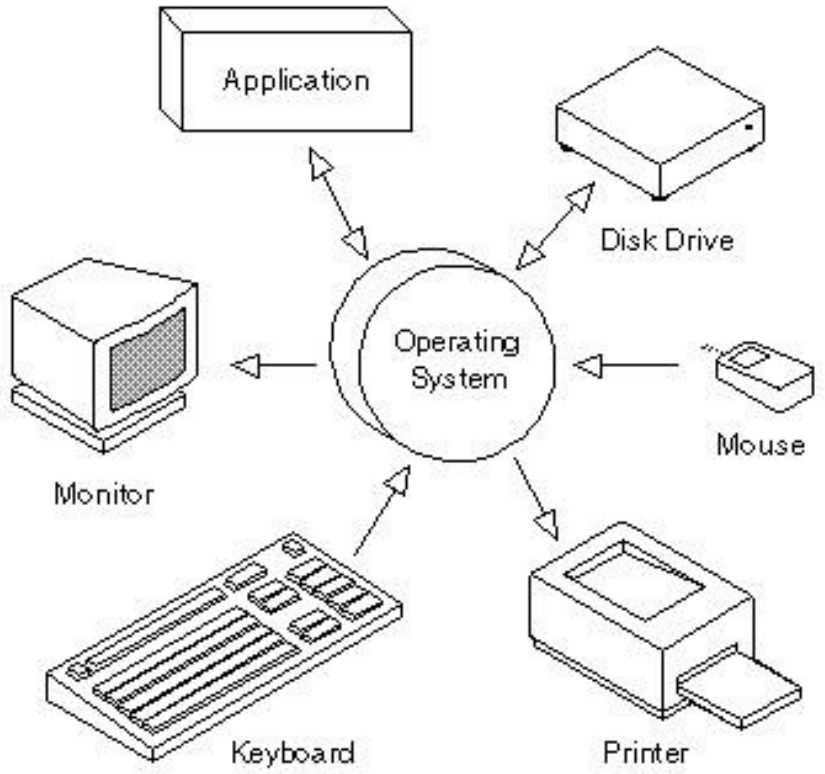
UNIT V
CASE STUDY

APEC

Features of Operating System

- Provide a user interface
- Organize files on disk
- Allocating resource to different users
- Co-ordinate programs to



APEC

work with devices and other programs



Operating System Case Study: Linux

Before Linux

- In 80's, Microsoft's DOS was the dominated OS for PC

- Apple MAC is better, but expensive
- UNIX is much better, but much much expensive.
- People was looking for a UNIX based system, which is cheaper and can run on PC
- Both DOS, MAC and UNIX are proprietary, i.e., the source code of their kernel is protected
- No modification is possible without paying high license fees

MAC – Macintosh Operating system
DOS – Disk Operating system

GNU project

GNU project

APEC

- "GNU's Not Unix"
- Established in 1984 by Richard Stallman, who believes that software should be free from restrictions against copying or modification in order to make better and efficient computer programs

Beginning of Linux

- A famous professor Andrew Tanenbaum developed Minix, a simplified version of UNIX that runs on PC
- Minix is for class teaching only. No intention for commercial use
- In Sept 1991, Linus Torvalds, a second year student of Computer Science at the University of Helsinki,

developed the preliminary kernel of Linux, known as Linux version 0.0.1

- It was put to the Internet and received enormous response from worldwide.



Linux Today

- Linux has been used for many computing platforms
- PC, PDA, Supercomputer,…
- Current kernel version 2.4, 2.5, 2.6
- Not only character user interface but graphical user interface.
- Commercial vendors moved in Linux itself to provide freely distributed code. They make their money by

compiling up various software and gathering them in a distributable format

- Red Hat, Slackware, etc
- Chinese distribution of Linux also appeared in Taiwan and China - CLE, Red Flag Linux

Where is Linux Used?

Where is Linux Used?

