TIM 50, LECTURE #7 (7/20/17)

Agenda:

1. Computer Networks
   - Basics
   - Networking between 2 application processes
   - Network design in a data-center

2. VIRTUALIZATION: Can we emulate hardware using software?

3. CLOUD COMPUTING: Can we host an entire data-center on a Cloud-based platform (Amazon Web Services; Microsoft Azure, ...)

4. Where next?
   (The Internet of Things: IOT)

1. Network Fundamentals

1.1 A network is a set of devices (or nodes) connected by communication links

node: computer, printer, mobile phones, any other device connected to the network

1.2 Types of Networks

LAN: local area network: private network in an organization, usually in 1 building

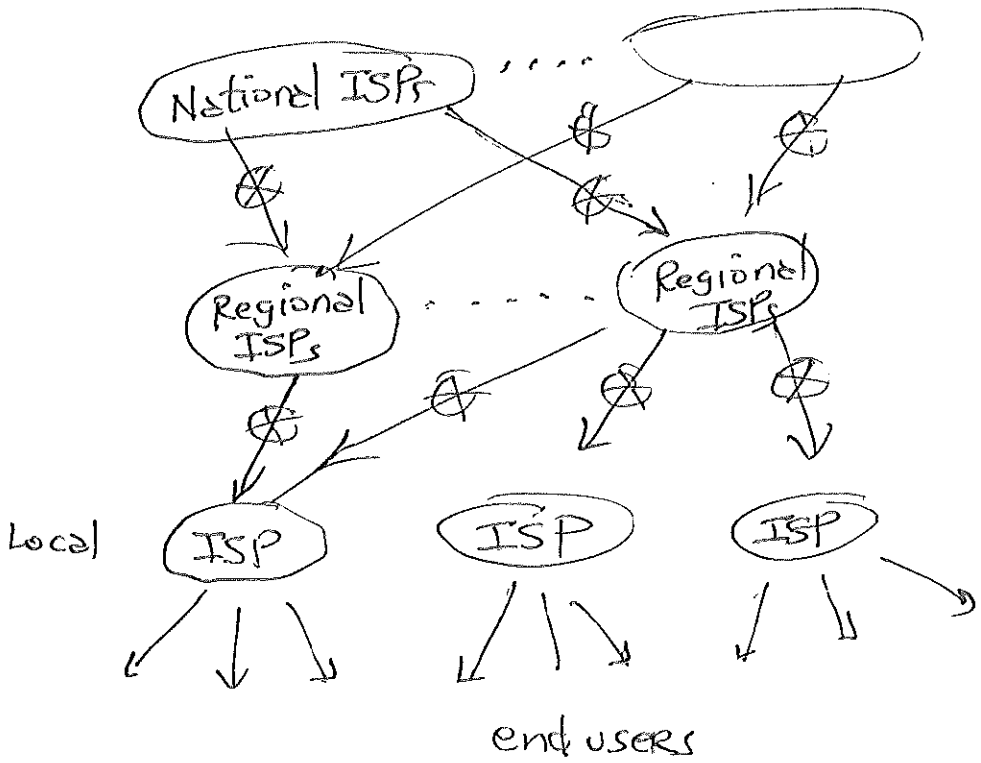
WAN: wide area network: provides long-distance transmission of data over large geographic areas: country, continent

MAN: Metropolitan area network (in between LAN and WAN)

