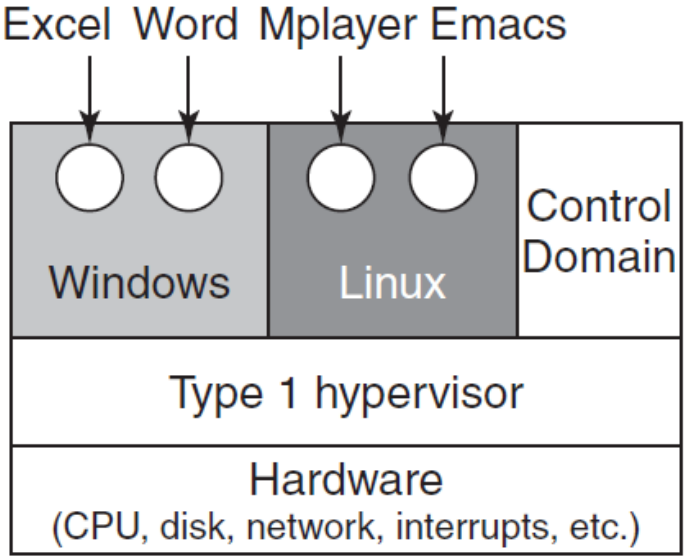
- I/O a challenge as difficult to have enough devices, controllers to dedicate to each guest
- Sometimes VMM implements a **control partition** running daemons that other guests communicate with for shared I/O



- Can provide virtualisation-within-virtualisation
  - Guest itself can be a VMM with guests, other types have difficulty doing this

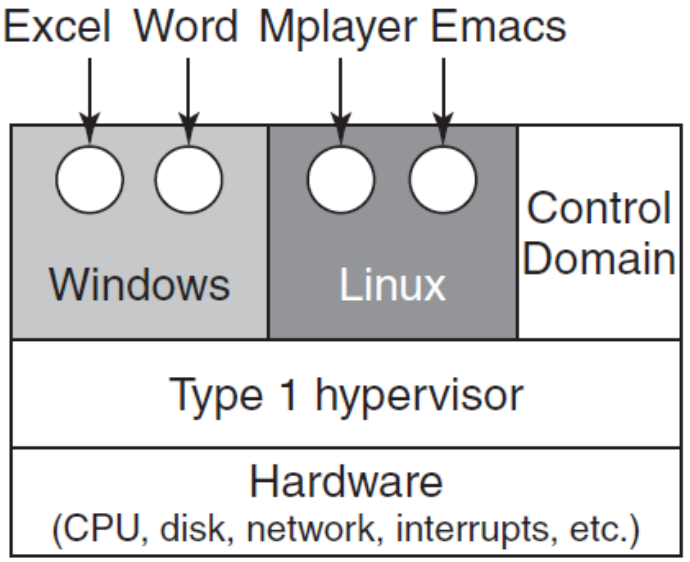
Types of VMs – Type 1 Hypervisor

- Special purpose operating systems that run natively on HW
- Consolidation of multiple OSes and apps onto less HW
- Move guests between systems to balance performance
- Commonly found in datacenters
- Datacenter managers control and manage OSes in new, sophisticated ways by controlling the Type 1 hypervisor
- Snapshots and cloning



