10.7.25

CO-2

Virtualization

Introduction

- Need for Virtualization
  - It is the core technology of cloud computing
  - It appears appealing to the users
  - It helps for the sustainability for CSP.

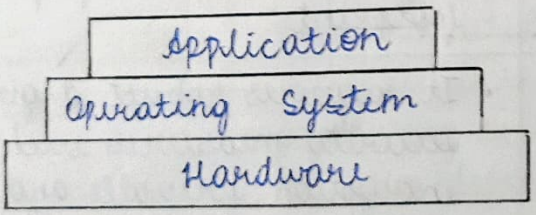
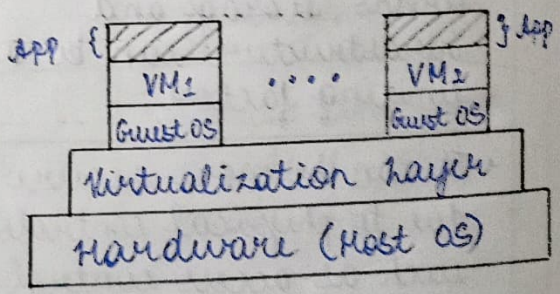
- Physical Resource vs Virtual Resource

Physical Resource	Virtual Resource
• It refers to any hardware equipments like processors, work stations, servers, networking devices, storage devices, peripheral devices	• It represents a digital replicated version of something real
• Limited scalability, requires hardware upgrades or addition can be time consuming and costly	• Highly scalable, can be easily increased or decreased as needed. Often automated and cost effective
• Requires physical space for servers, storage and infrastructure can be a limiting factor	• No physical space required, can be accessed from anywhere, reduces physical footprint
• It can be more secure due to physical controls such as access control and surveillance	• It requires robust digital security measures such as encryption, firewalls and access controls to protect against cyber threats
• It can be more complex & time consuming as it requires physical access to hardware	• Data recovery can be faster and more efficient, often automated and cloud based
• Limited flexibility, requires physical upgrades or changes	• Highly flexible, can be easily scaled, modified or reconfigured as needed, often automated

- Virtual Machine
  - It is a digitalized replicated version of a physical machine
  - Every virtual machine requires same set of requirements as in case of a physical machine
  - A computer running inside a computer is called as a virtual machine

- Virtualization
  - It is the process of conversion of a single physical resource into multiple virtual resources
  - Virtualization layer is responsible for:
    1) Creation of virtual machines
    2) Allocation of resources for virtual machines
    3) Coordination among the virtual machines

- Traditional Architecture vs Virtualization Architecture

Traditional Architecture	Virtualization Architecture
	
• Only a single instance can run in the traditional architecture	• Multiple instances can be parallely executed in the virtualization architecture
• Hardware and software are tightly coupled	• Hardware and software are loosely coupled
• Under utilization of resources	• Efficient utilization of resources
• Cost of infrastructure is high	• Cost of infrastructure is low (pay for use)

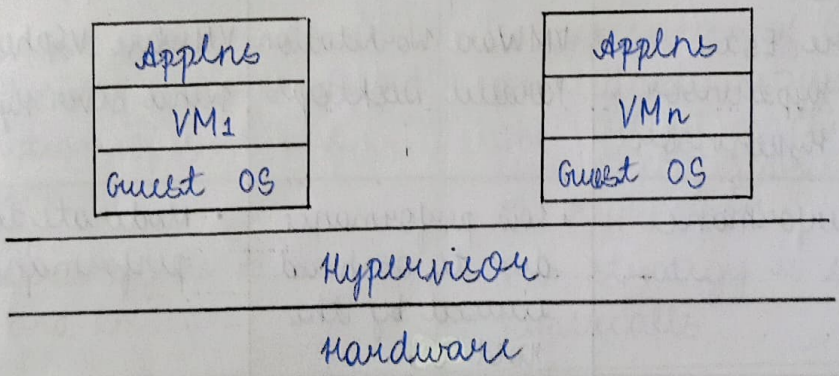
• Running different applications with different configurations in the same environment results in conflicts	• Easy to run different applications with different configurations in the same environment

