Introduction to Virtualization

Dr. Qingni Shen

Peking University

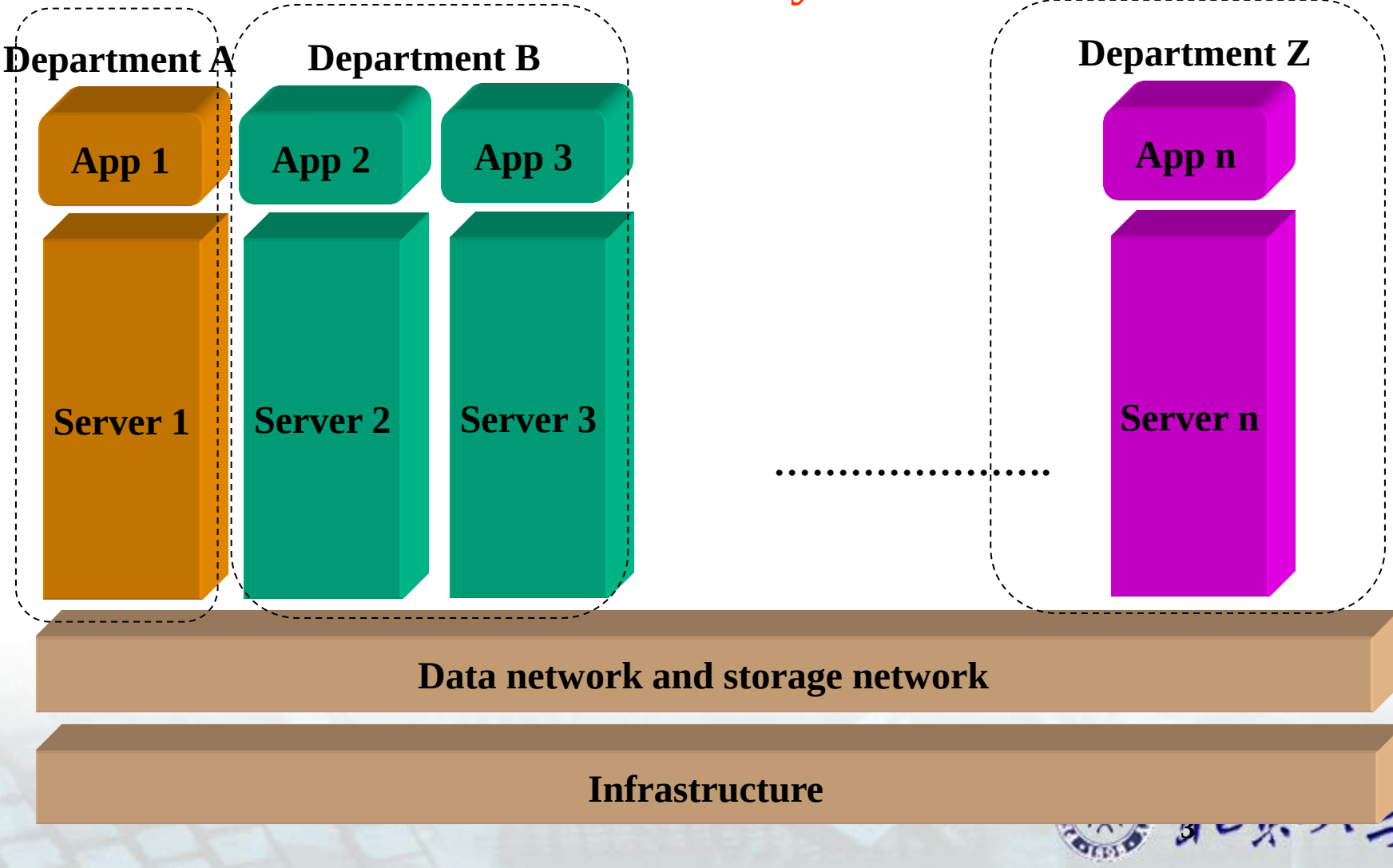
Intel UPO Supported

北京大学

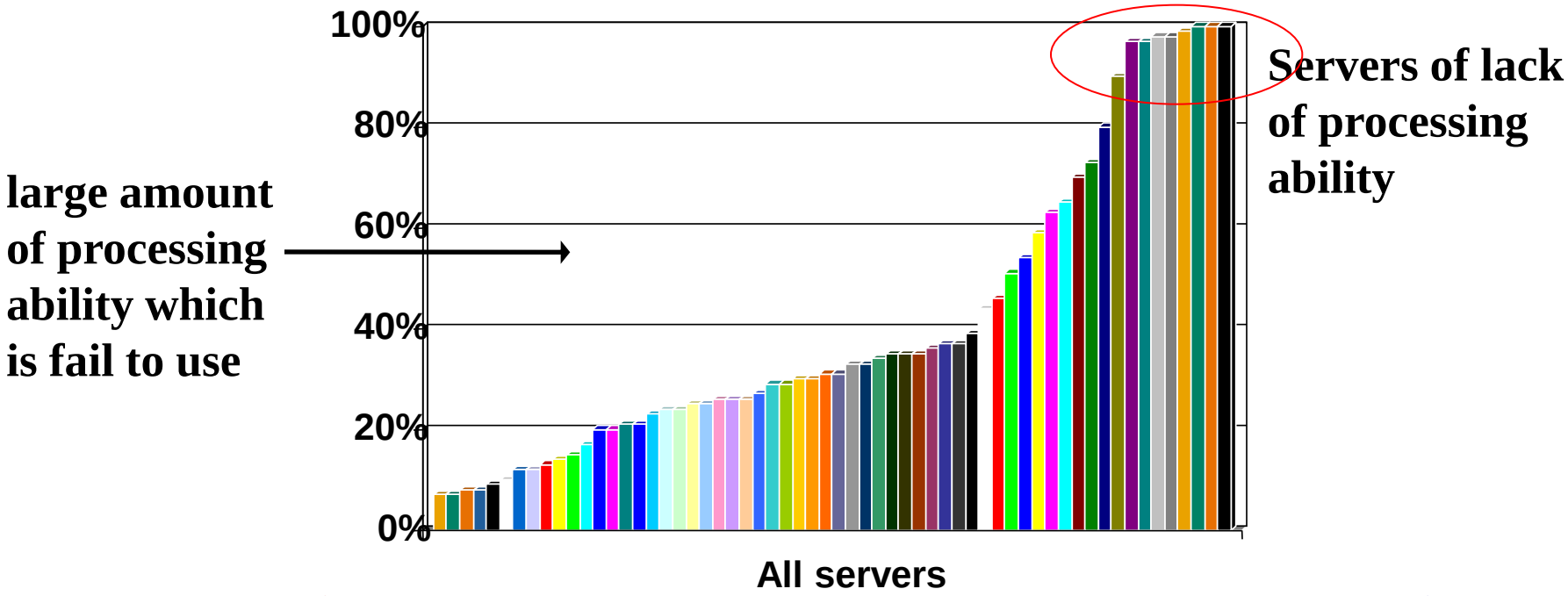
Main Points

- Status and trends in data center
- Definition of virtualization
- Common types of virtualization
- Key technologies of sever virtualization
- Mainstream virtualization softwares and the practice of virtualization technology

IT resource allocation mode of traditional data center --the Chimney structure



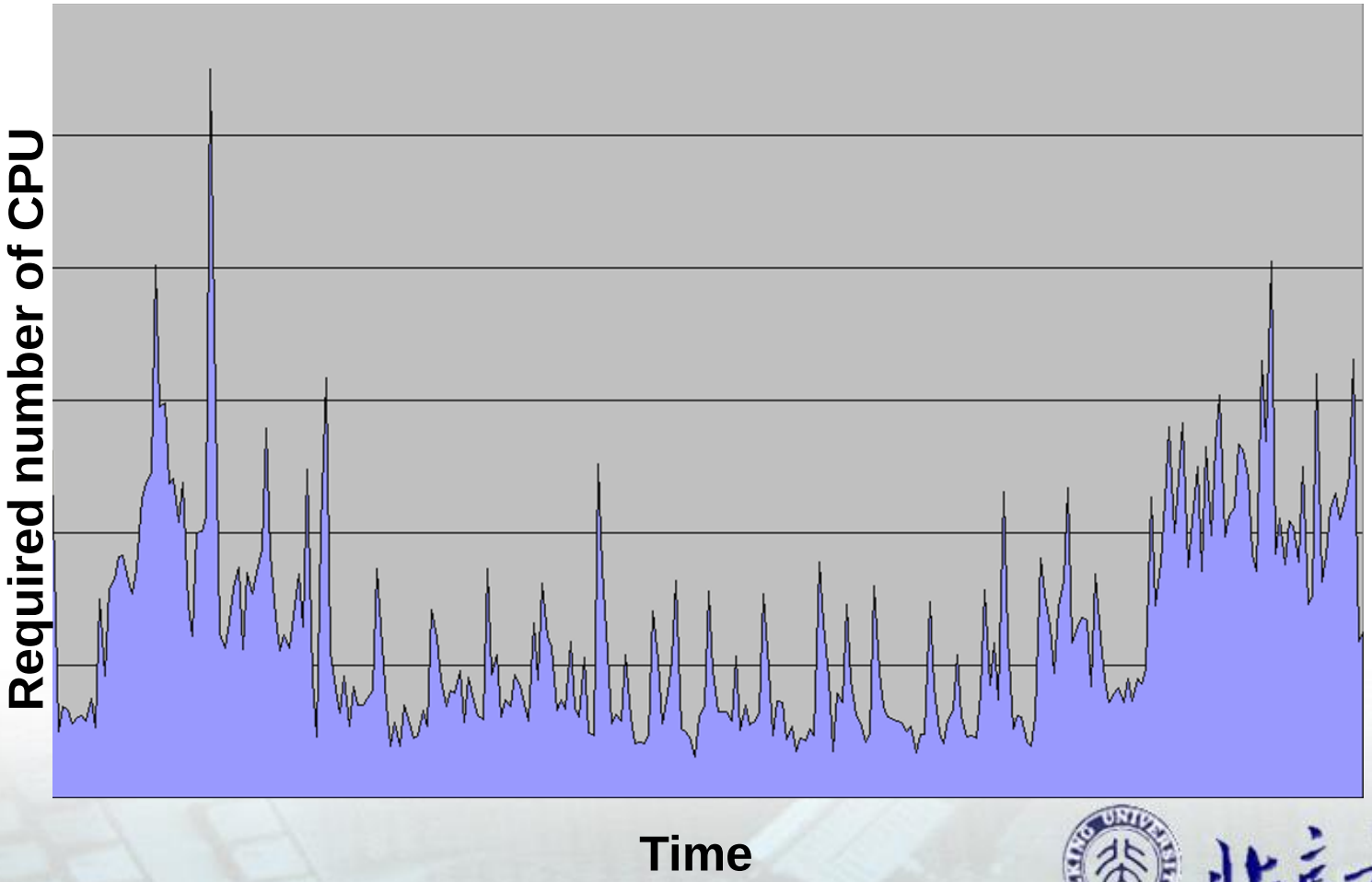
Defects of traditional chimney data center



- Defect 1: According to the statistics, the average server utilization in data center is below 30%, but there is still a considerable number of servers can not meet their service level objects.
- Defect 2: The deployment of a new application needs budget, procurement, installation and tests, product launching and other processes, and the cycle will be over a period of weeks to months, so it is difficult to response to the business needs timely.
- Defect 3: The number of servers and management costs have a linear relationship with the number of applications, so there is enormous pressure of IT management and cost.