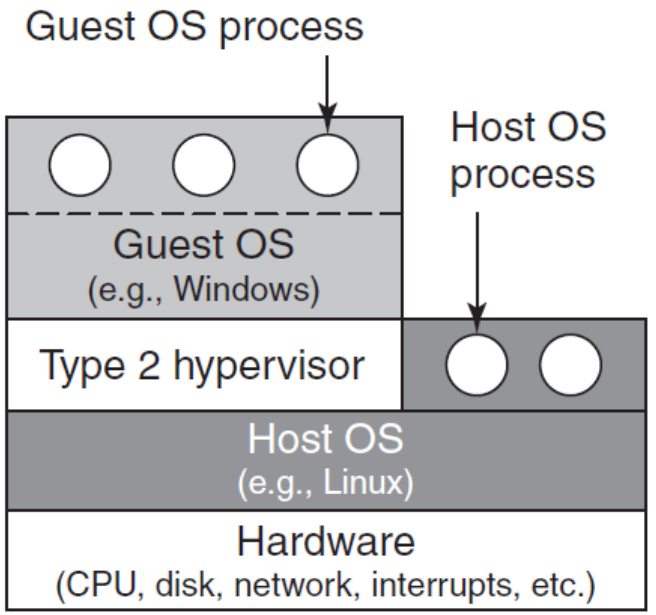
Types of VMs – Type 1 Hypervisor

- Run in kernel mode
- Can run on top of Type 0s but not on other Type 1s
- Guests generally don't know they are running in a VM
- Rather than providing system call interface, create run and manage guest OSes
- Implement device drivers for host HW because no other component can
- Also provide other traditional OS services like CPU and memory management