14 · 7 · 25

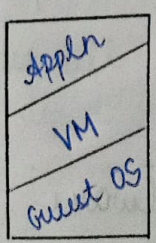
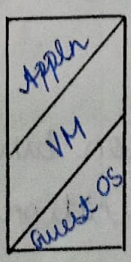
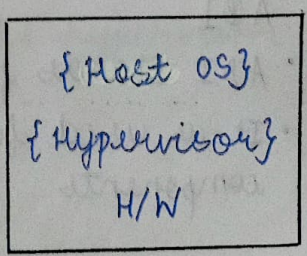
• Hypervisor

- The other name of Hypervisor is Virtual Machine Monitor (VMM).
- Hypervisor is a software program that manages multiple operating systems or multiple instances of a same operating system in a single piece of hardware
- There are three types of hypervisors namely:
  1) Bare Metal Hypervisor / Type 1
  2) Hosted Hypervisor / Type 2
  3) Embedded Hypervisor

* Users cannot directly access hardware, that's why hypervisor is placed in between the VMs and hardware



• Types

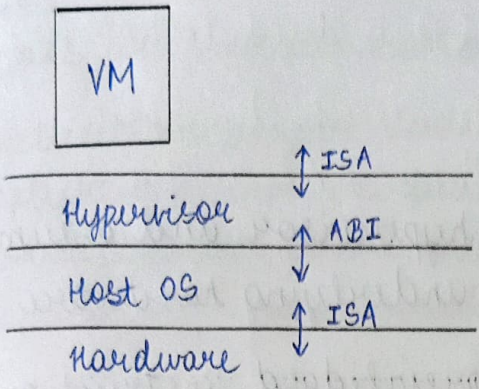
Bare Metal Hypervisor / Type 1	Hosted Hypervisor / Type 2	Embedded Hypervisor
		

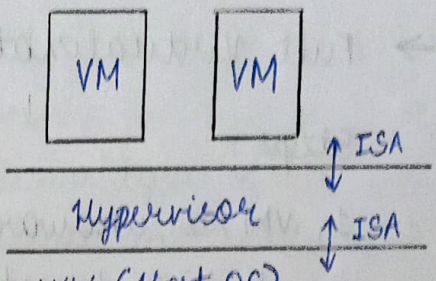
• Hypervisor runs on top of the hardware • Hypervisor prevents direct communication b/w VMs and underlying hardware	• Host OS runs on top of the hardware in a separate layer • Has overhead so the performance is low	• Hardware, hypervisor along with Host OS is embedded into a single software
• Guest OS runs at level 2 from the hardware	• Guest OS runs at level 3 from the hardware	• Guest OS runs on the same level as the hardware
• This type of hypervisor is used in server virtualization and provides high level of isolation	• This type of hypervisor is used in desktop virtualization	• It provides high level of security especially in case of control automated manufacturing/ control automated devices
• Examples: VMWare Esxi Citrix Hypervisor Xen Hypervisor	• Examples: VMWare Workstation Parallel Desktops	• Examples: VMWare VSphere Wind River Hypervisor
• High performance	• Low performance due to overhead caused by the host OS	• Moderate to high performance

15.7.25

- ISA
  - ISA stands for Instructure Set Architecture
  - It is used for communication b/w a h/w & s/w component

- ABI
  - ABI stands for Application Binary Interface
  - It is used for communication b/w two software components





- Levels of Virtualization

Full Virtualization	Para Virtualization
• It is an environment in which the virtual machines are completely unaware that execution of priviledged instructions w.r.t. the underlying hardware is not in their control	• It is an environment in which the virtual machines are aware that they cannot execute any priviledged instruction directly with the underlying hardware
• Hypervisor decides the execution of every priviledged instruction of a virtual machine	• For execution of any priviledged instruction, the virtual machine communicates directly with the hypervisor
• This strategy is called as Trap and Emulate	• This strategy is called as Hypercalls

a) Illustrate the steps involved for the execution of priviledged instructions like accessing memory, accessing input output devices in an environment with full virtualization & para virtualization