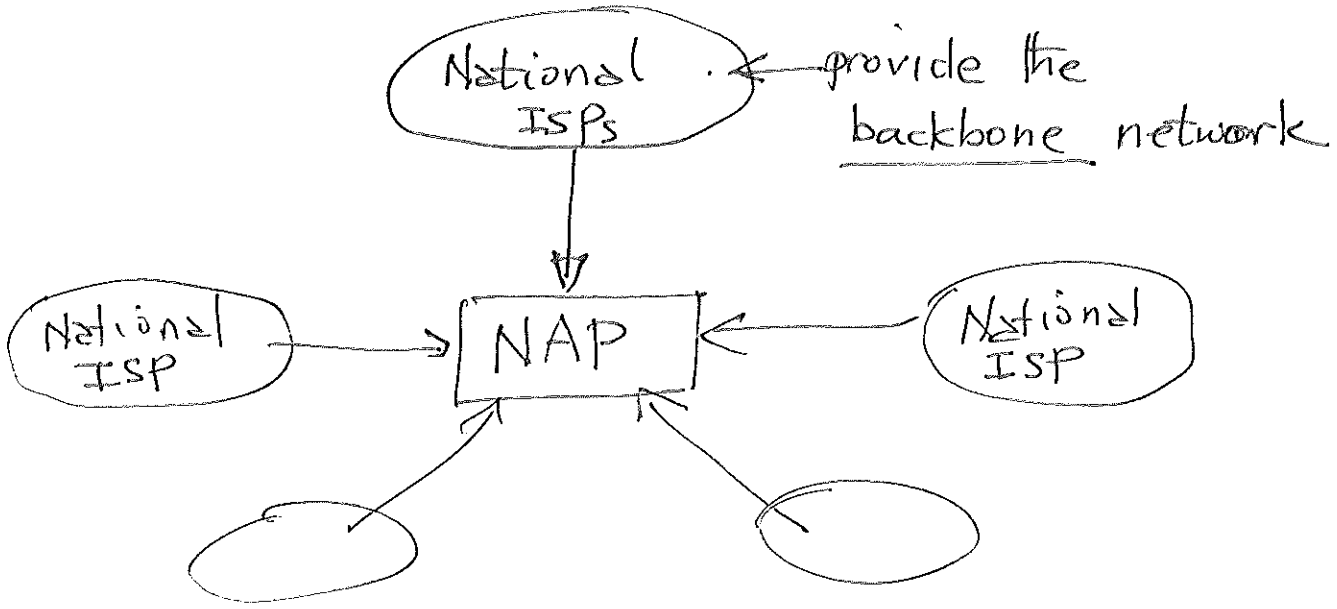
1.3 Interconnection of networks

- LANs, WANs, and MANs are connected to one another
- When two or more networks are connected to each other they become an Interconnected network or Internet

1.4. Internet Service Providers (ISPs) provide end-users with Internet connections



⊗: Routers used to transmit information



NAP: network access point is a complex switching station from which network access is provided to the end-users

1.5 LAYERS of the Network

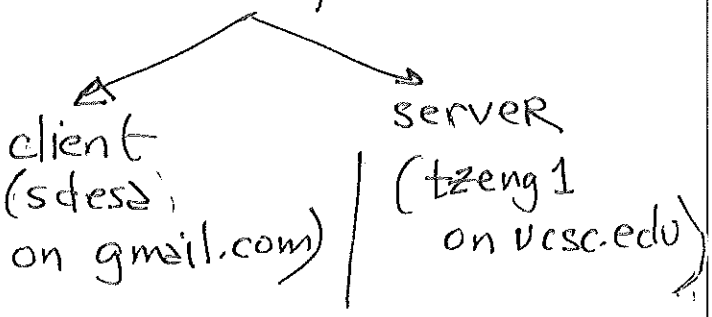
We have 4 layers (see Lecture #5)

- Data link layer
- Network layer
- Transport layer
- Application layer

1.6 How do the different layers of the network work together to transmit information from one host to another

Example: sending an e-mail message from my computer (sdesa@gmail.com) to the TA, Tianchi (tzeng1@ucsc.edu)