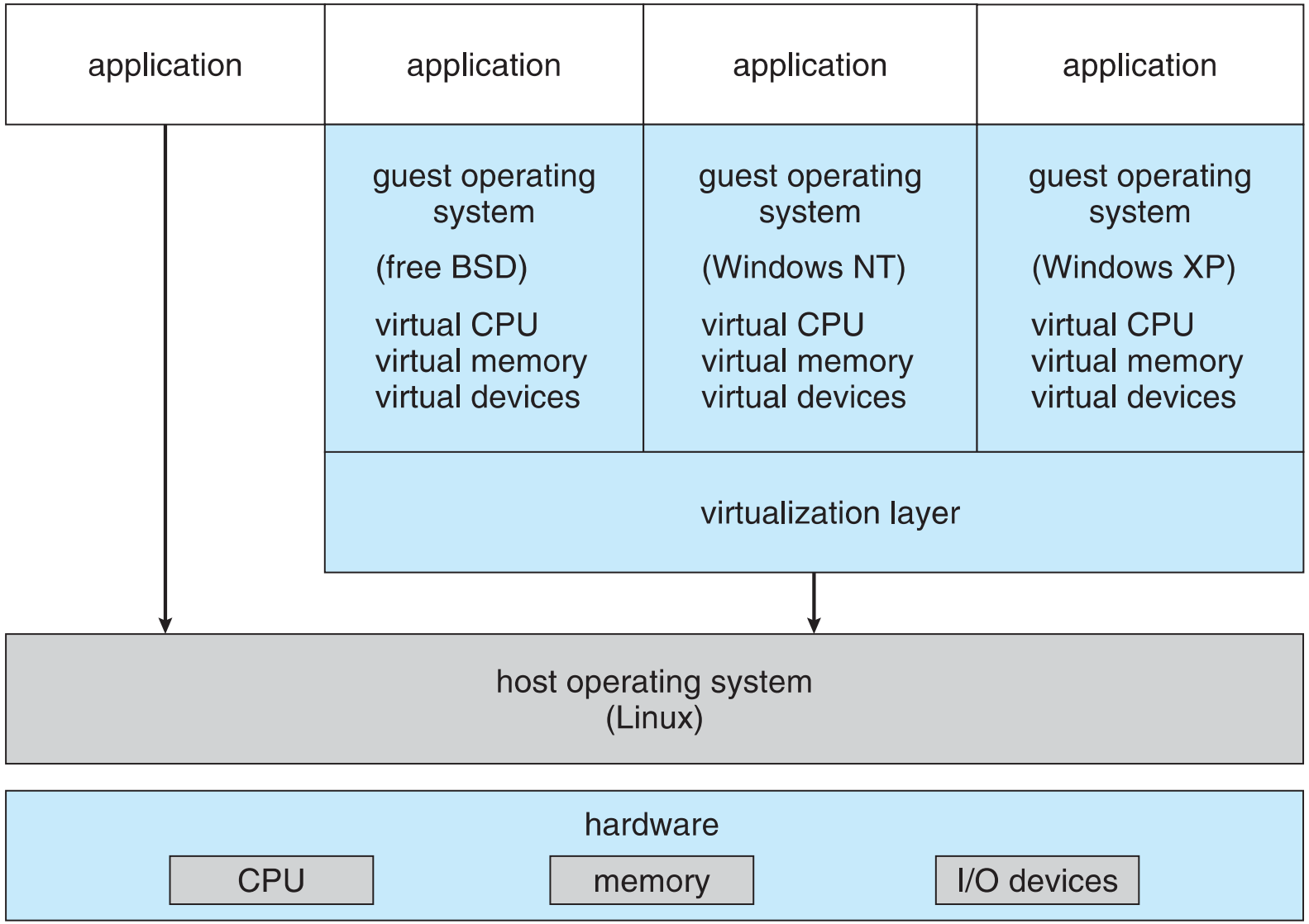


Types of VMs – Type 2 Hypervisor

- Very little OS involvement in virtualisation
- VMM is simply another process, run and managed by host
  - Even the host doesn't know they are a VMM running guests
- Tend to have poorer overall performance because can't take advantage of some HW features
- But also a benefit because require no changes to host OS
  - Student could have Type 2 hypervisor on native host, run multiple guests, all on standard host OS such as Windows, Linux, MacOS