Causes of low resource utilization

- **Over configure the servers to cope with a small amount of peak load**



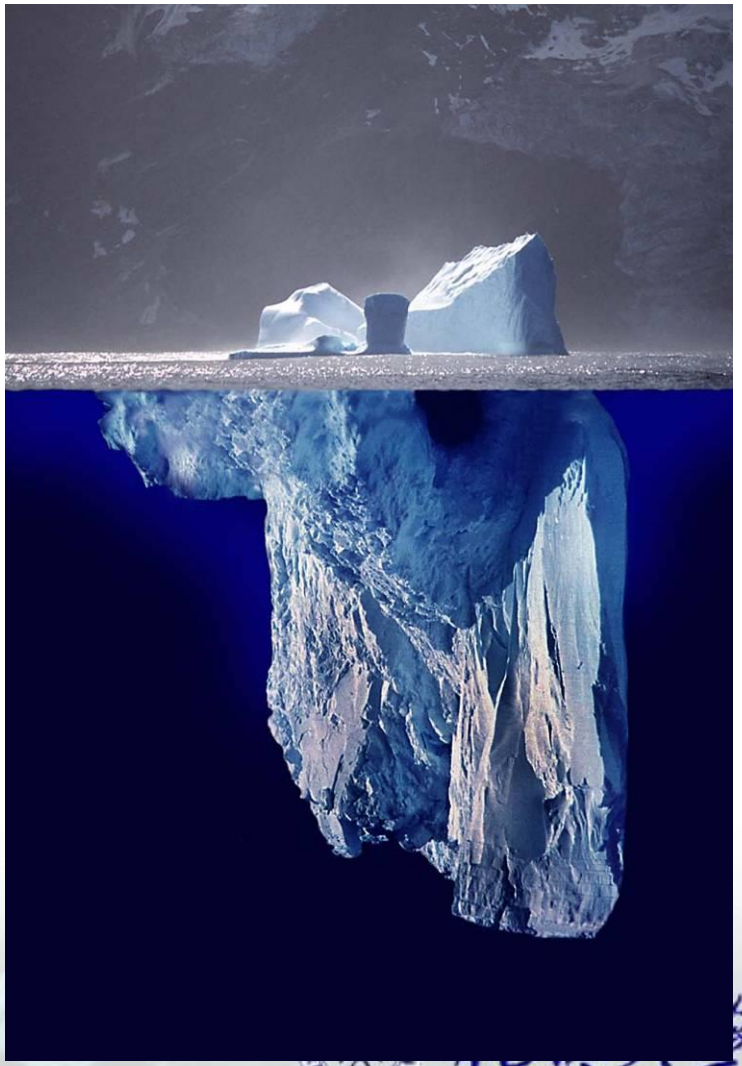
“Iceberg Model”

-- Cost structure of traditional data center

Visible cost :
30% of the budget will be used in new infrastructure and new application development

Invisible cost :

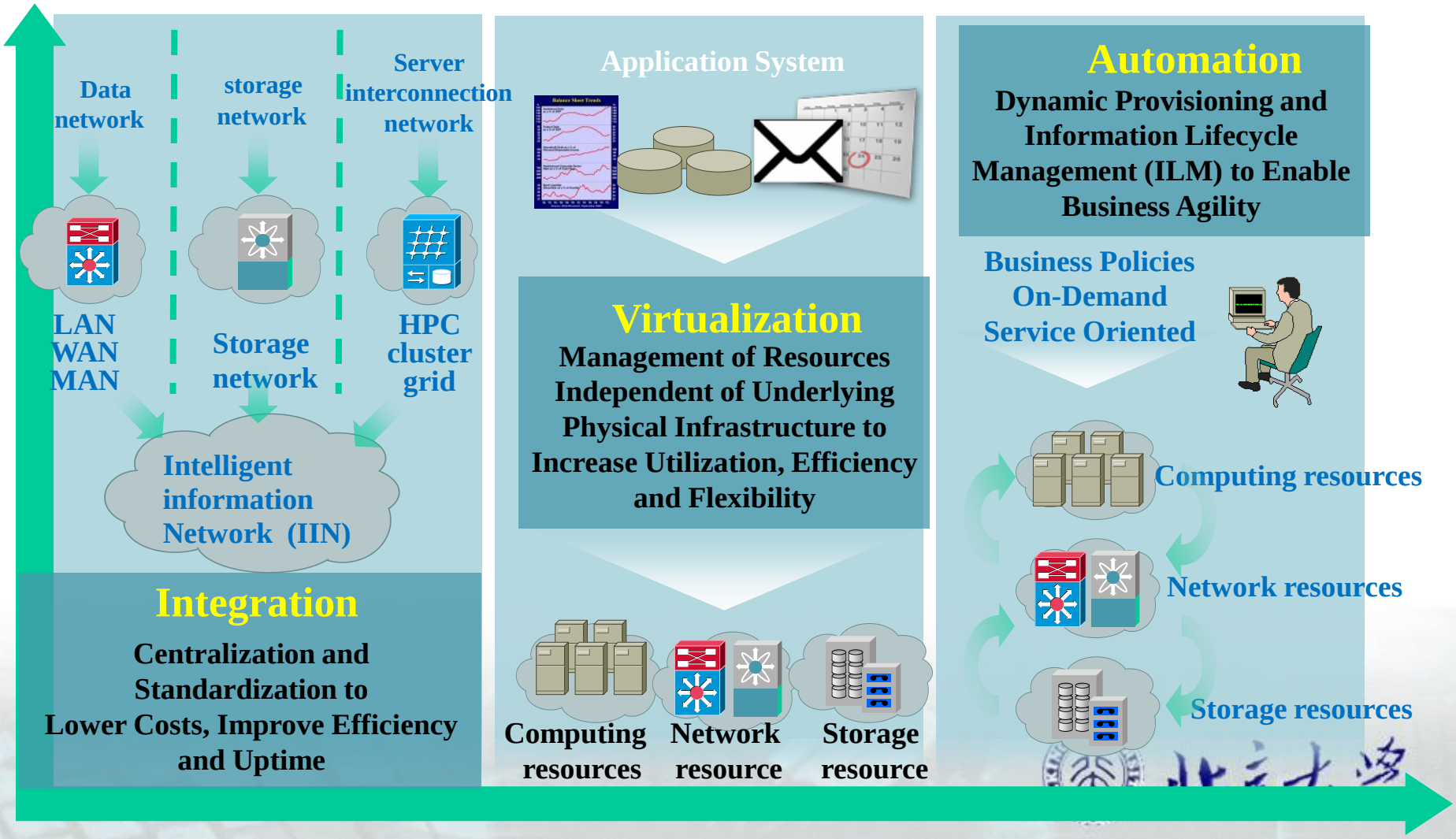
70% of the budget will be used in the maintenance of existing facilities and personnel expenses



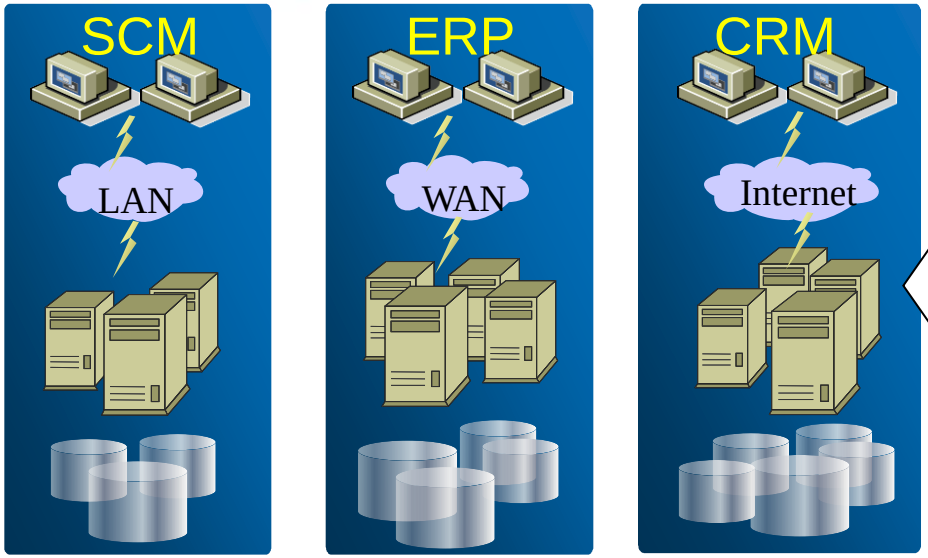
Question :
How to save the operation expenditure budget for more IT infrastructure innovation?

IT infrastructure development in data center

Three stages

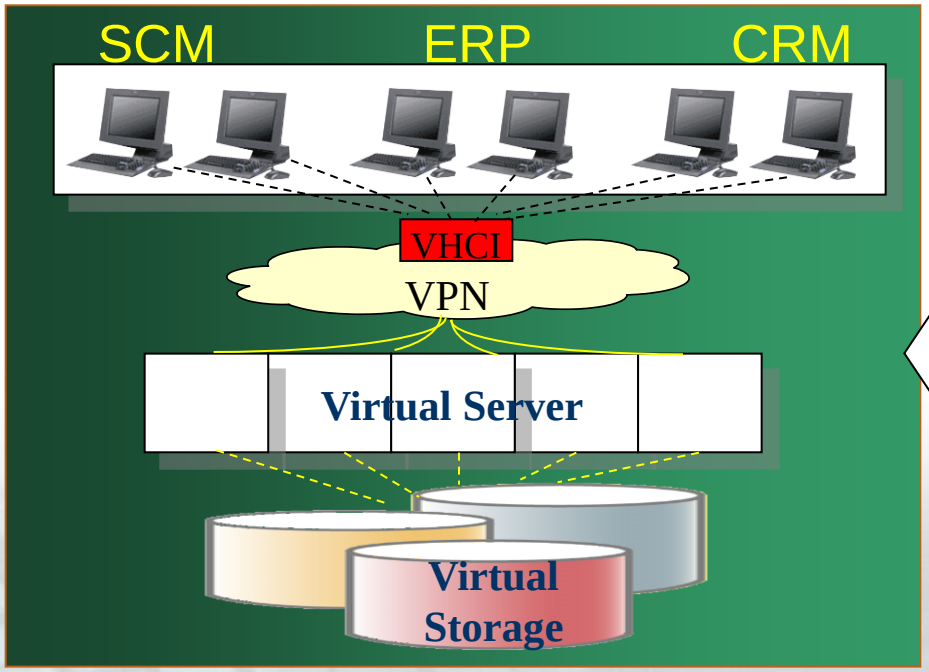


On-demand data center



Non-virtual Environment

- Isolated techno-island
- Complex management system
- Resource are not shared
- Huge architecture
- Difficult to configure a new workload
- Rigid and not inflexible



Virtual Environment

- General technical platform
- Easy management system
- Shared resource library
- Simple architecture
- Easy to configure the new workload
- On-demand and flexible

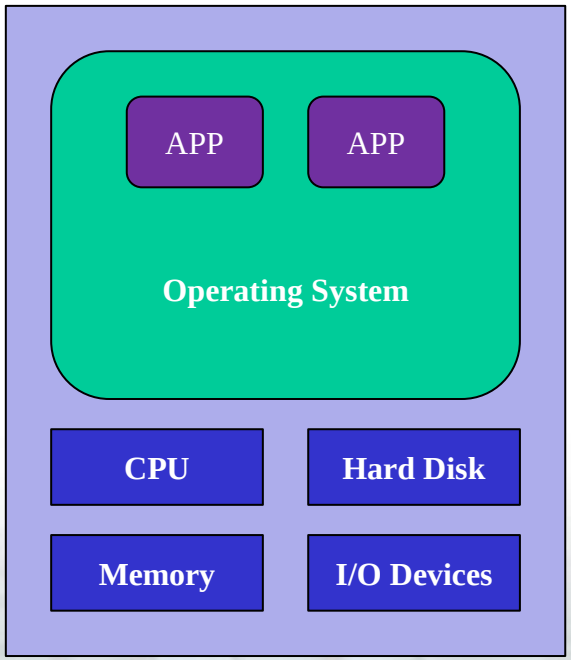
Main Points

- Status and trends in data center
- Definition of virtualization
- Common types of virtualization
- Key technologies of sever virtualization
- Mainstream virtualization softwares and the practice of virtualization technology

