The main contribution of a VMM is handling virtual resources: it presents to the guest OS the interface if a real resource, understands the OS requests and emulates them.

Virtualisation maps virtual resources to a set of managed ones, which are often physical and in rare cases are virtual, it can provide

1. The same interface (virtualisation): advantage is the quality of performances, but it is not always possible
2. A different interface (emulation): compatibility, interoperability and flexibility but also lower performances

Physical resources can be mapped into virtual ones in three ways

- One to one
- One to many: sharing, the main benefits are isolation, flexibility and resource management, it can be implemented using time or space multiplexing
- Many to one: aggregation, the main benefits are scalability, reliability and simplification

The CPU

CPU: the host must be able to execute the guest instruction, via emulation if there is a different ISA which prevents direct native execution

Usually, a core is shared among any virtual machines by partitioning it; it should be avoided to assign each machine a number of virtual cores that is greater than the total number of cores of the physical device, as the only way in which it can be implemented time sharing a code and it leads to bad performances. However, when more than one virtual machine is running, the total amount of their core can be greater than the physical one, as usually the machines are in a waiting state and therefore the cores are sufficient to execute something on one machine at a time.

It is also possible to set an execution cap, that is the maximum amount of time a core can be used by a machine, it allows to select less important machines and ensure they don't interfere with the execution on the most important ones.

The memory

The sum of the memory allocated for each machine should be less than the total physical memory, but it can lead to a poor utilisation of the real memory. So, it is preferred to assign memories that, if summed, result greater than the physical one. Allocating new memory can be done in two ways:

- Memory ballooning: the VMM asks the host for the list of the free pages when it needs more memory, it is possible only when the VMM is aware to be virtual (para virtualisation)
- Overcommit: the VMM rewrites the pages it supposes to be less used, it happens when it is not aware to be virtual and so it believes to have the entire memory available

Conventional operative systems virtualise memory, as they load only a few pages into the RAM and, if another page is needed, one if those in the RAM is put back into the disk and then another one is loaded. With virtualisation, another saga structure is needed, it is called **memory management unit** (MMU) and it allows to separate the process address space from the physical one. For each virtual page, it contains the physical address and three flags that tell whether or not the page is loaded into memory, whether or not it has been changed and whether or not it is free.

Each virtual machine has its own virtual memory, so it is necessary to maintain synchronisation and consistency among them. It can be done in two ways.

1. Shadow pages, which are maintained by the VMM and consist of the mapping of the virtual pages of the guest into the physical ones of the host, they are used by the hardware to translate the addresses and they are synchronised with the host's page table by the VMM. The counter effect is a lot of overhead when they are updated
2. Nested pages, which remove the overhead in translating but require a hardware that is able to support it. The translation lookaside buffer is able to cache the translation to make it faster.

I/O devices

The VMM builds a virtual version of the devices, it intercepts and handles the requests.
Devices can be dedicated (keyboard, mouse, …), partitioned (large disks) or shared (network adapter)

Virtual disks

They can convert the entire HDD into a file, there are three types

- Fixed size format creates a file that has the dimension of the entire HDD
- Variable size format starts with a reduced size and can grow up to the whole size of the disk, it stores only the used blocks

Both of them allow the user to create snapshots, which consist of saving the content of the disk to allow to return to it if needed. The first one is really saved, for the followings only the differences with the previous one are stored.

Network virtualisation

There are three ways in which the virtual machines can connect to the Internet

1. Network address translation (NAT): VM and the host have the same IP addresses, ports are different if forwarded

It is the simplest way of connecting, each machine is in a virtual private network that connects it only to the host, it can reach the external network through the VMM, which performs routing functions, it can be visible if ports are forwarded. The guest sees a virtual network with a DHCP server (simulated by the VMM) that assigns it always the same address, which depends on the virtual network card, while the host treats the VMM as any other application.
To correctly forward the packets, the VMM sends the request to the host and keeps track of the machine that originates it, so when the response arrives it knows which machine needs it.
If a server runs on a virtual machine, it must be forwarded, which is implemented by assigning one of the free ports pf the host to the machine: it will run on the host IP on the assigned port number.

2. Bridged networking: VM and the host have different IP address, the ports are managed independently

It allows the guest to directly send and receive packets, as if they were on a physical network by exploiting the possibility to assign multiple IP addresses t a single virtual network card. The host needs the Net Filter, a particular device that filters data from the network adapter, so that the VMM can forward them to the correct virtual machine. The guests behave exactly as if they were physically connected with the interface, with the exception that their traffic is sent to the host in addition to the outside Internet. To configure it, a real network adapter must be selected, as the host sees the traffic from the machines as if it was coming from the outside on that network adapter.
When the host is not connected to the Internet, VM need a DHCP server on the network or a statically assigned IP to be able to connect.

3. Host only networking: VM and the host have different IP address, the ports are managed independently

Connection is allowed only between the Virtual machines and the host, it is more secure, but it needs the host to perform routing mechanisms to allow the guests to connect to the Internet. The host has one (or more) special virtual network adapter, which is built exclusively for host-only networks, which allows the communication between virtual machines and the host. If needed, a DHCP server can be added.

4. Internal networking: VM and the host have different IP address, the ports are managed independently

Virtual machines are connected only among themselves, they cannot access the Internet and can communicate with the host only with the keyboard, the mouse and the graphic interface provided by the VMM. They have different IP addresses; this solution is the most limited but also the most secure and can be useful to test complex network configurations. Each machine is identified by a different name and IP.