

Virtualization

♦ Virtualization

Definition:

Virtualization is the process of creating a virtual version of a physical resource, such as a server, storage device, network, or operating system. It allows multiple virtual machines (VMs) to run on a single physical machine using a **hypervisor**, improving **efficiency**, **scalability**, and **isolation**.

♦ Hypervisor

A **hypervisor** is software that allows multiple virtual machines (VMs) to run on a single physical machine. It manages hardware resources (like CPU, memory, and storage) and allocates them to each VM. Examples include VMware, VirtualBox, and Hyper-V.

Types of Hypervisors:

- **Type 1 (Bare Metal):**
Runs directly on physical hardware without a host operating system. These are more secure, have lower latency, and are typically used in data centers. Examples: VMware ESXi, Microsoft Hyper-V.
 - **Type 2 (Hosted):**
Runs on top of a host operating system like any other application. Easier to set up but with more latency. Used mostly for testing or personal use. Examples: VMware Workstation, Oracle VirtualBox.
-

♦ Benefits of Virtualization

- **Cost Saving:**
Multiple virtual environments on one physical machine reduce the need for physical infrastructure, saving on electricity, maintenance, and hardware upgrades.
- **Speed and Agility:**
Creating VMs is faster than setting up physical systems, making testing, scaling, and deployment more efficient.

- **Lower Downtime:**
VMs can be moved between hypervisors on different servers, allowing fast recovery during shutdowns or failures.
-

♦ **Virtual Networking**

Définition:

Virtual networking creates connections between virtual machines using software rather than physical hardware. It allows VMs on different physical machines to communicate using virtual switches, routers, and tunnels.

♦ **Physical Network Components**

- **Underlay:**
The physical infrastructure that supports the virtual network, such as physical servers, switches, and routers.
 - **Fabric:**
All the physical components (servers, storage, and networking gear) that work together to run a virtualized environment efficiently.
 - **TEP (Tunnel Endpoint):**
A network point that enables VMs to communicate across physical networks. It handles the encapsulation and decapsulation of data between the virtual overlay and the physical underlay.
 - **Physical Routers and Bridges:**
These connect virtual machines to the physical network and allow VMs on different servers to communicate with each other and with external systems.
-

♦ **Overlay Network Components**

- **Overlay:**
The virtual side of the network that allows VMs to communicate over software-defined connections, even if they're on different physical machines.
- **Segments:**
Virtual Layer 2 networks (like local LANs). VMs in the same segment can communicate using MAC addresses. VMs in different segments need a router to

communicate.

- **Transport Zone:**

Defines which hypervisors and segments can communicate. It controls the scope of each segment by specifying which physical hosts are part of the virtual network.

- **Routers and Bridges:**

Used to connect segments together. They can also connect to physical routers, enabling communication between the virtual and physical networks.

- **Micro-Segmentation:**

A security method that creates smaller isolated zones within a segment. Each VM can have its own rules and policies, limiting internal threats even on the same segment.