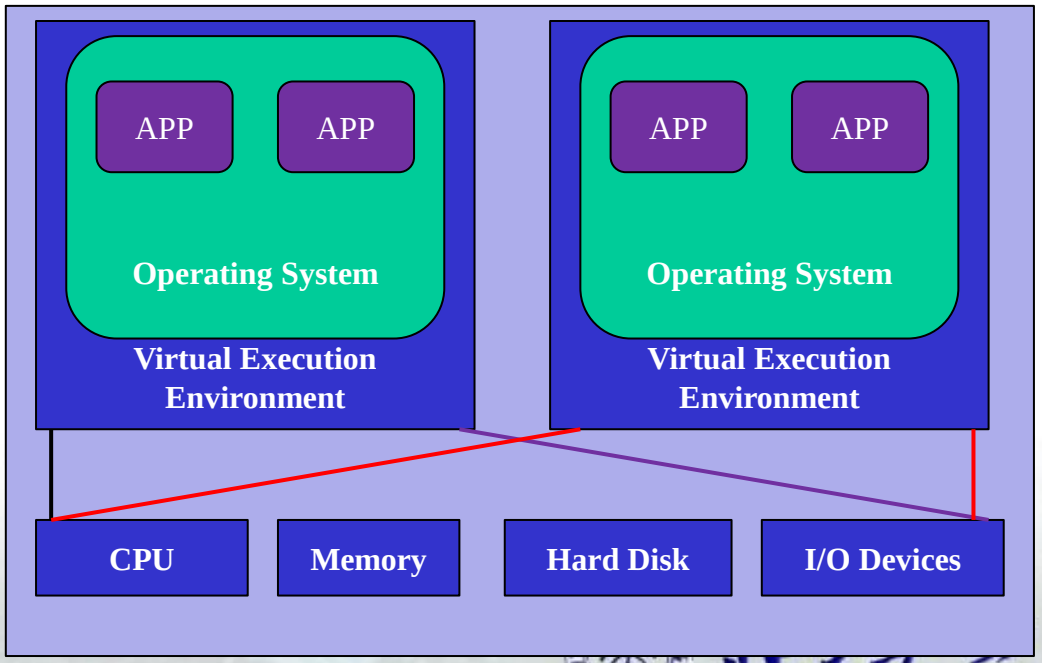
Definition of Virtualization

- **Nature of virtualization:** Previous computing system or components that run in real environment are now running in virtual environment.

Real computing model



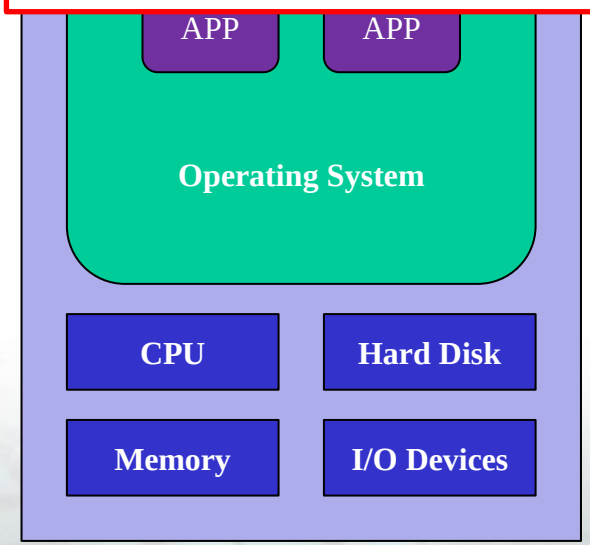
Virtual Computing model

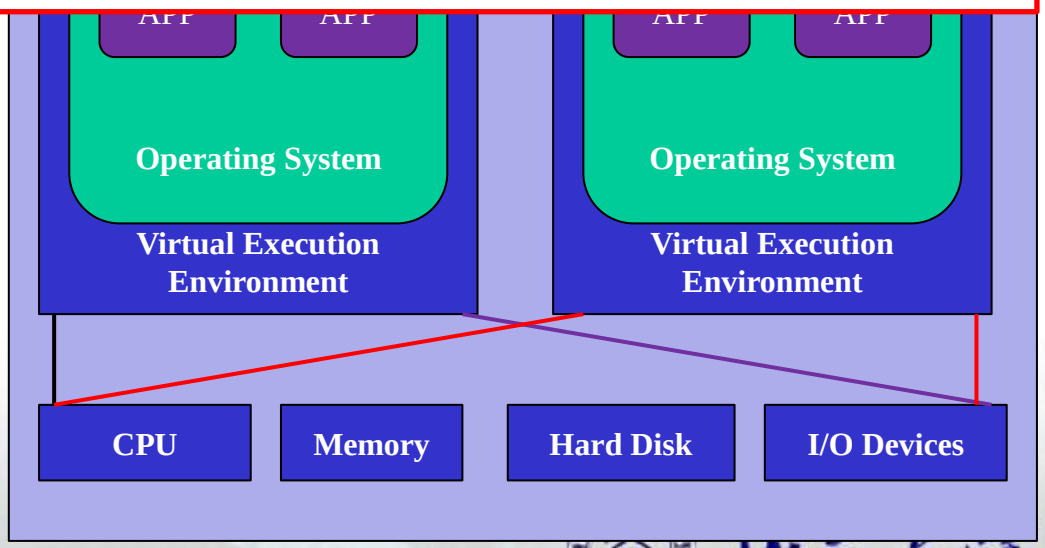


Definition of Virtualization

Definition

Virtualization is an abstraction of computer resources. We can access resources in a consistent way before and after abstraction through virtualization. This kind of resource abstraction is not limited by implementation, geographical location or the underlying physical configuration.



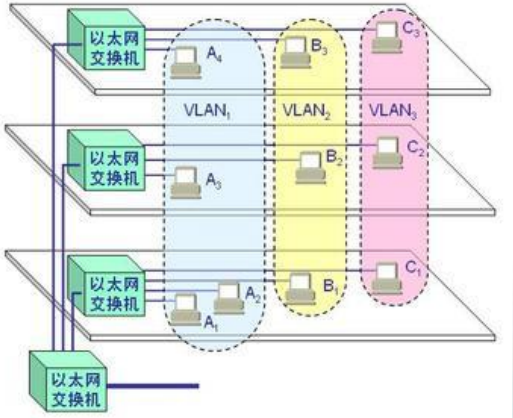


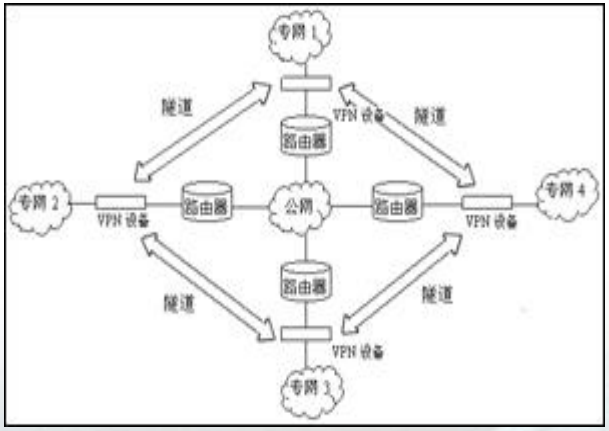
Main Points

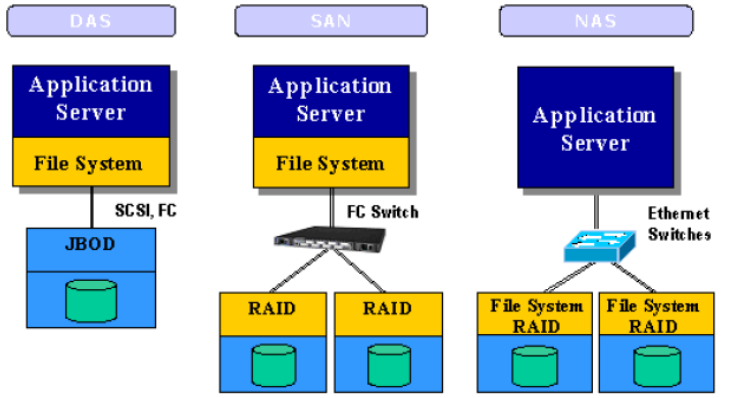
- Status and trends in data center
- Definition of virtualization
- Common types of virtualization
- Key technologies of sever virtualization
- Mainstream virtualization softwares and the practice of virtualization technology

Common types of Virtualization

- Types: Infrastructure Virtualization、System Virtualization、Software Virtualization.
- Infrastructure Virtualization
  - **Network Virtualization:** Integrate network hardware resources with software resources to provide users with virtualization technology of virtual network connection. It can be divided into VLAN and VPN.
  - **Storage Virtualization:** Provide an abstract logical view of physical storage device, so the user can access the integrated storage resources through unified logical interface of this view. It can be divided into storage device based storage virtualization(eg RAID) and network based storage virtualization(eg NAS, SAN).



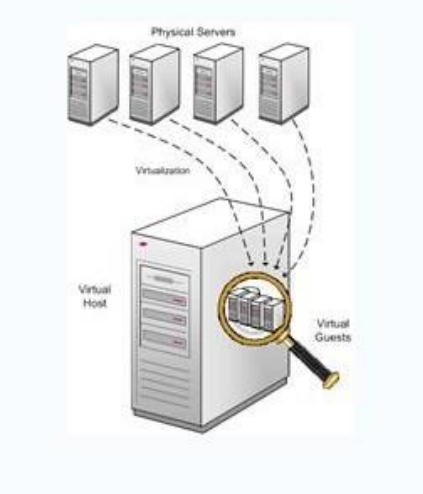


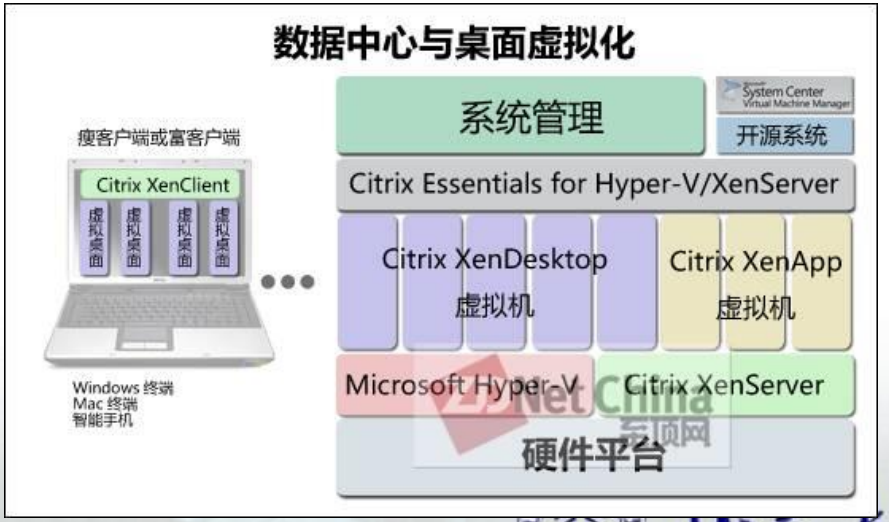


北京大学

System Virtualization

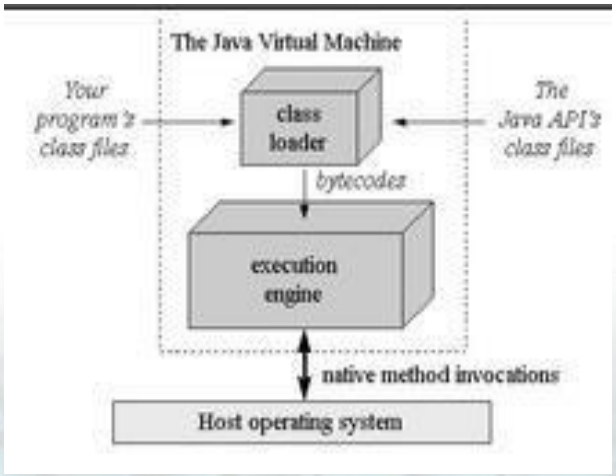
- **Core idea: Create one or more virtual machines using virtualization software on physical machine.**
- **PC/Server Virtualization: The maximum value of system virtualization.**
- **Desktop Virtualization: Solve the coupling relationship between PC desktop environment(including applications and files, etc.) and physical machines. Virtualized desktop environment is stored on a remote server, and when user has compatible device with sufficient display ability(eg PC, Smart Phones, etc.), all the programs and data will eventually stored in the remote server.**