- 75% of respondents were already using Linux and another 14% were evaluating it
- 43% of all web sites use Linux servers running the Apache Web server

APEC

Linux Pros and Cons

- Advantages over Windows
  - It's almost free to relatively inexpensive
  - Source code is included
  - Bugs are fixed quickly and help is readily available through the vast support in Internet
  - Linux is more stable than Windows
  - Linux is truly multi-user and multi-tasking
  - multiuser: OS that can simultaneously serve a number of users
  - multitasking: OS that can simultaneously execute a number of programs
  - Linux runs on equipment that other operating systems consider too underpowered, e.g. 386 systems, PDA, etc

Linux Pros and Cons (Cont)

- Disadvantages compared with Windows
  - My program cannot run on Linux
  - Isn't as popular as Windows
  - No one commercial company is responsible for Linux
  - Linux is relatively hard to install, learn and use

  - Hence currently, Linux is mainly used in commercial applications, server implementation
  - More than 75% current network servers are developed based on Linux or Unix systems

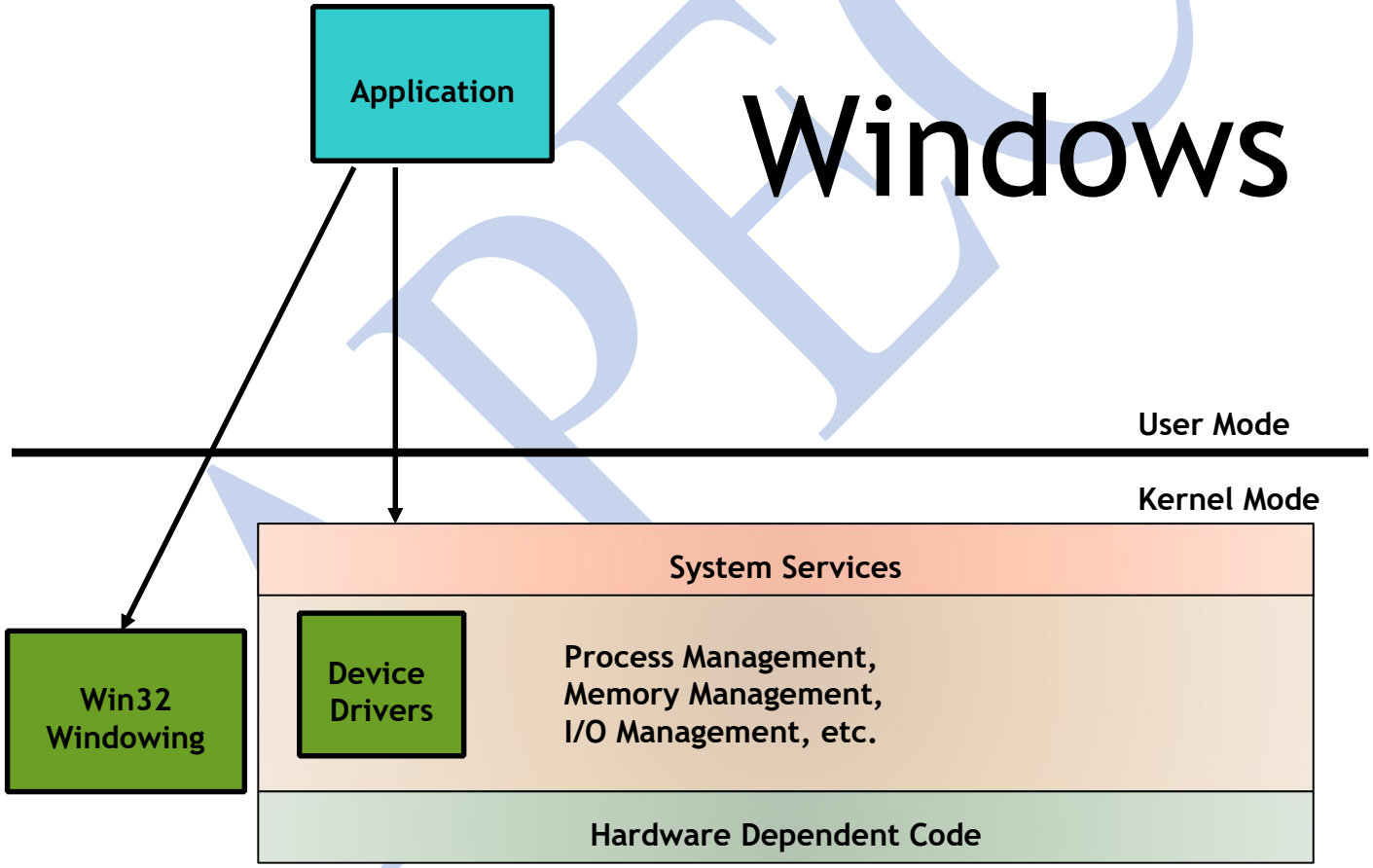
Linux Licensing

- The Linux kernel is distributed under the GNU General Public License (GPL), the terms of which are set out by the Free Software Foundation