- Hypercall
  - It is a request sent by Guest OS to the hypervisor

→ Full Virtualization

Steps:

1. VM is unaware about hypervisor and assumes it lies directly above underlying hardware.
2. Hypervisor traps the priviledged instruction
3. Check if safe to execute in underlying hardware if so executes it (emulate)
4. VM assumes that instruction is executed successfully in underlying hardware

Para Virtualization

Steps:

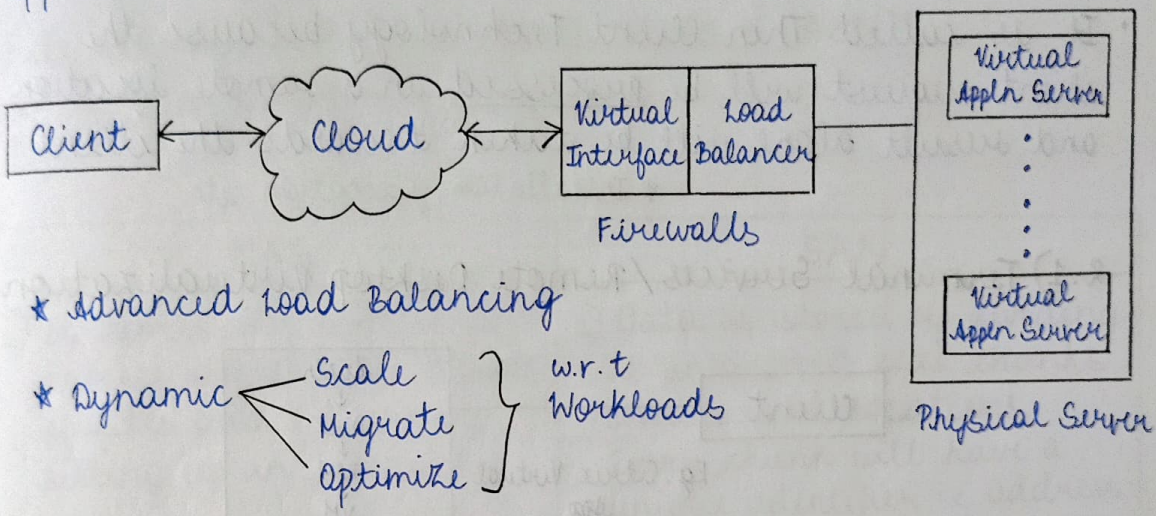
1. VM sends the hypercall
2. Hypervisor decides if the instruction does not affect the underlying hardware, it executes

17.7.25

Types of Virtualization

1) Application Server Virtualization

- Application Server Virtualization is a type of virtualization where multiple virtual instances of application server resides in a single physical server



* Advanced load Balancing
* Dynamic
  - Scale
  - Migrate
  - Optimize

  } w.r.t Workloads

* For 5 Mark question, write about:
  - Firewalls
  - Advanced load Balancing
  - Dynamic Features

* Advanced load Balancing
  - Manages heterogeneous applications too, apart from homogeneous
  - Bringing multiples servers into single machine

* Migrate
  - Server migration
  - Server consolidation

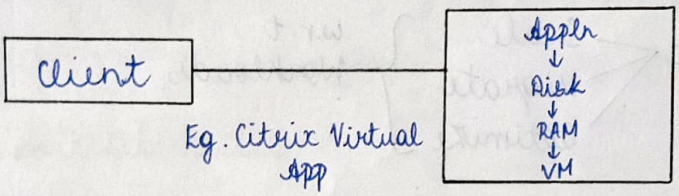
* Optimize
  Having an idea of where to move resources to