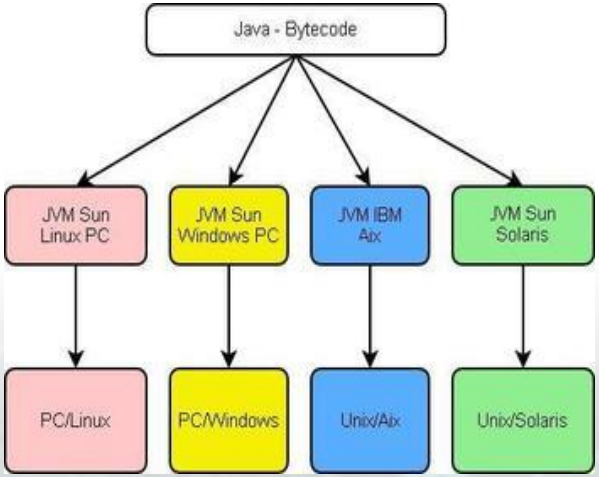




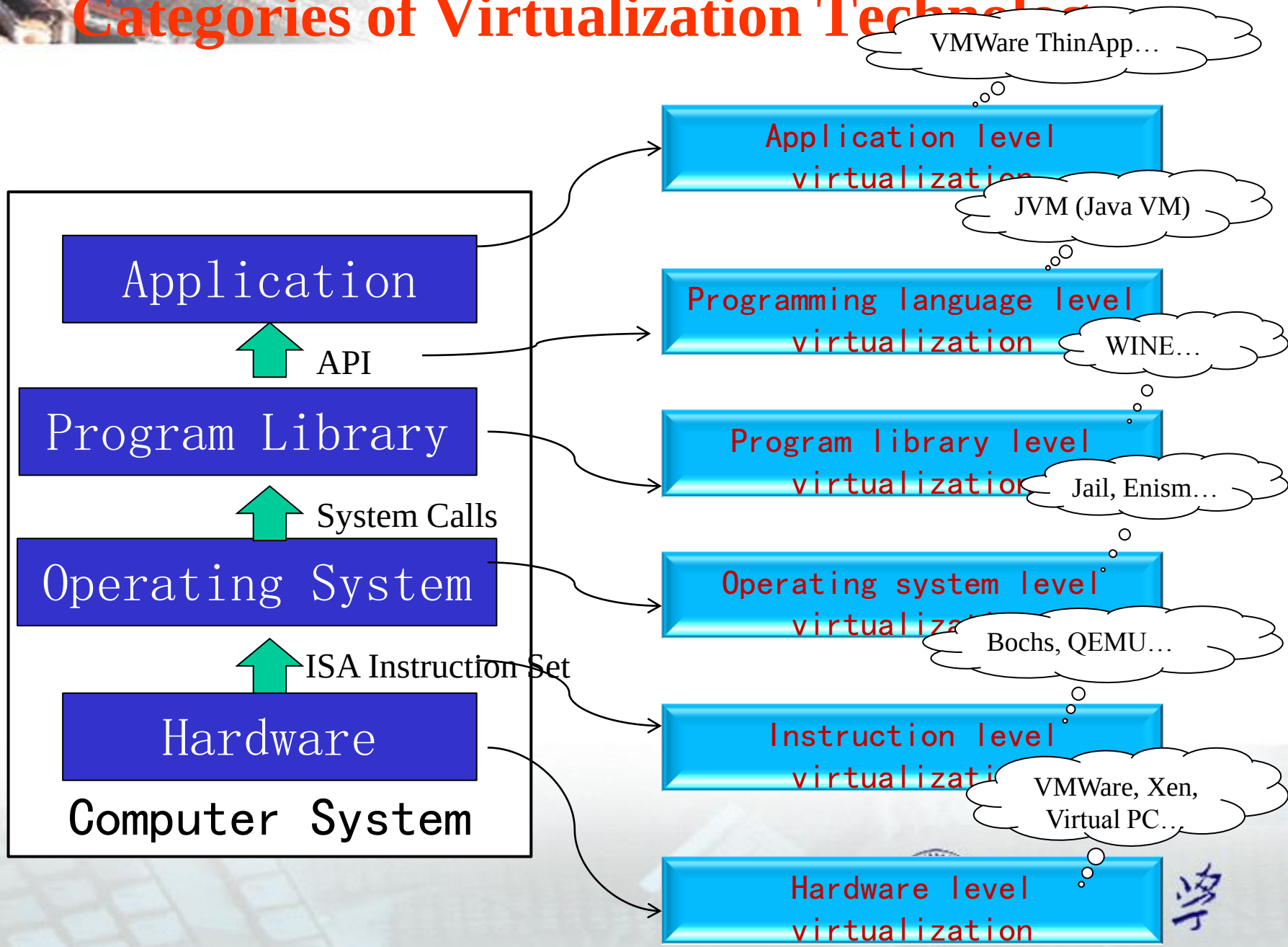
Software Virtualization

- **The High-level language virtualization:** Solve the migration problem of executable programs between different architectures. Programs which are written in high-level language will be compiled into standard intermediate instructions, and these instructions will be executed during interpretation or compiled environment(such as Java virtual machine JVM)
- **Application Virtualization:** Decouple applications from operation systems, and provide a virtual running environment for applications, including application executable files and required runtime environment. Application virtualization server can push user required program components to the client virtual running environment timely(such as VMWare ThinApp).





Categories of Virtualization Technology



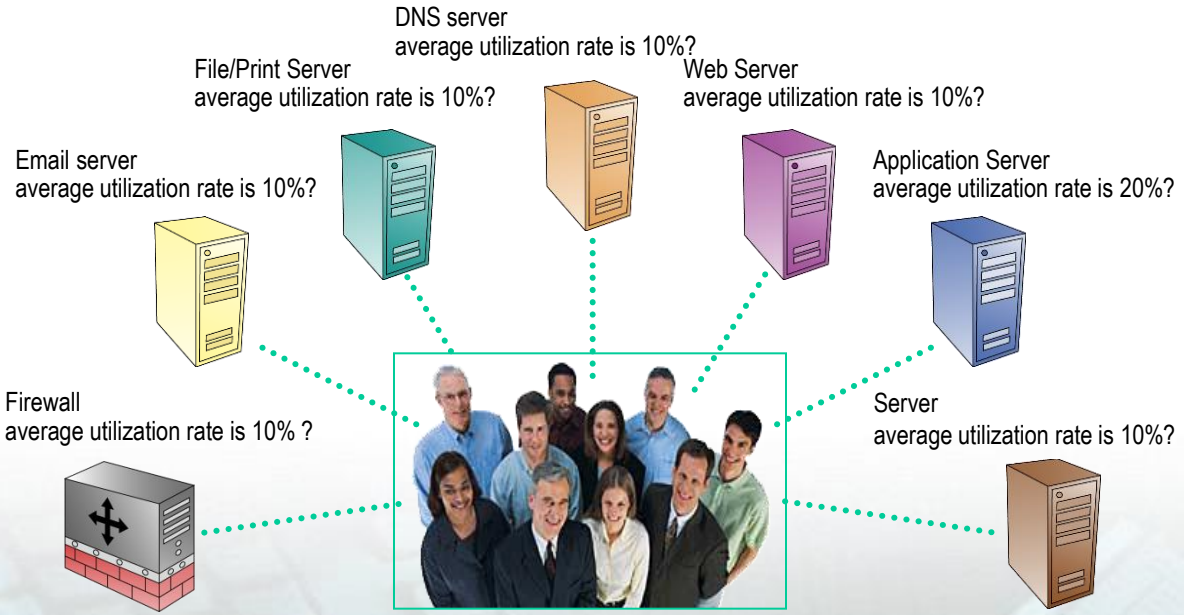
Main Points

- Status and trends in data center
- Definition of virtualization
- Common types of virtualization
- Key technologies of sever virtualization
- Mainstream virtualization softwares and the practice of virtualization technology

Server virtualization technology

Convenient to manage; Improve the utilization rate; reduce cost; focus on skills

- Purchase the needed only
- Simplify the environment
- Concentrate on core skills
- Improve the response speed of business change

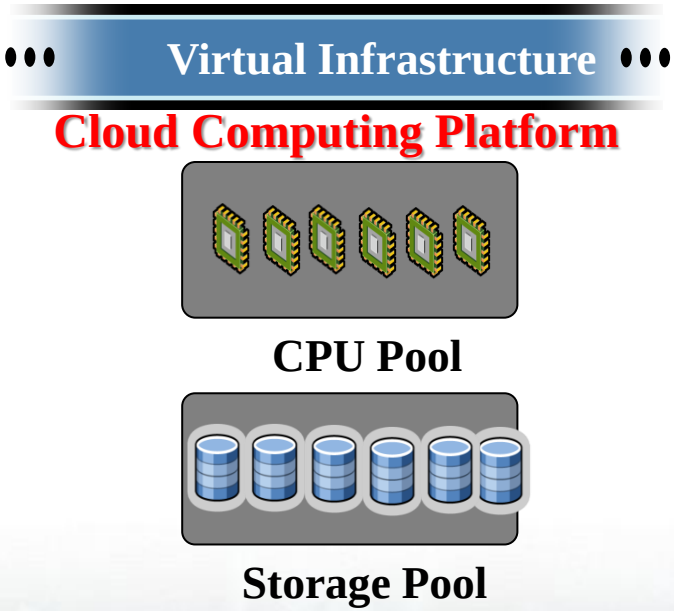


北京大学

Virtualization technology is the core of cloud computing

Lower IT cost

- Higher utilization rate
- Less complexity
- More automatic management



Higher quality of service

- Support dynamic migration
- Better fault tolerance
- With isolation, better safety
- Container based management, have encapsulation
- Flexible, easy to expand

北京大学

Development of virtualization technology

- **The virtual machine technology firstly appeared in the last 60's**

  in order to improve the utilization rate of precious computing resources

  impel the wide study and use of virtual machine technology

◆**In the 80's and 90's**

with the popularization of multitask and multiuser operating system

and the decline in the cost of hardware

virtual machine technology could not develop its advantage

people cooled down their study enthusiasm for it

- **Now,**

  Based on the high performance of the computer hardware

  how to reduce system cost and improve system resource utilization rate

  how to reduce management cost

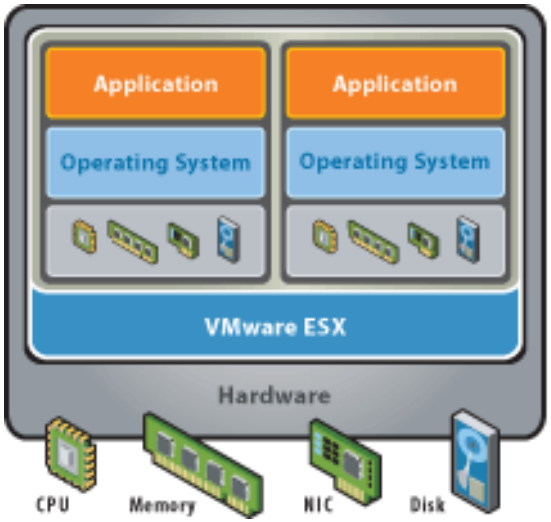
  how to enhance the safety and reliability