Example - VMware

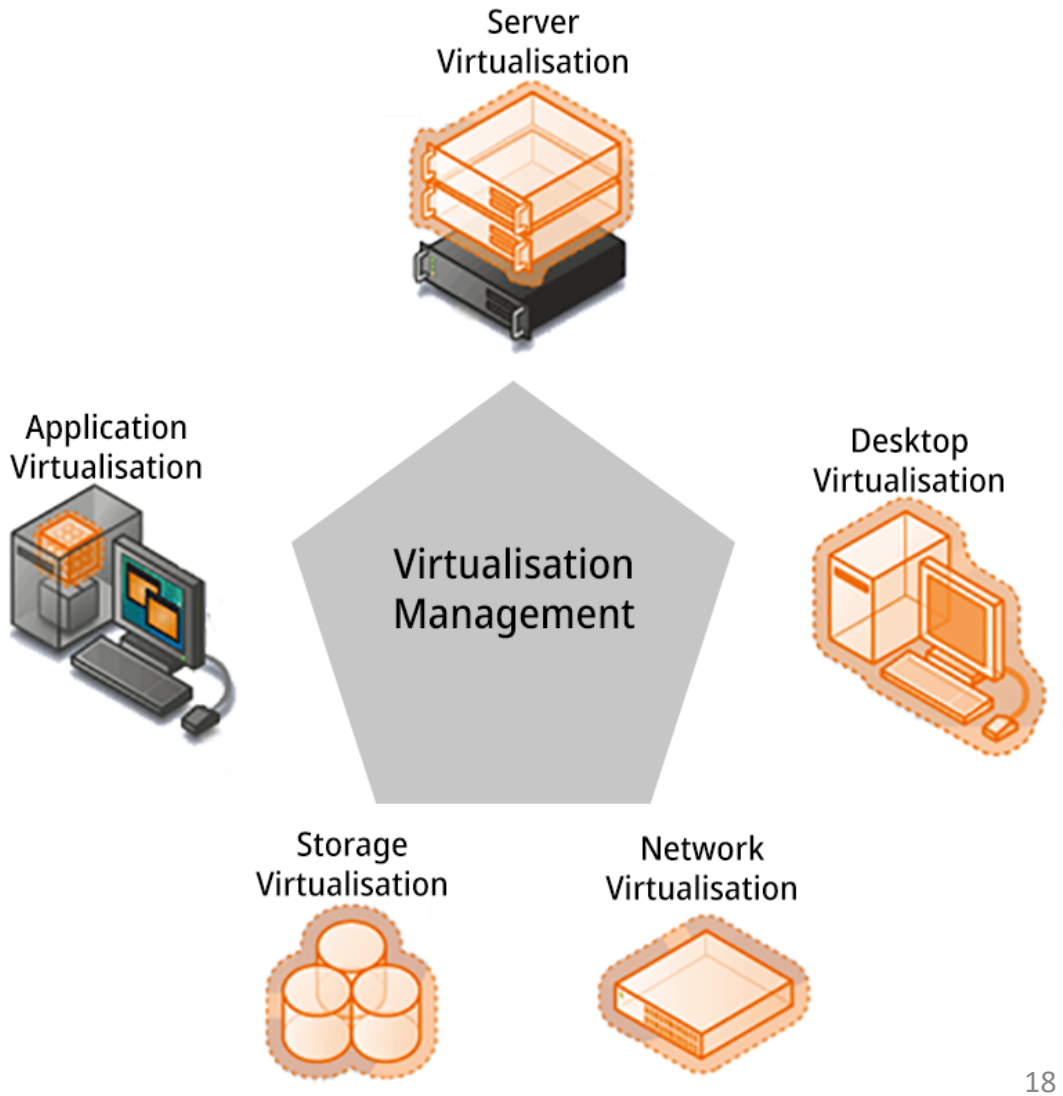


Example - VMware

- VMware Workstation runs on x86, provides VMM for guests
- Runs as application on other native, installed host operating system -> Type 2
- Lots of guests possible, including Windows, Linux, etc all runnable concurrently (as resources allow)
- Virtualisation layer abstracts underlying HW, providing guest with is own virtual CPUs, memory, disk drives, network interfaces, etc
- Physical disks can be provided to guests, or virtual physical disks (just files within host file system)

