Install KVM, create VM

- From [http://www.youtube.com/watch?v=nVvHCB-ixF4](http://www.youtube.com/watch?v=nVvHCB-ixF4)

- Install Linux, then KVM
- In Linux, login as root
- Check whether the hardware (CPU) is “vmx”
  - Whether it supports hardware-assisted virtualization
- Install KVM and other associated packages
  - Such as libvirt and virt-manager
- Set up default directories
  - Change Linux var that defines the default directories, chcon: change security context
  - Ln -s: symbolic link some default KVM directories to the directory you want, such as image directory that stores VM images

- Create a virtual disk???
  - Virtual disk can be shared among VMs
  - We need a virtual shared disk among hosts to facilitate migration
  - Use Linux Logical Volume Management (LVM) to create a volume for sharing
  - Then go to VMM to link the LVM to it
    - [https://www.virtualmin.com/documentation/cloudmin/virtualization/lvm](https://www.virtualmin.com/documentation/cloudmin/virtualization/lvm)

- Create a bridged network
  - Change network configuration file to include a bridge, for example, br0
  - Configure the bridge
  - This allows other VMs or external network to communicate with the VMs
  - Can use libvirt to create and configure bridged network in VMM

- Start KVM (service libvirt start)
- Download OS images (ISO) for VMs
- Create the virtual machine
  - Provide OS image, disk path and size, and bridge network
  - In the popup options during creation, provide console as the terminal
  - After installation of the VM and its OS, put regular setup parameters for OS
- Login to the virtual machine
  - Configure the virtual machine (host name, network setting)
  - DNS: can use that is available already on the network (or Google DNS 8.8.8.8)

Network settings
  - [https://www.virtualbox.org/manual/ch06.html](https://www.virtualbox.org/manual/ch06.html)

- A network adapter can be configured to operate in one of the following modes
- Not attached
  - In this mode, VMM reports to the guest that a network card is present, but that there is no connection -- as if no Ethernet cable was plugged into the card
  - This can be useful to inform a guest operating system that no network connection is available and enforce a reconfiguration
- Network Address Translation (NAT)
  - Also called port address translation (PAT), IP masquerading, NAT overload, etc.
  - A router generally performs NAT to connect internal network to external network
- Private network uses internal network addresses and router routes internal packets
- When the private network tries to access external network, the router changes internal IP to the IP of the router in the IP address of the packet
  - Only the sender IP address and port number, receiver IP and port should not be changed
- When the router receives a packet from the external network, it translates the IP address (the router’s IP) to internal IP
- But how does the router know which internal IP it should be? It is according to the port number in the receiver address
- External network has no way to directly access an internal address, the packet has to go through the router, and the router can reject all packets that are no responses to an existing request
- NAT helps protect the internal network, and helps reserve IP addresses
- In VMM, NAT can be used, it is like having a virtual router in between VM and host, and each VM is in its own private network
  - Better security, but the VM cannot be accessed from external network

- Port forwarding in NAT
  - Port forwarding allows external computers to connect to an internal computer that is protected within a private network
  - On the router, map a port number to a specific service (with its own internal IP and port number) on a specific computer
  - In VMM, VMM can make some services of the VMs available through port forwarding

- Host only networking
  - Similar to NAT, but creates a connection between VM and host (available in VMware only)

- Bridged networking
  - Instead of using native network interface on the NIC, bridged network introduces a software network interface on top of NIC
  - Can be used to create a different kind of software-based network, instead of the specific protocol used by the NIC
  - In VMM, NAT and port forwarding are performed by VMM, not the physical router
  - With bridged networking
    - The virtual network adapter in the virtual machine connects to a physical network adapter of the host
    - The host network adapter enables the virtual machine to connect to the LAN that the host system uses
    - So, VM connects to the bridge directly (running on top of NIC), by passing the VMM translation
  - Bridged networking allows inter-VM communication (can be among the selected VMs) and communication with the host, not with the external network

- Generic networking
  - Directly share the NIC, as though the VM is another host (rarely used)
  - There are two sub-modes currently supported

- Generic networking with UDP Tunnel
  - Can connect VMs running on different hosts directly over existing network infrastructure

- Generic networking with VDE (Virtual Distributed Ethernet)