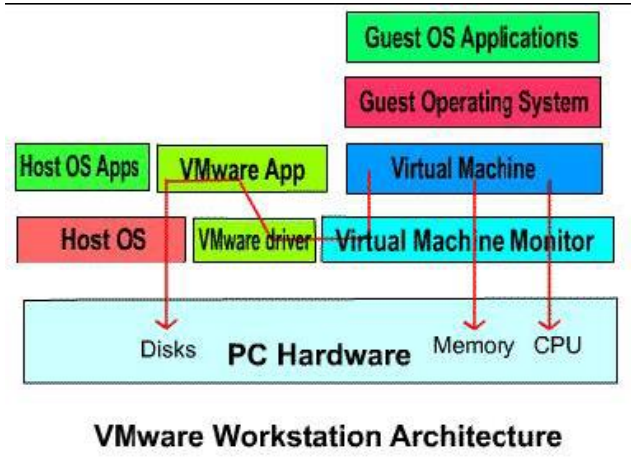
  how to improve portability, and increase software development efficiency

  make the importance of virtual machine technology more obvious

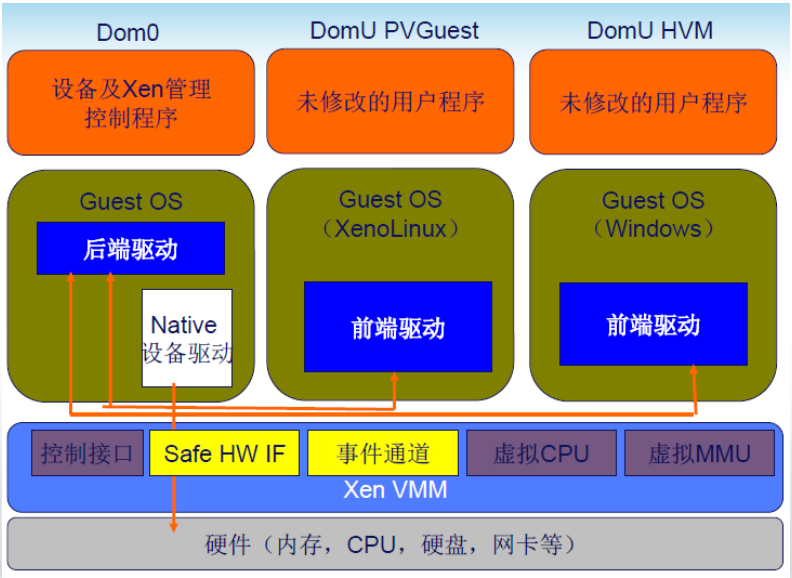
  make virtual machine technology become the research hotspot again

Architecture of Virtualization Technology





VMware Workstation Architecture



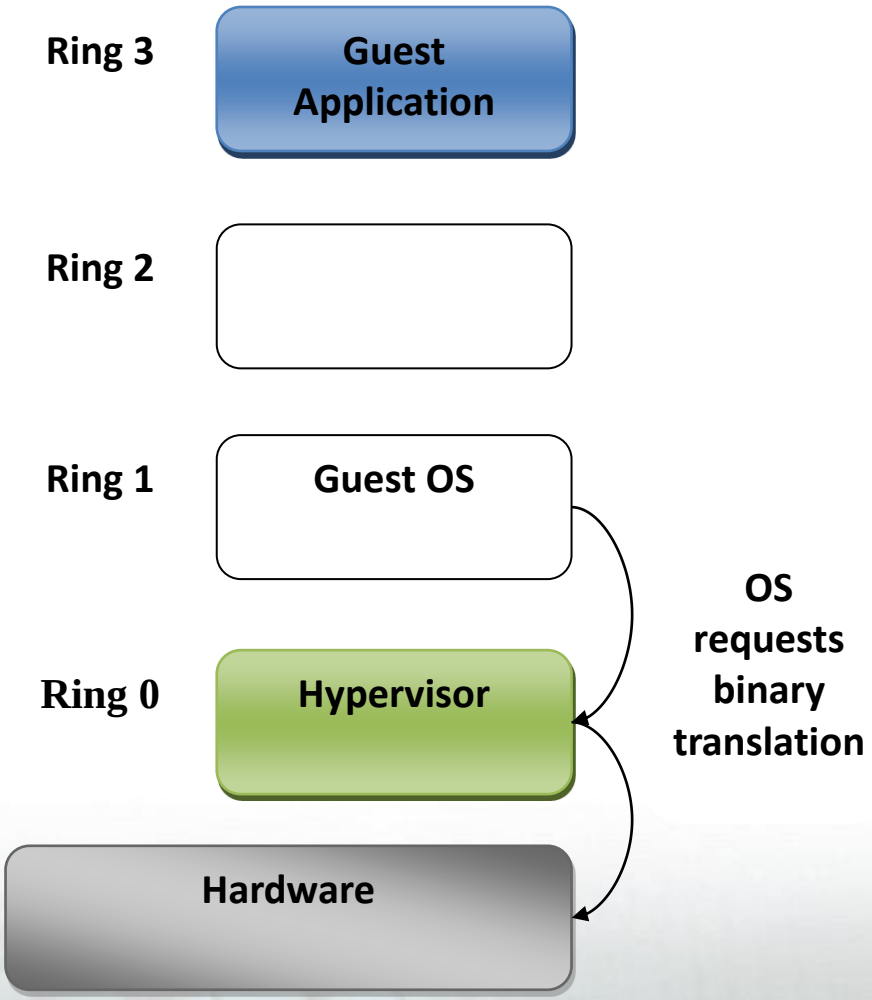
- **Virtual machine system is realized by adding a virtual layer VMM(virtual Machine Monitor or Hypervisor) to an existing platform(bare computer or operating system)**
  - **VMM**

    A system software, which can maintain multiple efficient and isolated program environment. VMM manages the real resources of computer system, and provides interface for virtual machines.
  - **VM（Virtual Machine）**

    A complete computer system with full functions of hardware system through software simulation, and runs in an absolutely isolated environment.
  - **Host OS**

    Some VMMs are installed on existing OS which is called the host OS.

Classification of Virtualization implementation technologies

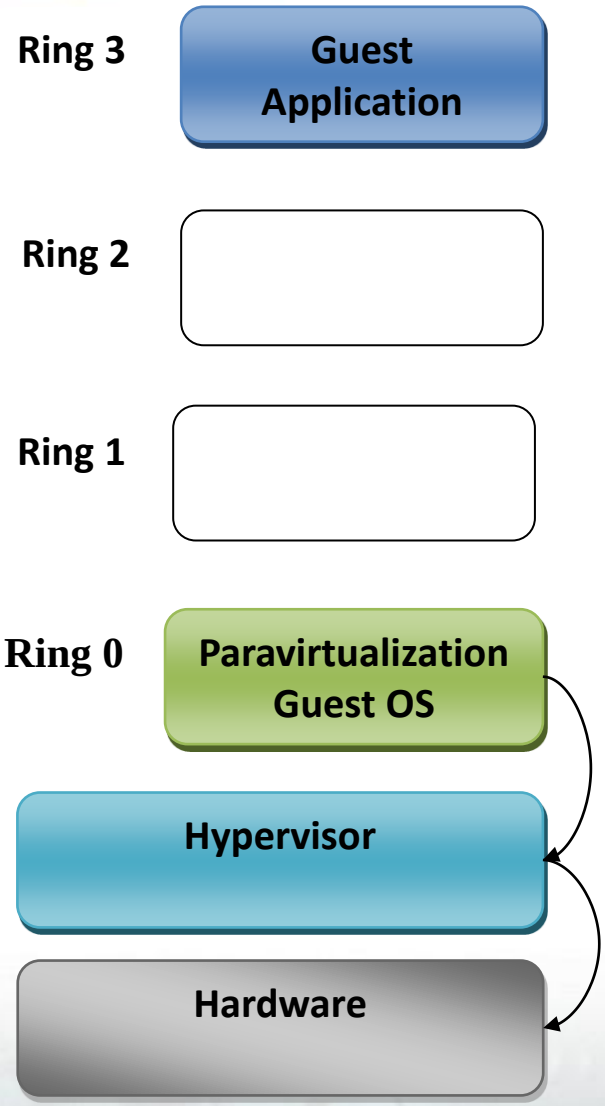


◆Full Virtualization

It uses a kind of technology called Binary Translation。The core idea is that the hypervisor runs in ring 0, which is responsible for the management of the underlying hardware. Guest OS runs in ring 1, and when they call the privileged instructions, VMM in the ring 0 will uses binary translation to stop these instructions and is responsible for the following work of the instructions.

Disadvantages:

software interception mechanism, high performance overhead

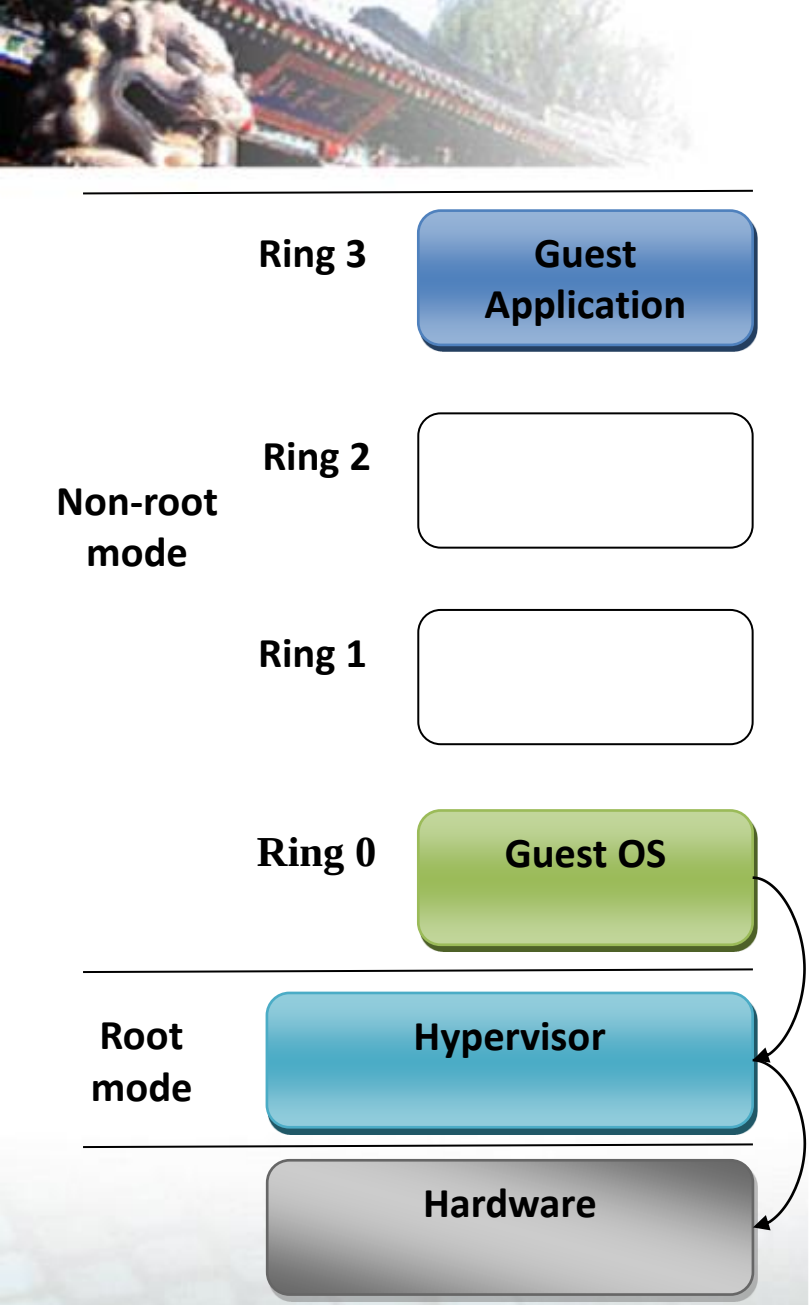


Para-virtualization

Guest OS can still run in ring 0, but we need to modify the OS kernel. The call for the privileged instructions calls into the hypervisor, which is called Hypercall. A typical representative of para-virtualization is Xen. So, when guest OS in the ring 0 calls privileged instructions, it will turn into Hypercall, but hypervisor still supervises the system hardware resources.