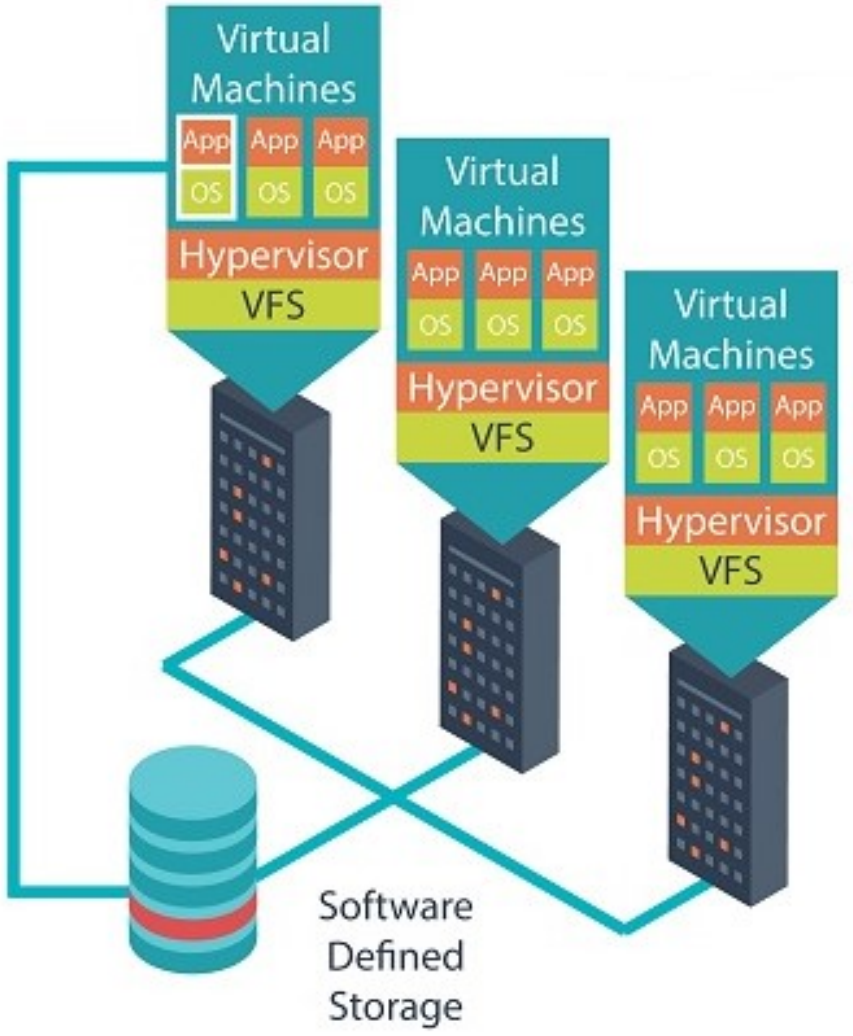
Types of Virtualisation Technologies

- Server Virtualisation
- Desktop Virtualisation
- Application Virtualisation
- Storage Virtualisation
- Network Virtualisation



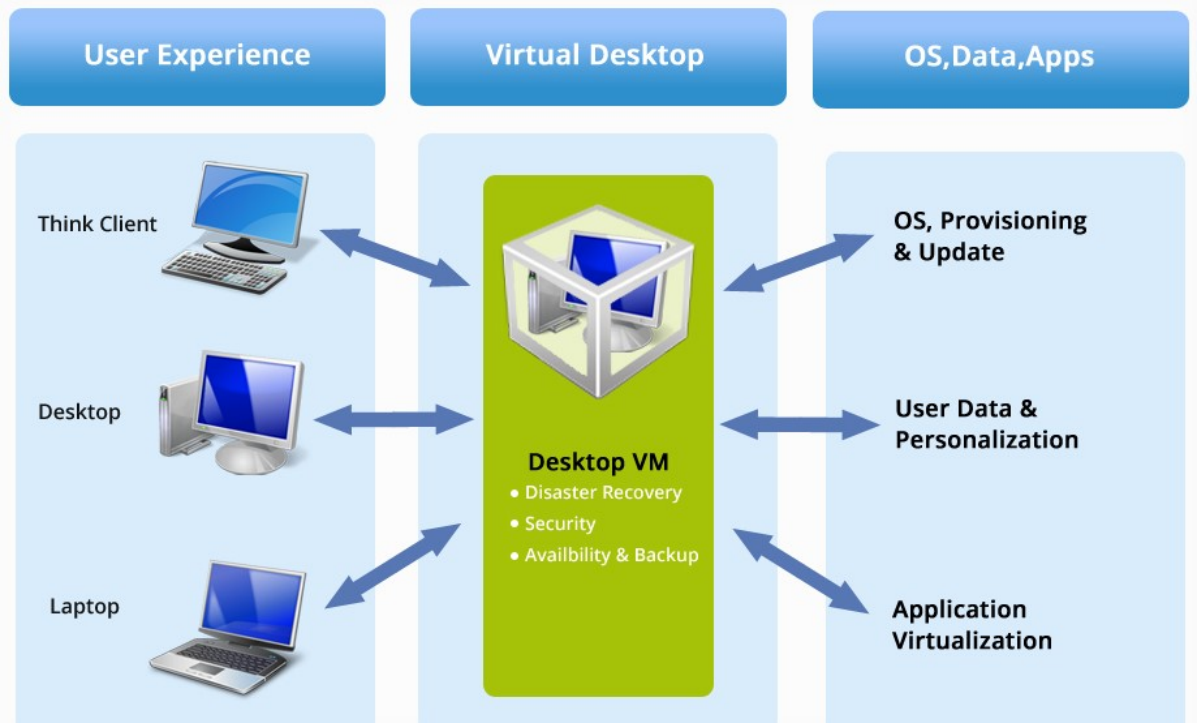
Server Virtualisation

- Dividing a physical server into multiple unique and isolated virtual servers.
- Each virtual server can run its own operating systems.
- Key Benefits:
  - Higher server ability
  - Cheaper operating costs
  - Eliminate server complexity
  - Increased application performance
  - Deploy workload quicker
- Examples: Citrix Hypervisor, VMware vSphere, Red Hat Virtualisation (RHV)