Eg. 1) Tomcat
2) Logic
3) JBase

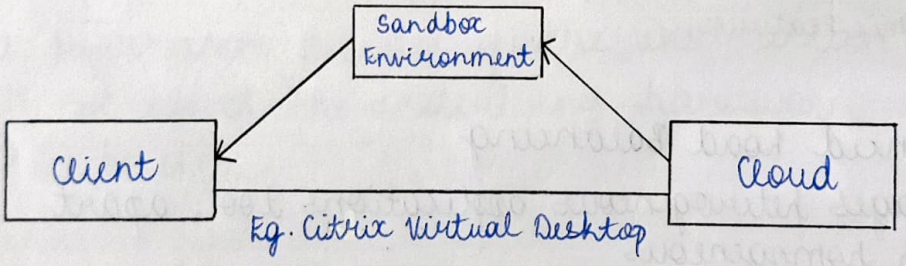
2) Application Virtualization (Thin Client Technology)

- It is a type of virtualization in which applications are independent of the operating system of a local device and the User Interface displays only the results of the application * Installation will not occur
- It is called Thin Client Technology because the client request will be processed in a remote location and result alone will be taken towards the client * Installation, Execution, etc.

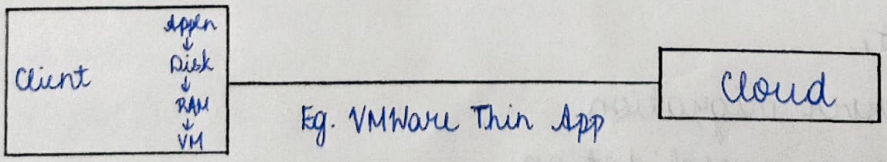
2.1) Terminal Services / Remote Desktop Virtualization



2.2) Desktop Virtualization (Sand Boxing)



2.3) Application Streaming



3) Storage Virtualization

- Need
  1) Remote access
  ii) Extending the lifetime of old devices

- File Storage (NAS) vs Block Storage (SAN)

  NAS - Network Attached Storage

  SAN -

NAS	SAN
i) It stores, retrieves and process the data in terms of files and folders by setting up an hierarchy	i) Data is stored by dividing it into fixed size chunks in different locations. Every chunk will have a unique identifier i.e. address
ii) Less expensive	ii) Highly expensive
iii) Low Performance	iii) High Performance
iv) File-based storage is used in NAS	iv) Block-based storage is used in SAN
v) NAS - A storage unit supports functioning of a network based on file storage systems	v) SAN - A high-computing network with block-based storage

- Pool of Resources

  Resources not in same configuration

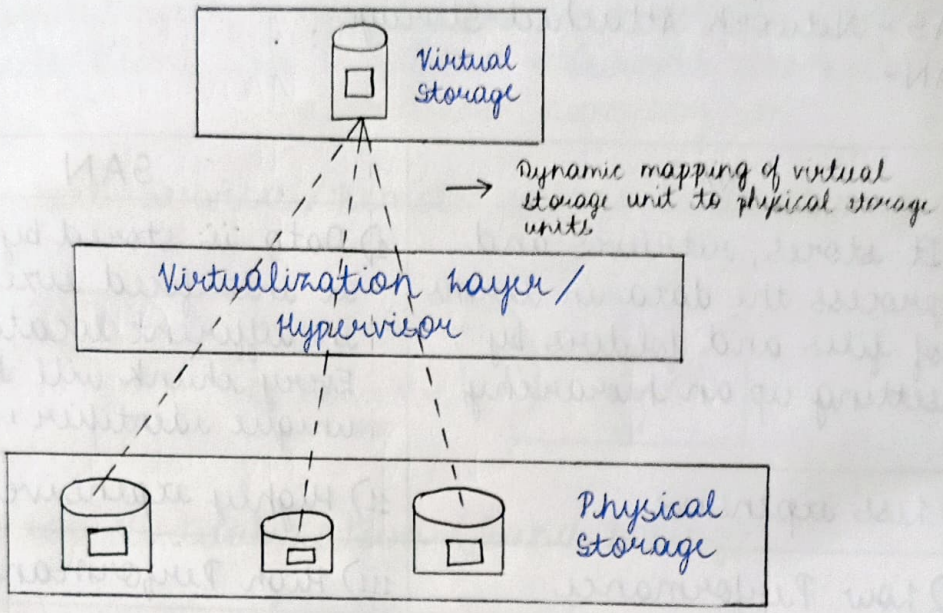
  * Nearline - data is frequently used
    Coldline - data is rarely used