Disadvantage:

The need to modify OS kernel.



Hardware-assisted Virtualization

CPU needs to support virtualization technology. Besides ring 0 to ring 3, CPU needs to provide an additional ring for Hypervisor only, calling ring -1。 Guest OS still runs in ring 0, but when OS calls privileged instructions, they will be turned to Hypervisor in the ring -1 through hardware mechanism, and the Hypervisor manages the hardware.

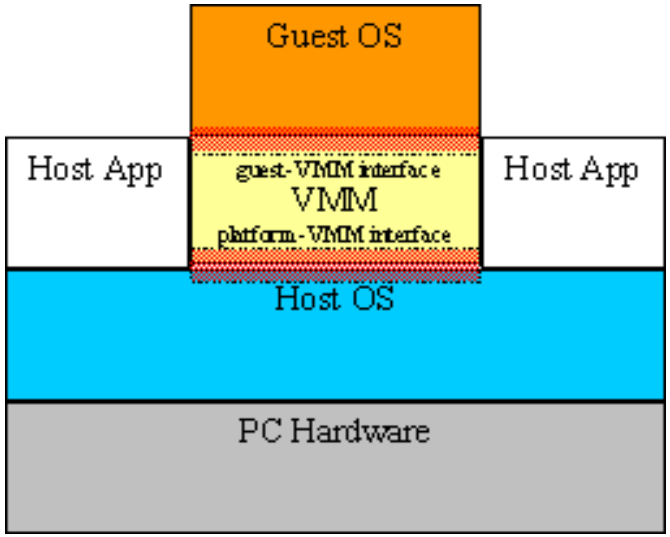
Disadvantages:

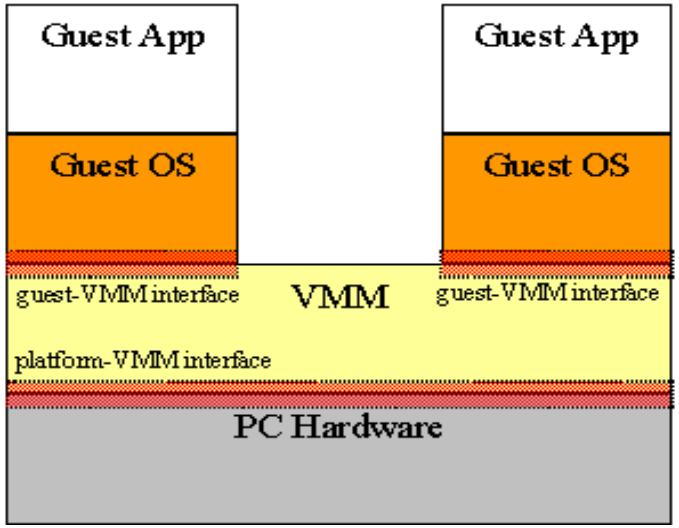
Need hardware support.(such as Intel VT, AMD SVM)

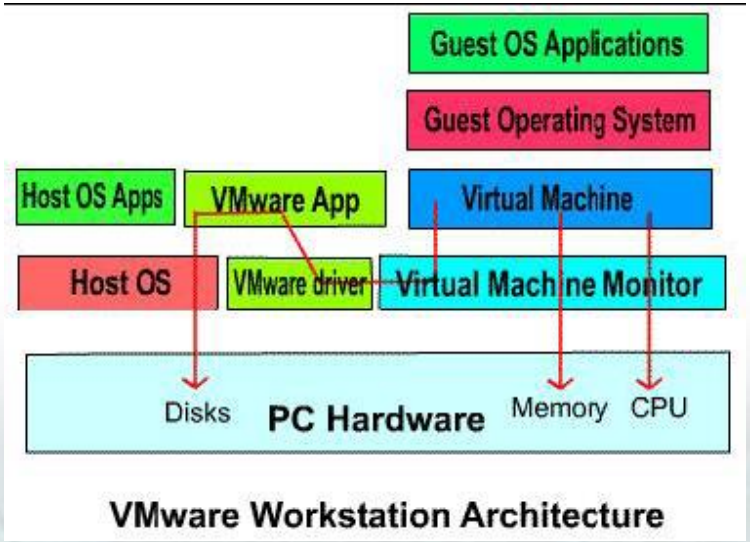
Classification of VMM

- Hosted -Need to run on Host OS, which provides the driver and hardware communication
  - ✓UMLinux, User-Mode Linux.
- Independent monitoring-Run directly on hardware layer
  - ✓VMware’s ESX Server.
  - ✓Xen
- Hybrid
  - ✓VMWare Workstation

Classification of VMM-I、II

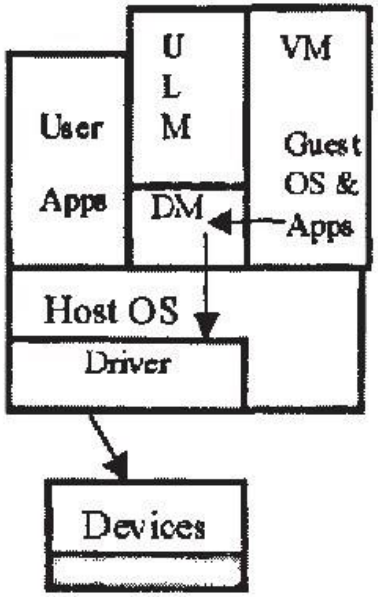




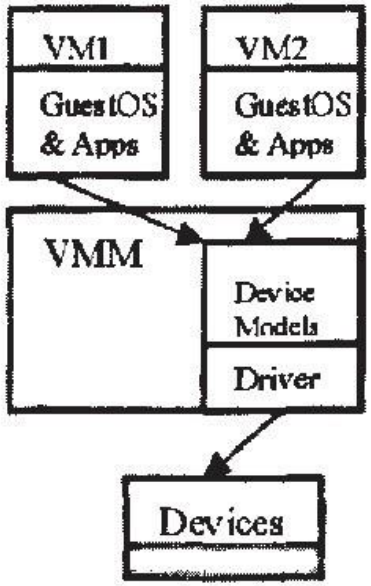


VMware Workstation Architecture

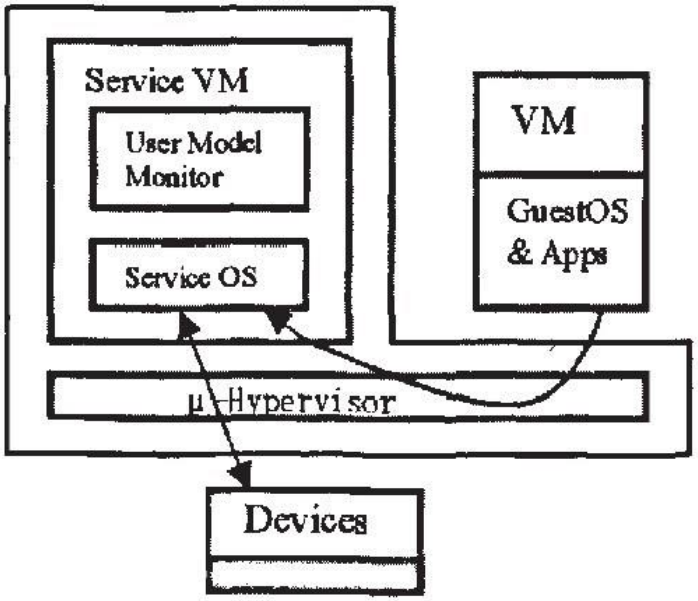
Classification of VMM



(a)宿主型 VMM



(b) 独立监控型 VMM



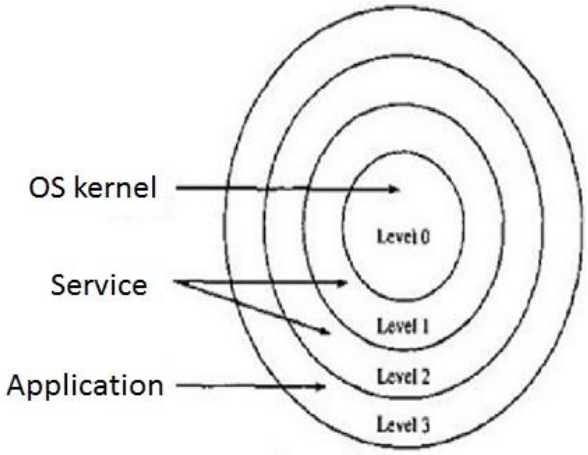
(c) 混合型 VMM

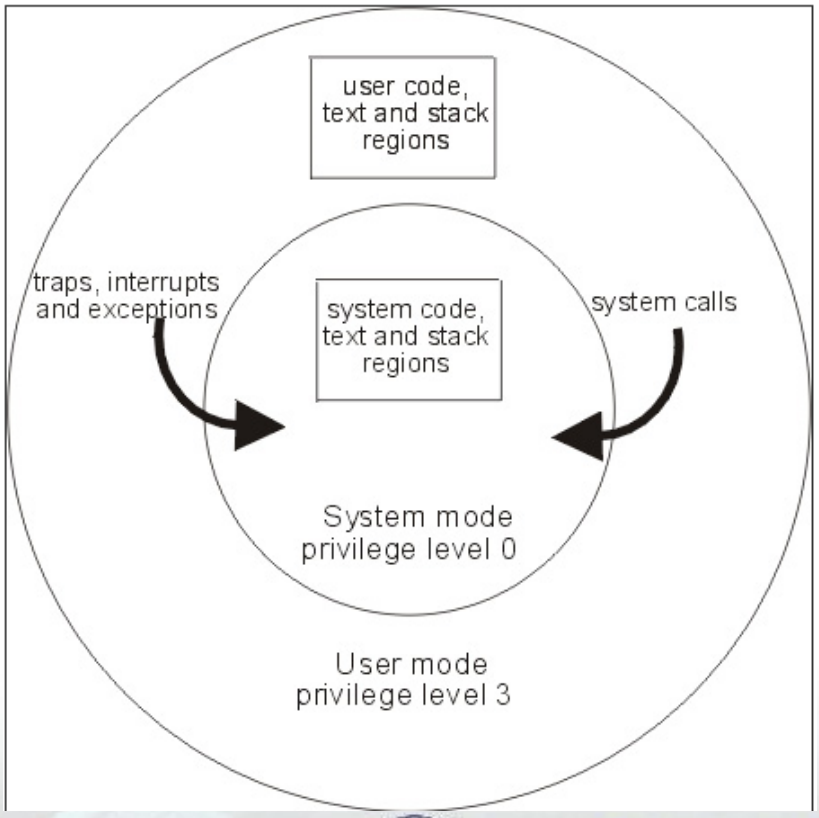
The implementation technology of VMM

- CPU Virtualization
- Memory Virtualization
- I/O Virtualization

CPU Virtualization

Traditional CPU level classification





- The x86 processor responses to 4 different priority, called ring 0 to ring 3. Ring 0 has the highest priority, and ring 3 has the lowest priority. Ring 0 is used for OS kernel, ring 1 and ring 2 are used for OS services, and ring 3 is used for applications.

北京大学

Privileged and non-privileged instructions

The instruction set is usually divided into two kinds of instructions, which are non-privileged and privileged instructions.

Non-privileged does not change the value or state of shared resources。Shared resources include processor, memory, timer, and registers of special purposes. Non-privileged instructions include arithmetic instructions、logic instructions, and so on.