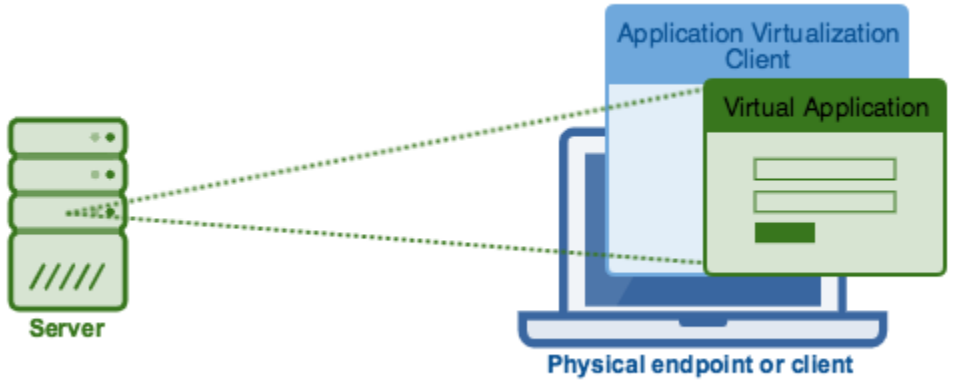
Desktop Virtualisation

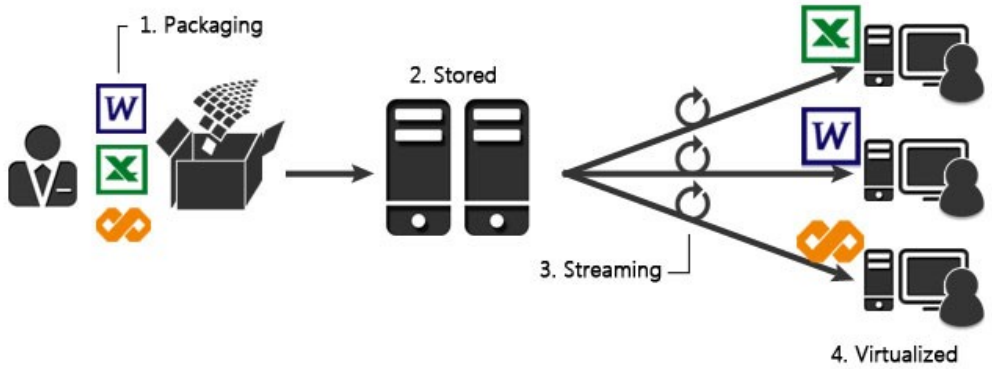
- Creates a software-based virtual versio
  an end user's desktop environment.
- Separates the desktop environment and
  applications from the physical client de
  used to access it.
- Key benefits:
  - Simpler administration
  - Resource Management
  - Remote Working
  - Stronger security
- Examples: Citrix XenDesktop, VMware Horizon View, Microsoft Hyper-V