Application layer: e-mail process: two parts



Step 1

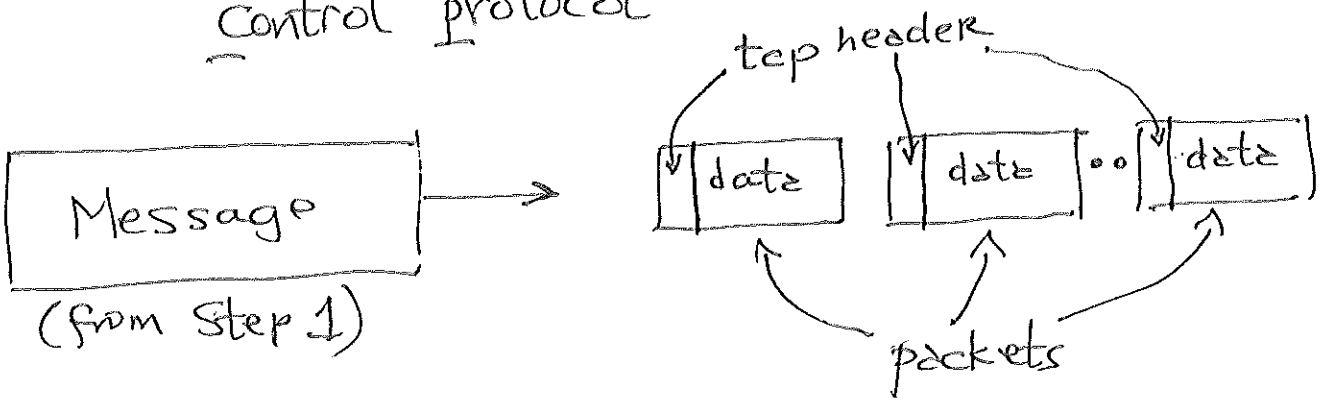
my gmail client process converts my e-mail message into a message for transmission across the internet uses an application protocol

smtp: simple mail transmission protocol

another familiar application protocol for web-browsers: http (hypertext transmission protocol)

Step 2 : The converted message (using smtp) is passed on to the Transport layer where it is broken up into packets for transmission across the internet.

The protocol for transmitting data packets is called tcp : transmission control protocol



Transport layer has 2 functions

- guarantees delivery of the packets
- re-assembles packets in the right-order

Step 3 : These packets are sent to the Network layer, where we add the source and destination address

We use a protocol called ip (internet protocol)

which specifies the source and destination address, for example: 128.41.23

↑ for example the ip address of vesc.edu e-mail server

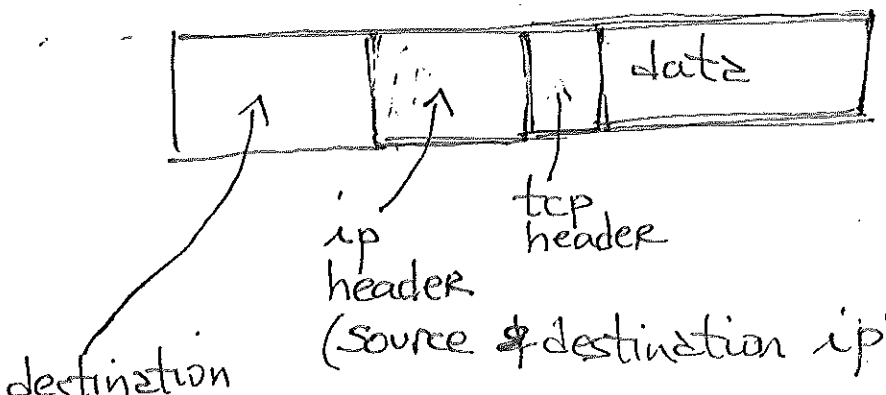
domain name of the vesc e-mail server

(DNS)

Domain Name System maps:

- domain names to their ip addresses on the internet

At the network level the data packet looks like this:

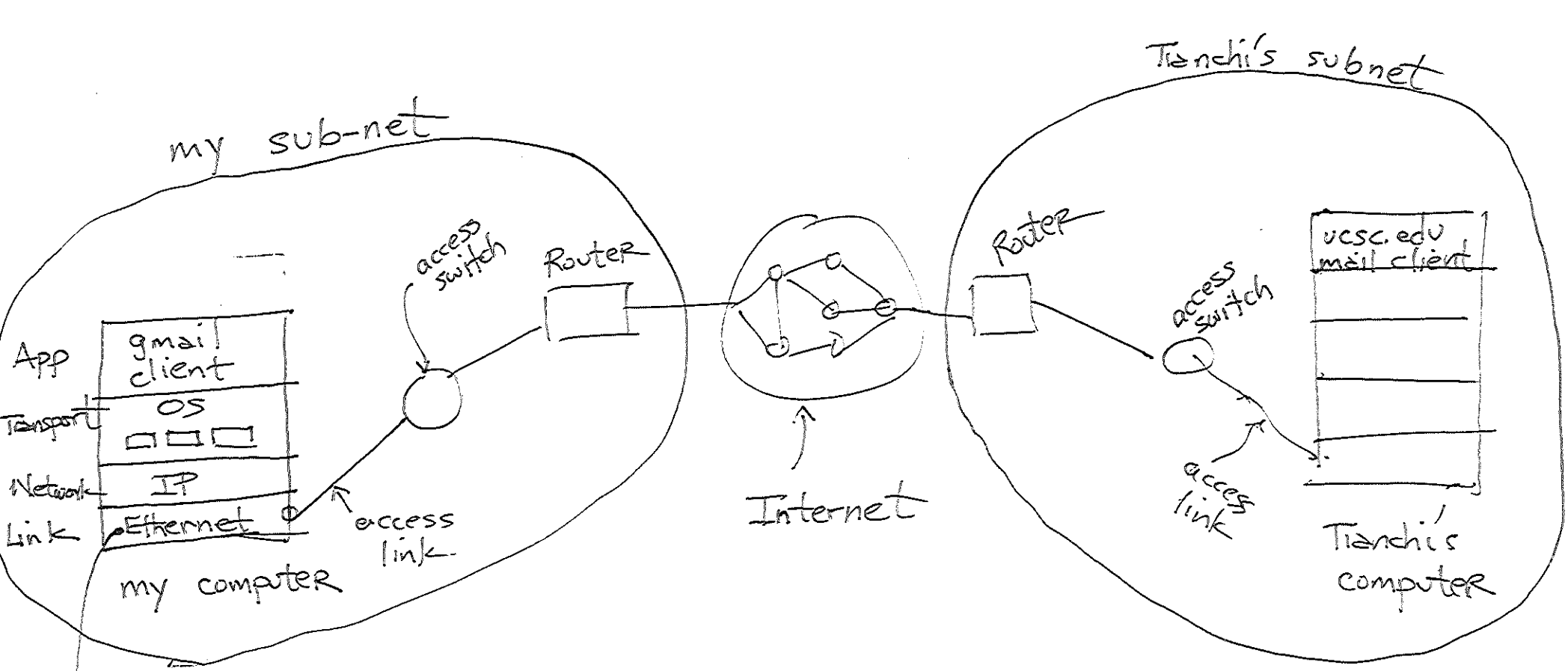


link address: address of the next node in the transmission of the data-packet ("next hop" across the internet)

Step 4 : Pass the packets to the Link layer for transmission across a single link (single "hop"), in this case the access link

Step 5 : The packets are now transmitted from link (hop) to link (hop) using a Routing Table created by the internet (ip) layer.

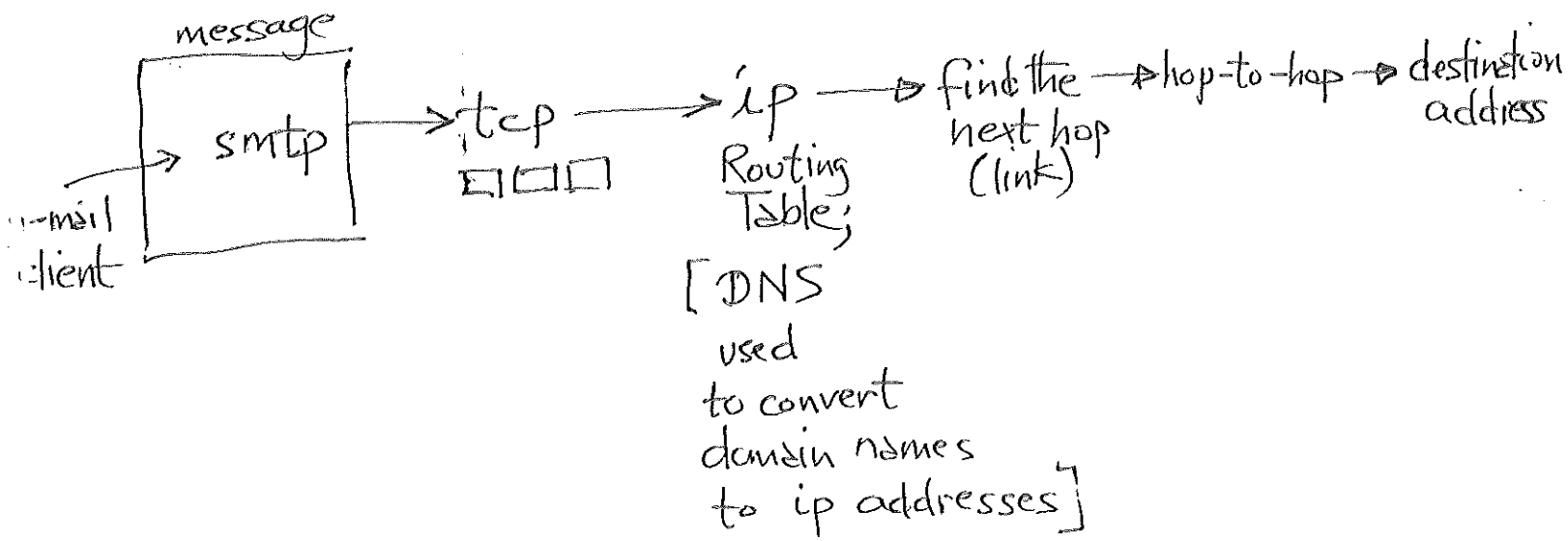
At the link layer, packets are called frames.