Privileged instructions are all used to access the value or state of shared resources, including shutdown, set the timer, set the program counter, change the value of the relocation register and instructions associated with I/O。

Non-privileged instructions can be directly executed by VMM, while the privileged instructions require simulation execution

北京大学

Difficulties of the CPU classification in virtual system

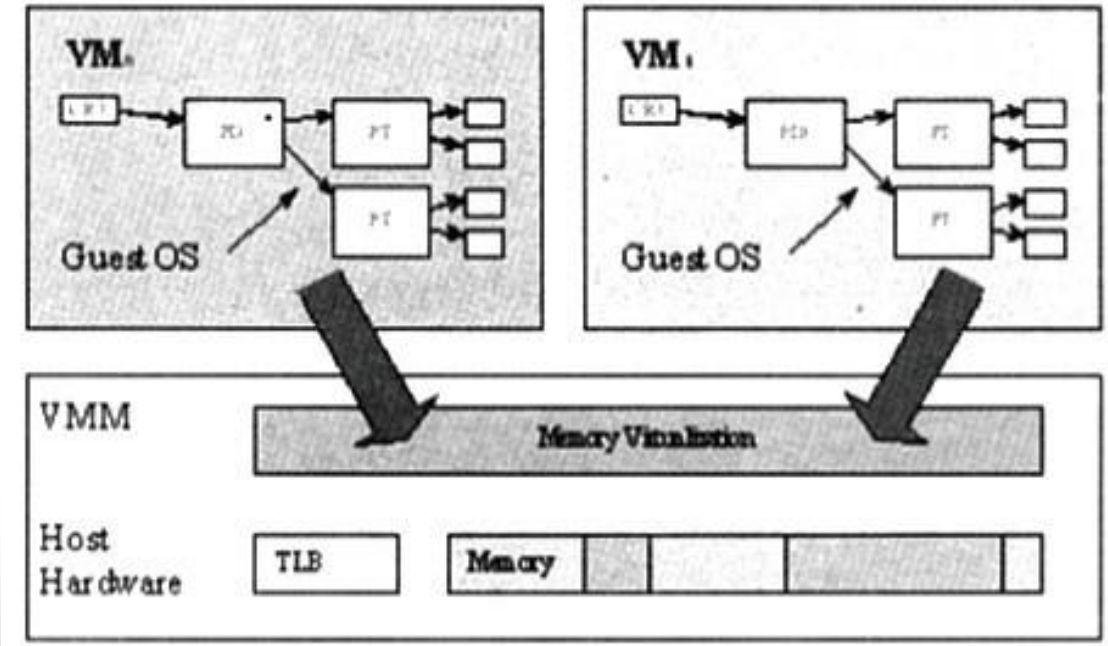
- Generally speaking, Host OS should run in Ring 0, but in order to avoid the destruction to Host OS by Guest OS , Guest OS must run under Ring 0(such as Ring 1). The problem is that, in order to realize the full system functions of Guest OS, the thread must be in Ring 0. So virtual software needs to coordinate with Guest OS and Host OS of the thread priority, and this kind of transformation will inevitably increase system complexity, which leads to poor performance of software virtual technology, and the processing ability of CPU and memory will be largely spent during this process. Data shows that this kind of degradation of system performance will be 5% to 40%.

Hardware CPU virtualization

- **In order to improve the efficiency of CPU virtualization, we need to use hardware to realize the switch of different levels.**
- **In the field of server, CPU can put VMM in ring -1.**
- **Thus, Intel and AMD develop VT-x and AMD-V technology respectively, realizing the isolation between VMM and Guest OS with the help of CPU.**

Memory Virtualization

VMM must has the ultimate control of physical memory, that is to say, it must control the operation of mapping guest physical address space to host address space. In this way, we can realize memory virtualization.



Method of memory virtualization

VMM maintains a virtual machine memory management data structure --shadow page table. VMM allocates memory pages to different virtual machines through shadow page table. Like OS virtual memory, VMM can map virtual machine memory pages to disk, so virtual machine can apply for more memory than machine physical memory. VMM is also able to allocate memory dynamically according to each virtual machine's requirements.

Frequent change to page tables by OS increases the **overhead** of **updating the shadow page table operation**, so **using hardware** to **manage shadow page table will be the future research direction**.

I/O Virtualization

Hosted I/O Virtualization

With the structure of host, and **use drivers of hosted OS's I/O device**.

Disadvantages:

✓**It greatly increases the performance overhead of virtualization.**

✓ **Modern OSs such as Windows and Linux have no support for resources management to provide performance isolation and service assurance, which are basic requirements of many server environment.**

Hardware I/O Virtualization

The trend of I/O subsystem is toward the direction of the development of hardware support. It is possible to transmit I/O device to software in virtual machines directly with enough hardware support. This will effectively eliminates all I/O virtual overhead. To do this, I/O device needs to get hold of virtual machine and support multiple virtual interface, so that VMM can safely map interface to virtual machine.

Intel VT-d is **the representative of hardware I/O virtualization**

Main Points

- Status and trends in data center
- Definition of virtualization
- Common types of virtualization
- Key technologies of sever virtualization
- Mainstream virtualization softwares and the practice of virtualization technology

Mainstream virtualization softwares

VMWare: Not open source

- **VMware-ESX-Server**

  Can directly run on top of hardware without host OS.
  In fact, it is a modified Linux kernel.

- **VMware-WorkStation, VMware-GSX-Server**

  Need host OS

◆Xen: Open source

- Xen virtual machine which is also called Xen VMM, is an open source project developed by computer laboratory of Cambridge University.
- Xen virtual machine has two kinds of operation modes:
  - Full virtualization
  - Para virtualization

北京大学

Hardware support for virtualization

INTEL VT series

VT-x: Virtualization Technology for IA-32

Processor assisted virtualization

VT-d: Virtualization Technology for Directed I/O

I/O assisted virtualization: direct I/O

VT-c: Virtualization Technology for Connectivity

Network assisted virtualization

TXT- Trusted Execution Technology

Practice of virtualization technology

Tasks:Choose one of the following topics.

VM name of each group should be unified as follows:

Group Number + Crew initials +VM Sequence number

For example : The second VM of group one should be name 1zslswwzl2 while all the members are Zhang Shan, Li Si, Wang Wu and Zhao Liu. Please screenshot the name.

1.Install an operating system in virtual platform, and create an account (Degree of difficulty☺)

1-2 people per group

2.Establish a ftp connection between two OSes in virtual platform(Degree of difficulty☺☺)

2-5 people per group

3.Build virtual platform on the OS on virtual platform, and install an OS on it. (Degree of difficulty☺☺☺)

5-7 people per group

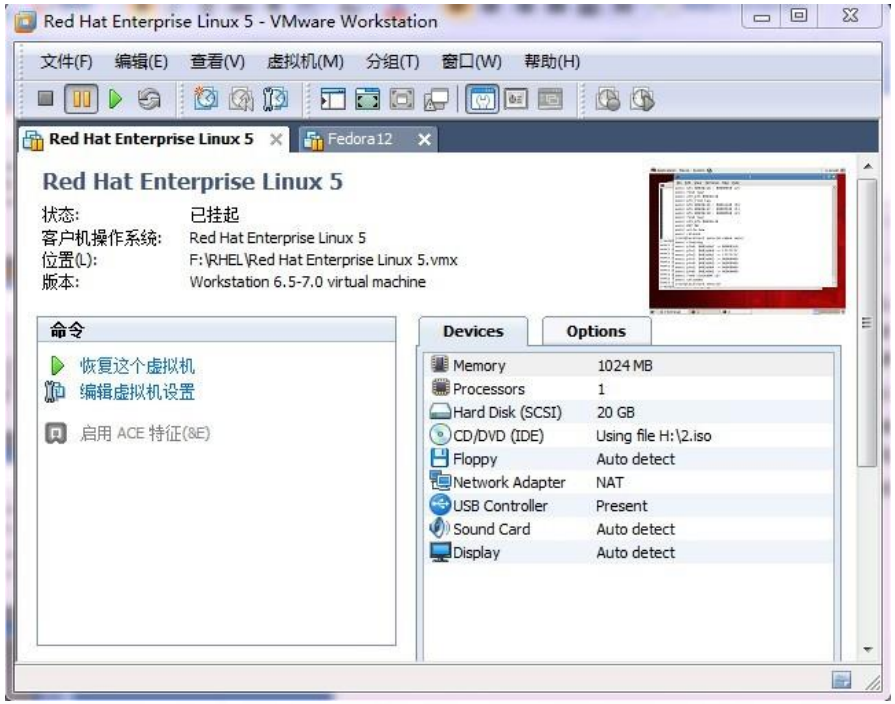
Experimental purposes

1>Understand the concept of virtualization
2> Master how to set-up and use virtual machine
3> Understand the way of establishing a network connection between VMs(2)
4> Understand basic operations of Vmware and Xen, and how to install OS on them.(3)

Experimental requiremnt

1>Install a Virtual machine Monitor.
2>Install OS on virtual platform
3>Establish a ftp connection between VMs(2)
4>Build a virtual platform on the VM on virtual platform , and install os on it.(3)
5>Write lab reports, screenshots and proper interpretation of each step is required.

Resource Required



- Vmware Workstation
- http://www.xdowns.com/soft/softdown.asp?softid=64236

北京大学

Resource Required II (1 out of 3)

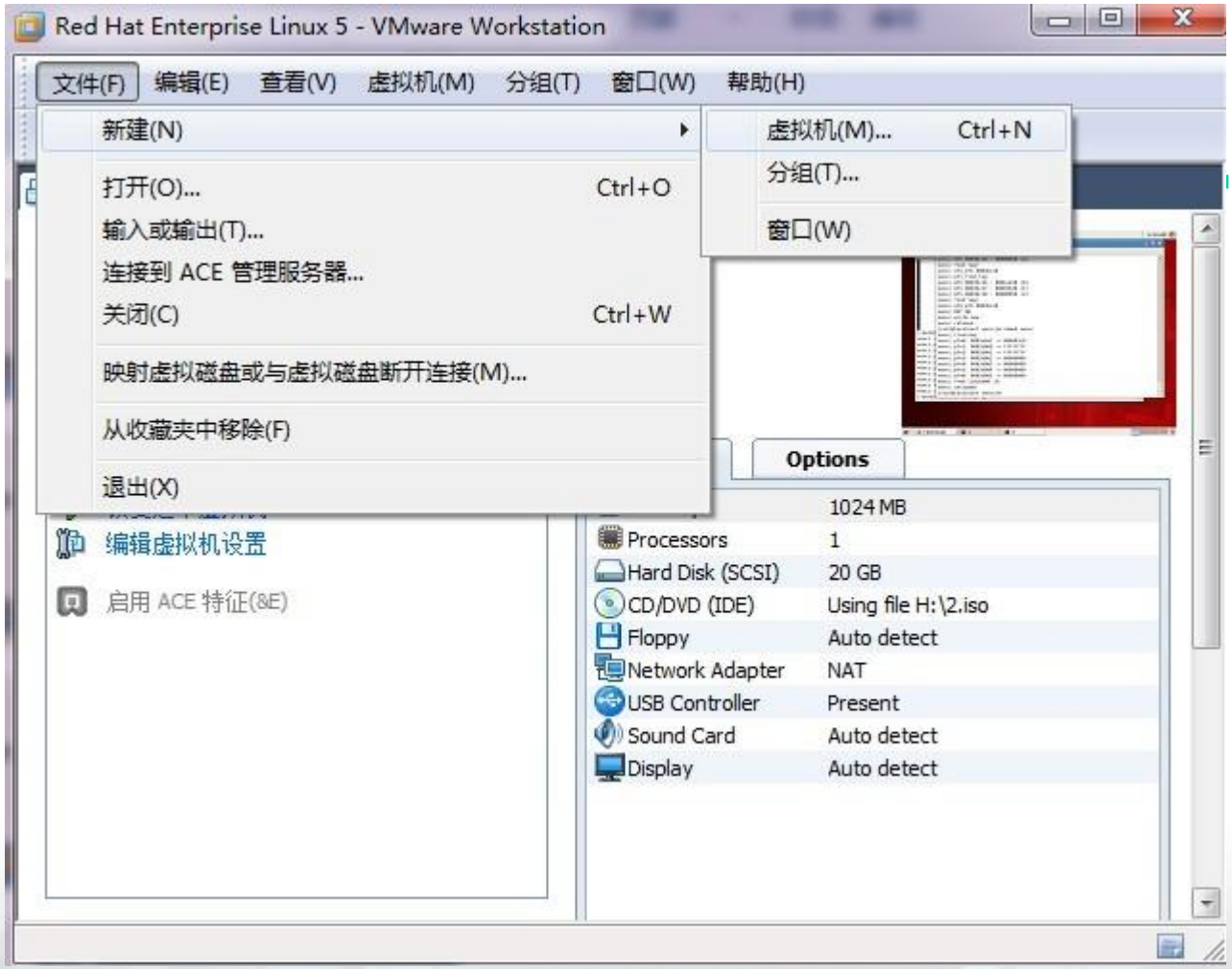
- Ubuntu
- http://cdimage.ubuntu.com/dvd/current/maverick-dvd-i386.iso