Application Virtualisation

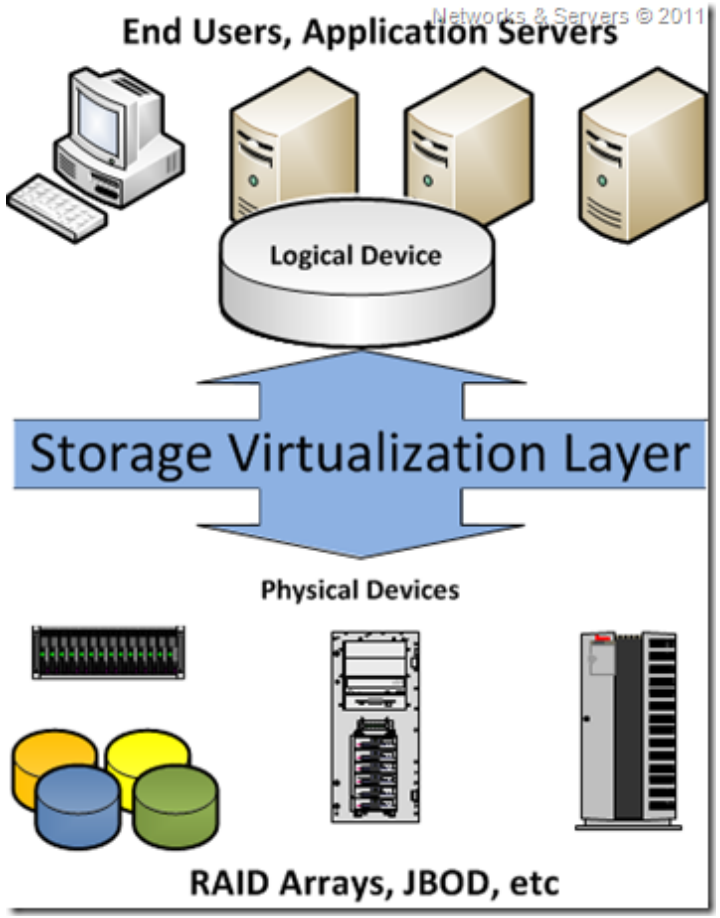
- Access and use an application from a separate computer than the one on which the application is installed
- Same user experience as using the installed app on a physical machine
- Key benefits:
  - Application management
  - Support legacy applications
  - Scalability
  - Security
- Examples: Citrix XenApp, VMware ThinApp, Microsoft App-V





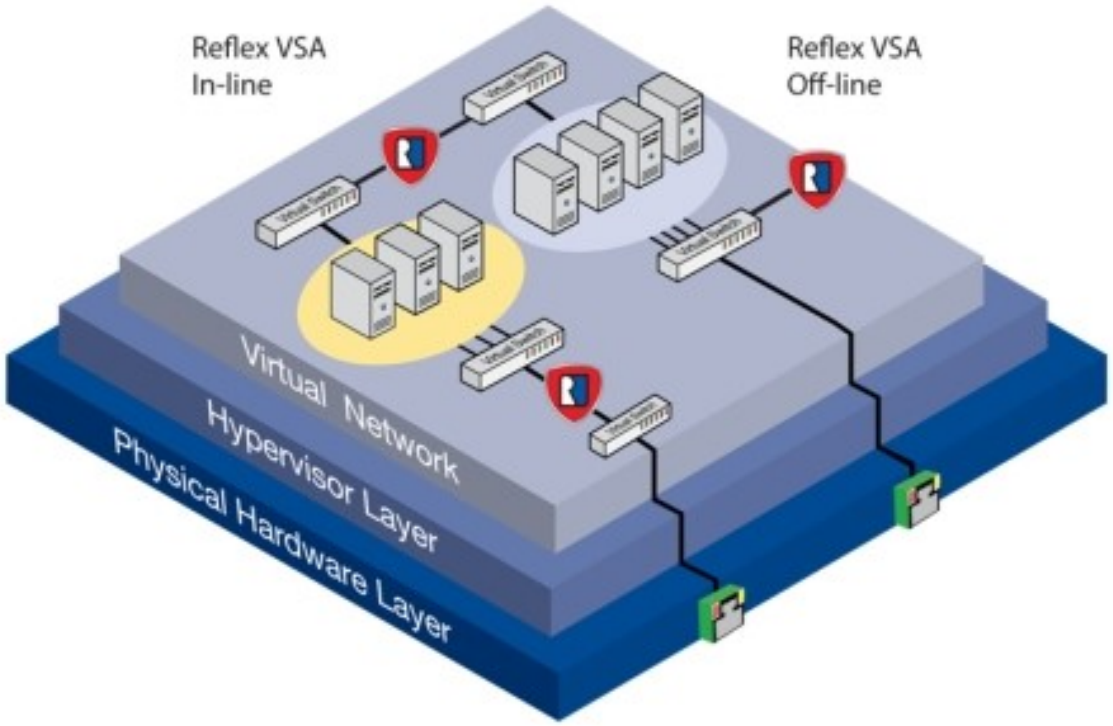
Storage Virtualisation

- Physical storage from multiple devices on a network is pooled together in a unified virtual storage device
- Sometimes called software-defined storage or a virtual SAN
- Key benefits:
  - Non-disruptive data migration
  - Reliability and performance
  - Maximise utilisation
  - Reduce costs