Ethernet Network Interface Card: enables frames to be transmitted across the network (Step 5)

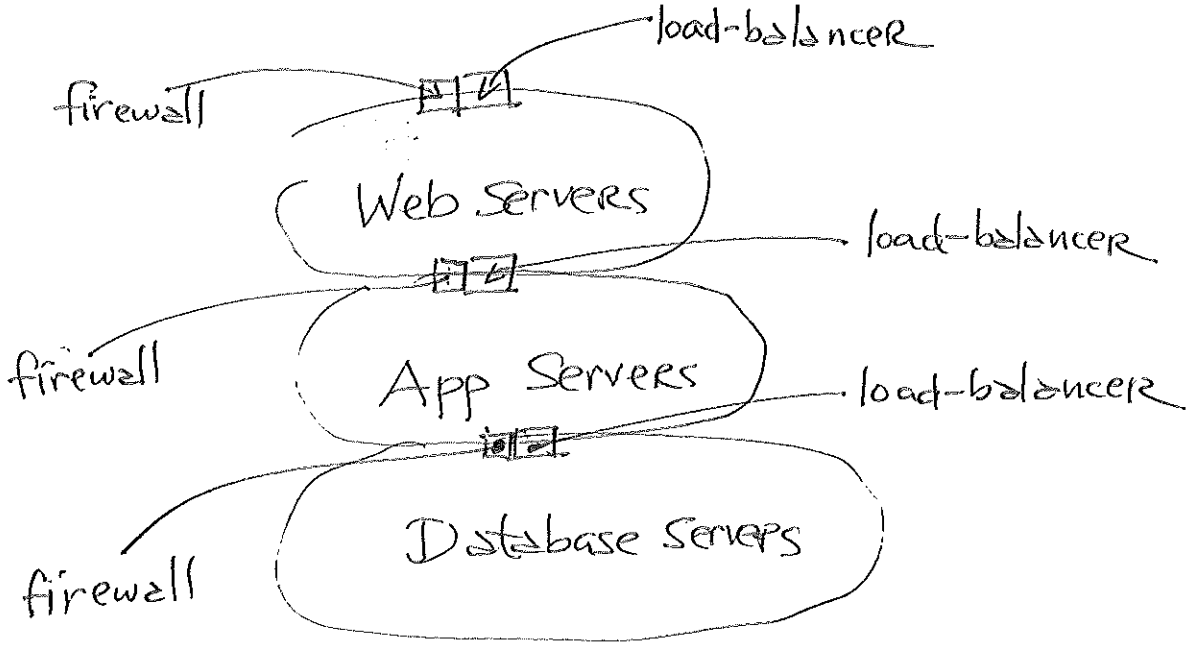
step 6 : When the frames (from step 5) reach the destination address (i.e., the ip address of the ucsc e-mail server), they are converted into data packets at the network (ip) layer, then re-assembled at the transport (tcp) layer; and finally converted into the actual e-mail message by the ucsc e-mail server application process.