Definition

It is a process of pooling up of multiple physical storage units and presenting it as one virtual storage unit to the users

Working

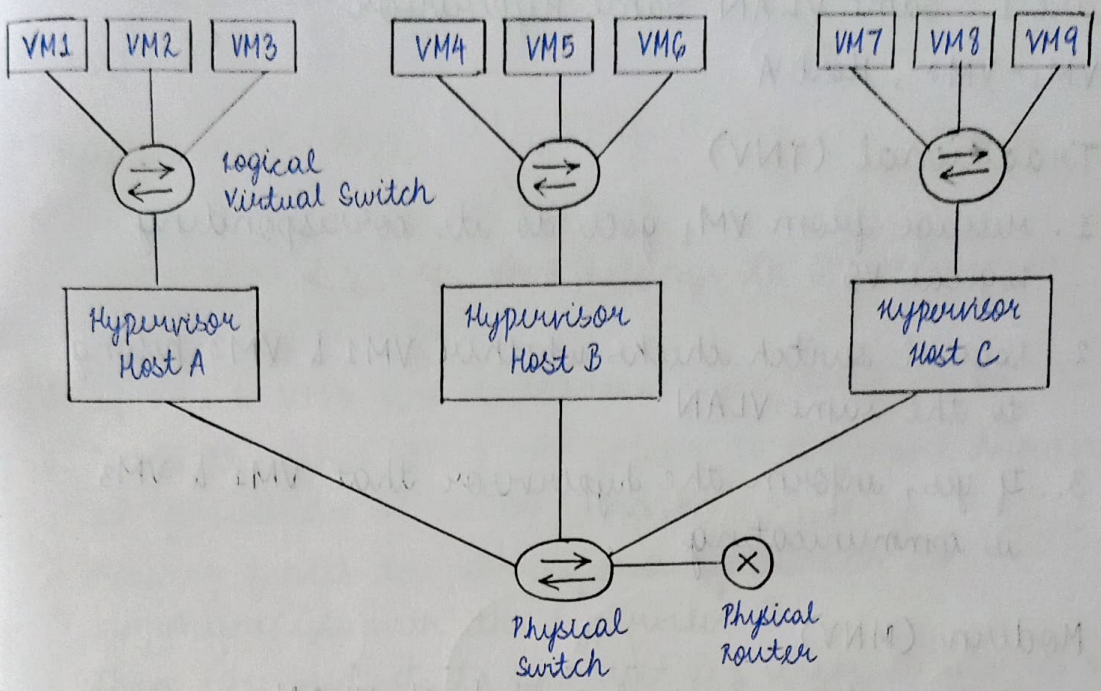
- User stores data in virtual storage
- Hypervisor divides it into multiple chunks
- It stores it in different physical storage devices
- If user wants to access this back, then can do it using linked list



Merits

- Efficient management of storage units (Easy to store, easy to recover, backup, archive)
- Extending the lifetime of old devices using the advanced concepts of:
  i) Tiering
  ii) Caching
  iii) Replication

4) Traditional Network Virtualization



$VLAN_{100}$ → VM 1, 3, 5, 7, 9

$VLAN_{200}$ → VM 2, 4, 6, 8

1 or 3 physical switch
No. of switches = No. of hypervisors
3 networks = A, B, C
LAN is same

22 · 7 · 25

* A hypervisor cannot communicate with another hypervisor
* Every hypervisor requires logical virtual switch for itself to connect to VM in its network

• Difference between Physical and Virtual Switch

Physical Switch	Virtual Switch
Networking device enables communication between two machines	Software enables communication between VMs

* VMs of one hypervisor is not allowed to communicate with VMs of other hypervisor using logical virtual switch because of security concerns. It has to pass only through physical router.