Virtualisation Security Requirements

- A secure network interface
  - Transport layer security (TLS)
- A secure secondary storage
  - Network File System (NFS)
- A secure run-time environment
  - Build, save, restore, destroy
  - All the cryptographic algorithms and security protocols reside in the run-time environment



Cloud Computing

- Virtualisation technology played a crucial role in the rise of cloud computing.
- Cloud providers typically offer different categories of resources, such as ‘‘big machines’’ versus ‘‘little machines,’’ etc.
- Can be private (to an organisation), or public (to anyone)
- Can access to physical hardware, or virtualise their environments
- Can be only bare machines, or offered with ready to use software

Characteristics of Clouds

- Five essential characteristics of clouds according to the National Institute of Standards and Technology:

1. **On-demand self-service.** Users should be able to provision resources automatically, without requiring human interaction.
2. **Broad network access.** All these resources should be available over the network via standard mechanisms so that heterogeneous devices can make use of them.

Characteristics of Clouds

3. **Resource pooling.** The computing resource owned by the provider should be pooled to serve multiple users and with the ability to assign and reassign resources dynamically. The users generally do not even know the exact location of ‘‘their’’ resources or even which country they are located in.
4. **Rapid elasticity.** It should be possible to acquire and release resources elastically, perhaps even automatically, to scale immediately with the users’ demands.
5. **Measured service.** The cloud provider meters the resources used in a way that matches the type of service agreed upon.

Clouds as a Service

- **SAAS** (**Software As A Service)**
  - offers access to specific software, such as Microsoft Office 365 or Google Apps
- **PAAS** (**Platform As A Service)**
  - delivers an environment that includes things such as a specific OS, database, Web server, and so on
- **IAAS** (**Infrastructure As A Service**)
  - offer direct access to a virtual machine, which the user can use in any way
  - example of an IAAS cloud is Amazon EC2

Clouds as a Service

- Clouds can transform the way companies do computing.
- Benefits from economy of scale,
  - Consolidating the computing resources in a small number of places
  - Conveniently located near a power source and cheap cooling
- No need to worry so much about managing the IT infrastructure, backups, maintenance, depreciation, scalability, reliability, performance, and perhaps security.

Cloud Computing vs. Virtualisation

	Cloud	**Virtualization**
Definition	Methodology	Technology
Purpose	Pool and automate virtual resources for on-demand use	Create multiple simulated environments from 1 physical hardware system
Use	Deliver variable resources to groups of users for a variety of purposes	Deliver packaged resources to specific users for a specific purpose
Configuration	Template-based	Image-based
Lifespan	Hours to months (short-term)	Years (long-term)
Cost	Private cloud: High CAPEX, low OPEX Public cloud: Low CAPEX, high OPEX	High capital expenditures (CAPEX), Low operating expenses (OPEX)
Scalability	Scale out	Scale up
Workload	Stateless	Stateful
Tenancy	Multiple tenants	Single tenant

From: https://www.redhat.com/en/topics/cloud-computing/cloud-vs-virtualization

Emerging Challengers with Clouds

- Can you really trust a cloud provider to keep your sensitive data safe?
- Will a competitor running on the same infrastructure be able to infer information you wanted to keep private?
- What law(s) apply to your data? *(for instance, if the cloud provider is from the United States, is your data subject to the PATRIOT Act, even if your company is in Europe or Asia)*
- Once you store all your data in cloud X, will you be able to get them out again, or will you be tied to that cloud and its provider forever, something known as **vendor lock-in**?