- Fedora
- http://download.fedoraproject.org/pub/fedora/linux/releases/14/Fedora/i386/iso/Fedora-14-i386-DVD.iso

- Opensuse
- http://ftp.jaist.ac.jp/pub/Linux/openSUSE/distribution/11.3/iso/openSUSE-11.3-DVD-i586.iso

北京大学

Creation of VM



Step 1: Open Vmware, Choose **File > New > Virtual Machine**

- **Step 2 :** Select **Typical** configuration

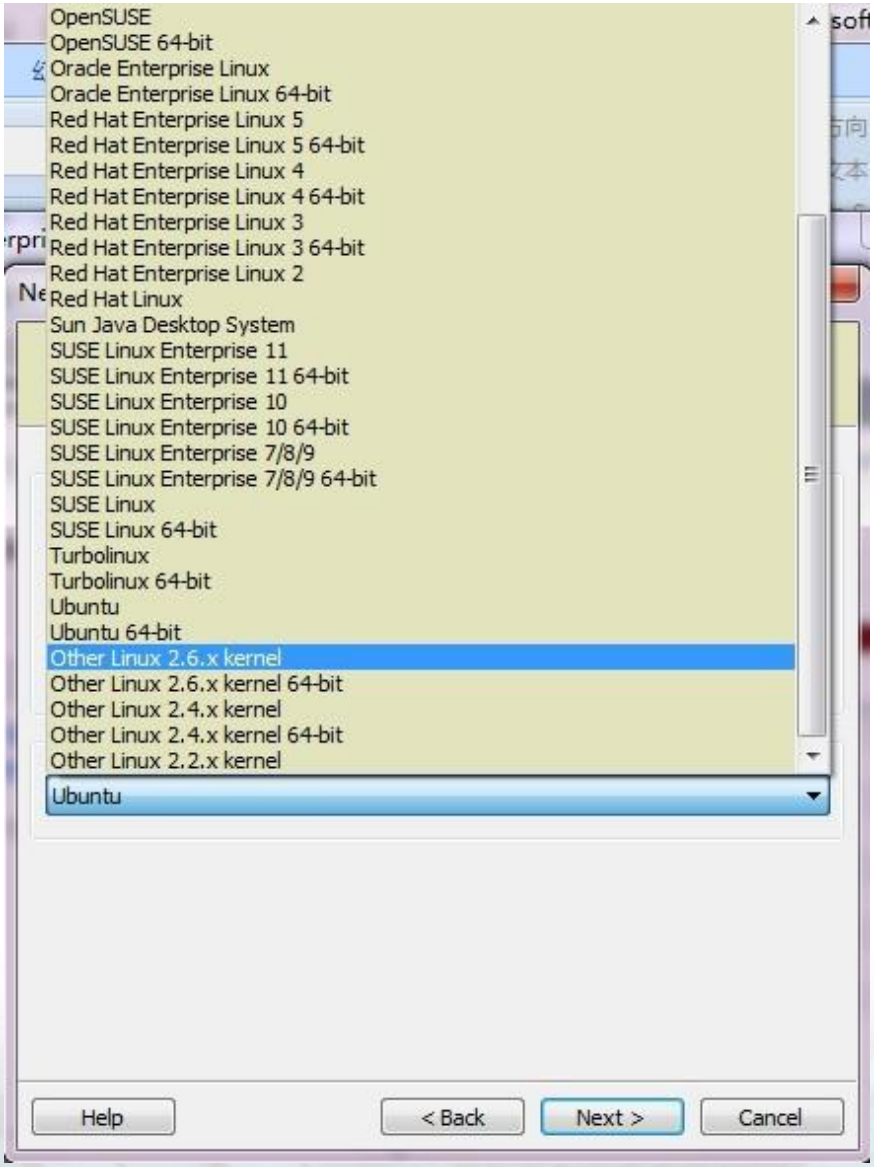
北京大学

- **Step 3： Select installation image-iso**
- **In the browser, select the downloaded installation disk file.**

北京大学

- **Step 4： Select a guest operating system.** Select Windows(Windows 2000/xp)
- Select Linux(Fedora,Ubuntu, OpenSUSE,RHEL)

北京大学



- **Step 5： Select a specific type of operating system**
- Choose “other linux 2.6.x kernel” in case it is Fedora.
- Choose directly if it is Ubuntu or opensuse.

北京大学

- **Step 6 : Select a name and folder for the virtual machine.**
- **Name method again**:

Group Number + Crew initials +VM Sequence number

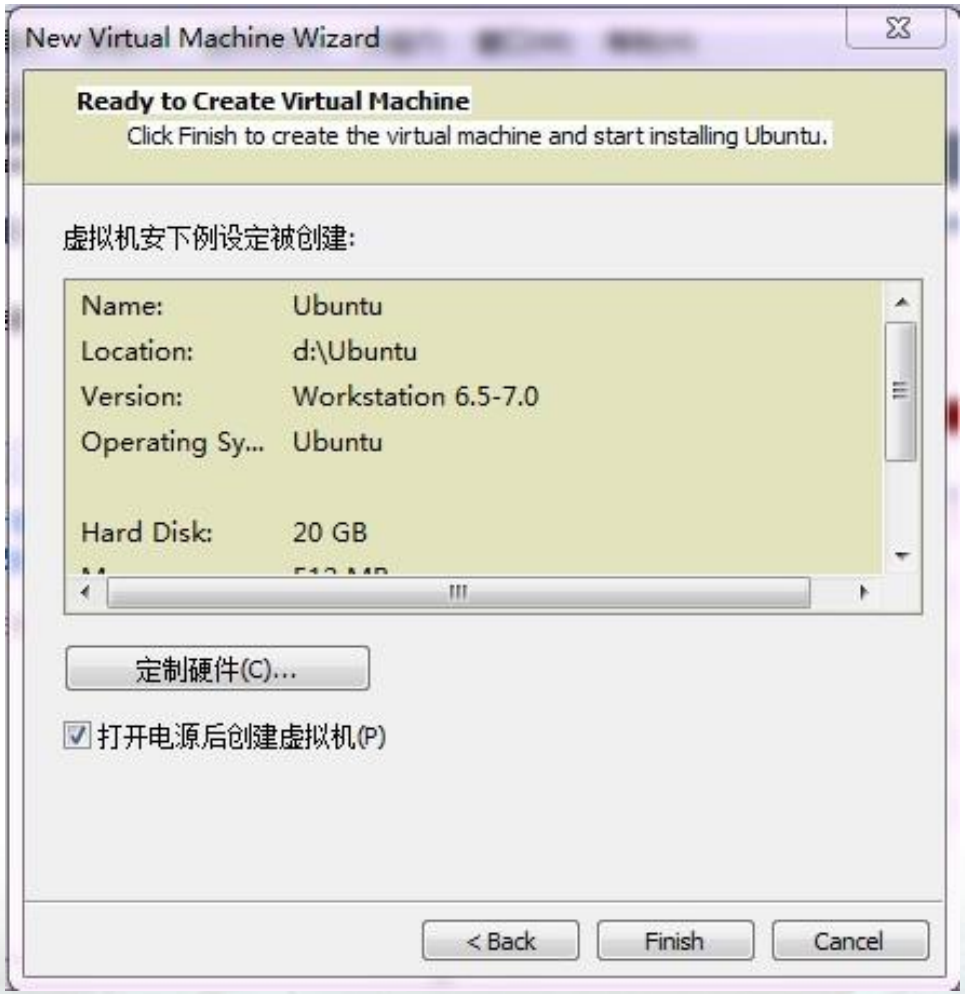
For example: The second VM of group one should be name 1zslswwzl2 while all the members are Zhang Shan, Li Si, Wang Wu and Zhao Liu.

- **Enter VM installation address.**

北京大学

- Step 7： Specify the capacity of the virtual disk, generally more than 10G
- Choose>Store as a single file

北京大学



- Step 8，Click **Finish**

北京大学

- **Installation of the operating system is very friendly to the novice, and it can be finished independently.**

Note that

- 1. root is equivalent to the Windows administrator, and you probably need to set a administrator password, similar to the password of Windows administrator

- 2. Recommend gnome desktop for Fedora and Ubuntu, KDE desktop for OpenSUSE

If you need to get in depth knowledge, please refer to:

- Opensuse:http://linux.chinaunix.net/techdoc/beginner/2009/01/01/1055973.shtml
- Fedora:http://wenku.baidu.com/view/ce7083ce05087632311212cd.html
- Ubuntu:http://server.zol.com.cn/121/1218526.html

Set-up of FTP Server (Optional)

- start up the virtual machine
- Open a terminal in the virtual machine operating system
- **Note: In general, the terminal program can be found in the application menu**

北京大学

- **start ftp service:**
- **Note that it is likely to be in normal user mode when you start the terminal at first. We need to enter the root mode to start it. The method is: enter the command: su**
- **then enter the password of root.**
- **then enter the commands as shown, you can start ftp service.**

```
[ [redacted]@[redacted] init.d]$ su
密码：
[ root@[redacted] init.d]# /etc/init.d/vsftpd start
为 vsftpd 启动 vsftpd：                                    [确定]
[ root@[redacted] init.d]#
```

- **Use ifconfig command to find the ip address of the local network adapter**
- **Inet addr of Eth0 is the local IP address**

```
bash-3.2# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0C:29:02:A7:C7
          inet addr:192.168.66.136  Bcast:192.168.66.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe02:a7c7/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:9344 errors:0 dropped:0 overruns:0 frame:0
          TX packets:89 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:2503588 (2.3 MiB)  TX bytes:21306 (20.8 KiB)
```

- **Start a VM terminal, and enter:**
  - **ftp (ip address of ftp server)**
- **Then, enter root/root password or user/user password that you create, or anonymous, so that you own another VM ftp client.**
- **Use "get (filename)" command to download file**
- **Use "bye" command to quit**

- **Detailed introduction of vsftpd can be found:**
- **http://linux.vbird.org/linux_server/0410vsftpd.php#server_vsftpd.conf**

Bibliography

1. University of Cambridge. User's Manual Xen v3.0.2002[EB/OL]. http://www.cl.cam.ac.uk/research/srg/netos/xen/readmes/user/
2. Paul Barham, Boris Dragovic, Keir Fraser. Xen and Art of virtualization. Proceeding of the nineteenth ACM symposium on Operating system principles, 2003,164-177
3. R.P.Goldberg. Survey of Virtual Machine Research[J]. IEEE Computer Magazine, 1974:34-45
4. Nanda, S., Chiueh. T. A survey on virtualization technologies 2005, http://www.ecsl.cs.sunysb.edu/tr/TR179.pdf
5. Michael Steil. Inside VMware. 2006 http://events.ccc.de/congress/2006/Fahrplan/attachments/1132-InsideVMware.pdf
6. 石磊, 邹德清, 金海. Xen虚拟化技术,湖北：华中科技大学出版社, 2009
7. Uhlig, R., Neiger, G..,Rodgers, D., et al. Intel virtualization technology. Computer, 2005,38(5):48-56

THE END, THANK YOU!

Intel UPO Supported

北京大学