- Cases

Case I : Same VLAN Same Hypervisor

VM_1 - VM_3 , Host A

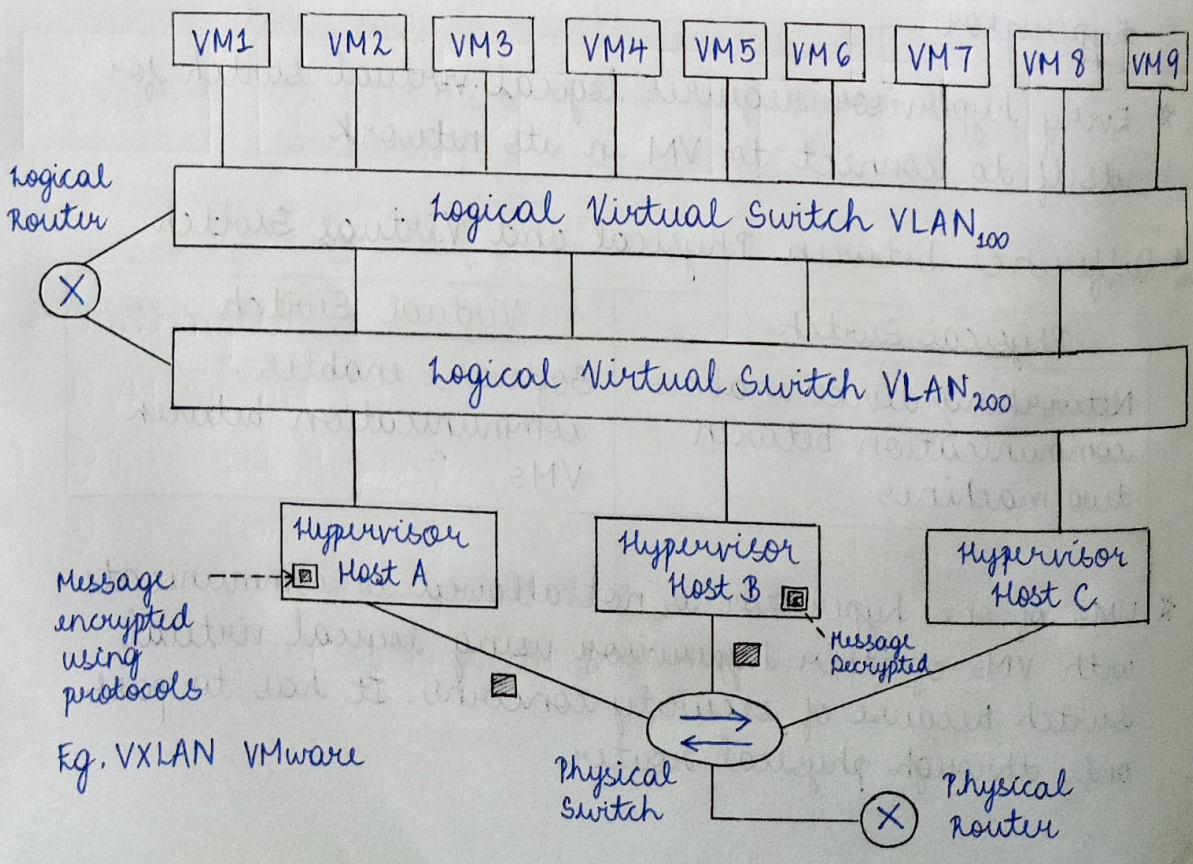
Traditional (TNV)

1. Message from VM_1 goes to its corresponding logical VS
2. Logical switch checks whether VM1 & VM3 belong to the same VLAN
3. If yes, inform the hypervisor that VM_1 & VM_3 is communicating