Protocol view of things:



Step 7: Determine where fire-walls & load-balancers need to be added

For example, in the 4-Tier on-line bookseller IT architecture



Database servers have a load-balancer to balance the traffic between the data-base servers; and a firewall (a router that places restrictions on the data that is transmitted accross it) to ensure the security of the data transmitted across it.

& similarly app servers & web servers } will have firewalls & load-balancers as shown above.

Read the chapter "Telecommunications, the Internet, and Wireless Technology" in the EMIS text by L[2].

3. Network architecture for a Data-Center (e.g. for the on-line bookseller studied in earlier lectures)

Def. of the problem:

Design the network architecture for a data center in an organization that is

- Reliable
- Secure
- Scalable

} requirements

Process:

1. Define the network devices that are needed
   (a) routers/switches (R/S)
   (b) load balancers (LB)
   (c) firewalls (FW)

2. Map the requirements to the necessary devices

Requirement	R/S	LB	FW
Scalability	X	X	
Reliability		X	
Security			X

Step 3: Based on layering (software & hardware) of the IT architecture, define a set of sub-nets

Example

web-server layer → web-server sub-net (that connects all the web-servers)

app server layer → app server sub-net

DB server layer → DB server sub-net

Step 4: For each sub-net, determine the network topology (or configuration) to connect the servers in the sub-net using switches (& routers)

Step 5 : Connect between the sub-nets using routers to achieve the n-tier hosting architecture

Step 6 : [Scalability & Reliability] Add load-balancers for each layer of the architecture

step 7 : (Security) Add firewalls for each layer of the architecture.

4. Virtualization

4.1 Motivation:

Currently most computer systems use only 5–10% of their computing resources: processing, storage, etc.

How do you maximize the use of the computer resources available on a computing device (laptop, server, cell-phone...)?

One solution: add an abstraction layer (or software layer) that abstracts (or emulates) the physical computing resources & re-allocates them more efficiently to maximize the use of available resources:

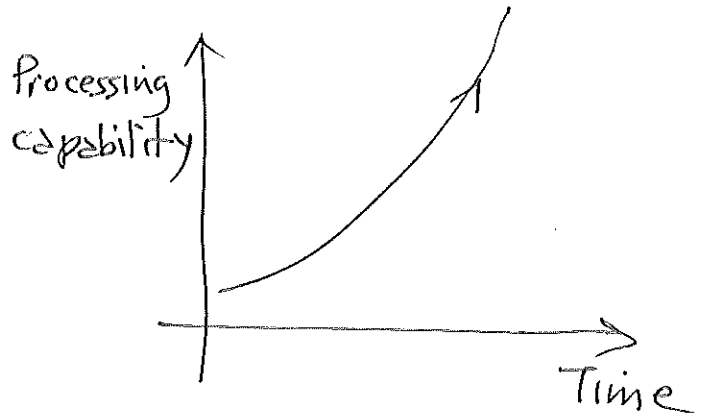
OS: most computers have a software layer, called the operating system, that supervises (controls) all the operations performed by the computer: applications, file manipulation, interaction with other devices, ...

In one version of virtualization, we add a software layer, called the Hypervisor ("supervisor of supervisors") that allows the host computer to run several guest Operating systems.

4.2. Key drivers of virtualization:

(1) Increase in processing power

Moore's Law: processing capability doubles every 18 months



Processing "supply" is available in large quantities

(2) Physical space: As we increase the number of servers, we need more physical space, which increases cost

If we can maximize the use of a physical server, then we can minimize the physical space we need

(3) Energy costs are increasing

If we can minimize hardware resources, then we can minimize energy consumption

(4) Data center administration costs can be decreased if we reduce the hardware requirements

Virtualization can minimize the costs associated with the 4 drivers above.

4.3 Definition of Virtualization

Here are the key attributes of virtualization

- single underlying piece of hardware, e.g., server, is coordinated by a software layer, called the hypervisor, so that multiple guest operating systems share a single piece of hardware
- Guest OS is the OS hosted by an underlying virtual software layer called the Host system
- Guest OS is unaware that it is "sitting" on top of a software layer rather than directly on physical hardware
- Guest OS appears to the application running on it as a complete OS.