Modern (MNV)

1. Message from logical switch of $VLAN_{100}$
2. It checks for VM3's VLAN
3. And inform to the hypervisor

Here TNV & MNV working are the same



Case II : Same VLAN Different

VM1 - VM5
↓ ↓
Host A B

Traditional (TNV)

1. Message from VM1 → LVS of A
2. Check VM5's VLAN, VM5 belongs to B so inform this to Hypervisor A
3. If VM1 & VM5 are authenticated, send it to the PS
4. From PS, since VM1 & VM5 belong to different hypervisor, it forwards it to the router
5. Router finds the corresponding switch to communicate with the hypervisor B
6. Then forward it to the Host B & then to its LS of B and then VM5

$VM_1 \rightarrow \underset{A}{LVS} \rightarrow A \rightarrow PS \rightarrow PR \rightarrow PS \rightarrow B \rightarrow \underset{B}{LVS} \rightarrow VM_2$

Modern (MNV)

$VM_1 \rightarrow LS\ VLAN_{100} \rightarrow L\ Router \rightarrow$ Hypervisor A (Encrypt the message)

↓

$VM5 \leftarrow \underset{VLAN100}{LS} \leftarrow \underset{B}{Hypervisor} \leftarrow PS \leftarrow PR$

(Decrypt the message)

* Adv : Encrypt & Decrypt the message

Case III : Different VLAN Different Hypervisor

VM1 - VM6
A B

Traditional (TNV)

$VM_1 \rightarrow \underset{A}{LVS} \rightarrow A \rightarrow PS \rightarrow PR \rightarrow^{\text{Diff network}} PS \rightarrow B \rightarrow \underset{B}{LVS} \rightarrow VM5$

Modern (MNV)

Here, it is the same as TNV but LR easily says the shortest distance & traffic

Case III : Different VLAN Same Hypervisor

VM1 - VM2

Traditional (TNV)

It goes till the bottom layer (PR)

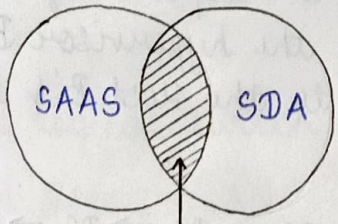
Modern (MNV)

It goes to the logical router, same hypervisor communicate

24.7.25

5) Service Virtualization

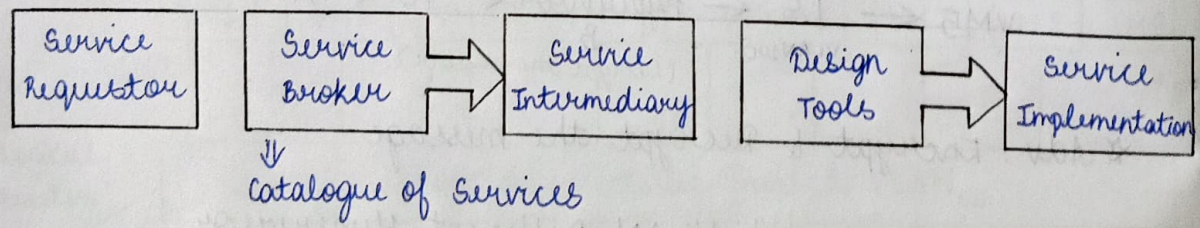
S/W Testing Team
⊕
Development Team



Reusable Components,
Interface Support

- Components (API, Database, 3rd Party Tools)
- Emulate the behaviour of the components

1) Multitenancy
2) Provisioning
3) Service Monitoring
4) SLA
5) Subscription



- Challenges

1) VM Sprawl
2) Resource Hogging
3) Data Commingling
(Data that is supposed to be isolated, will get mingled together)
4) Integration of Physical & Virtual Machines

- Benefits

1) Save Time, Energy, Resources → Economical Returns
2) Server Consolidation
3) Scalability
4) Disaster Recovery
5) Good Degree of Customization