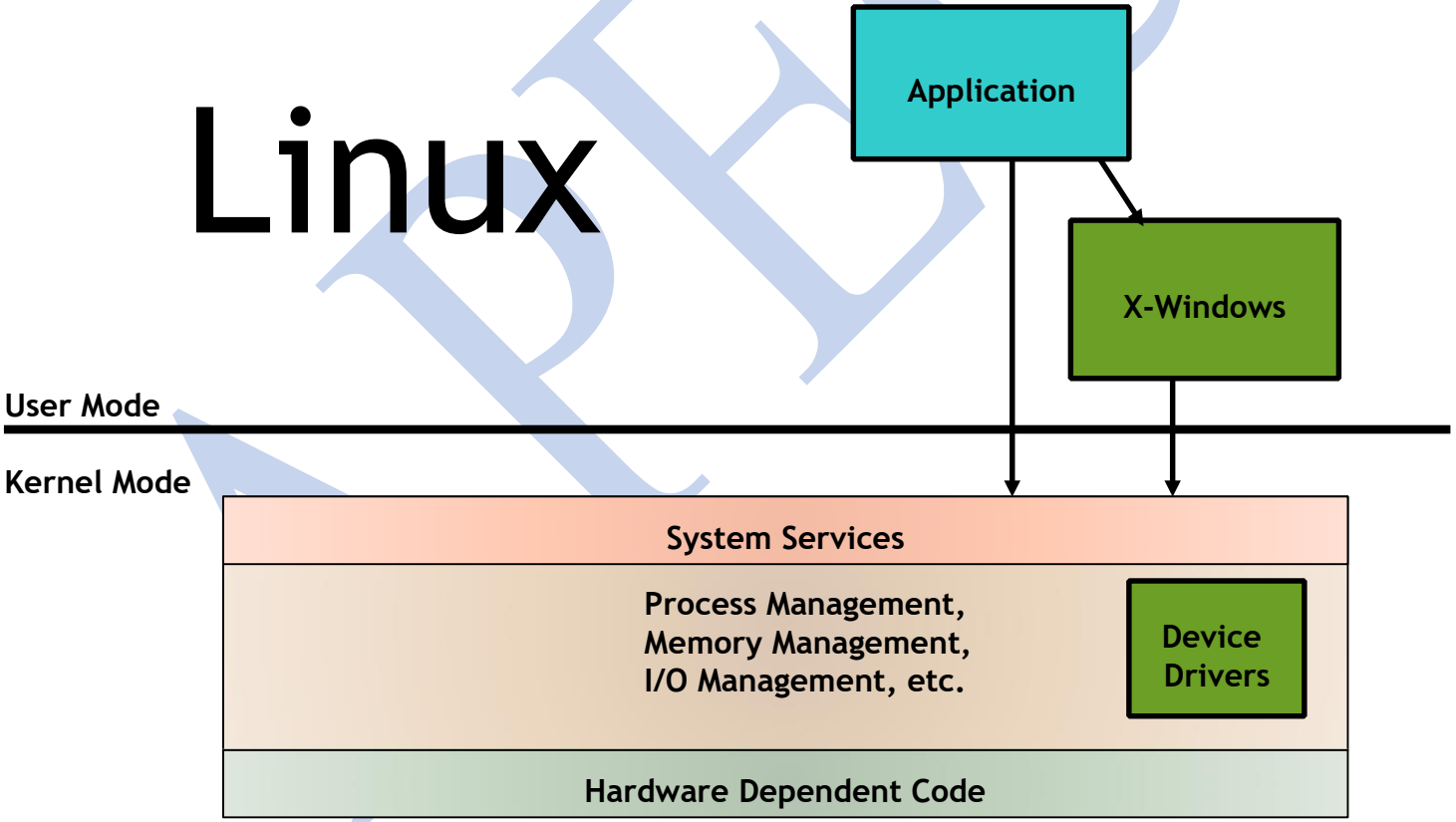
APEC

APEC

Kernel Architectures



Kernel Architectures



Linux Distributions

- Corel Linux
- Debian GNU/Linux
- OpenLinux (Caldera)
- Red Hat
- Slackware
- SuSE
- TurboLinux

Design principles

- Linux is a multiuser, multitasking operating system with a full set of UNIX compatible tools

APEC

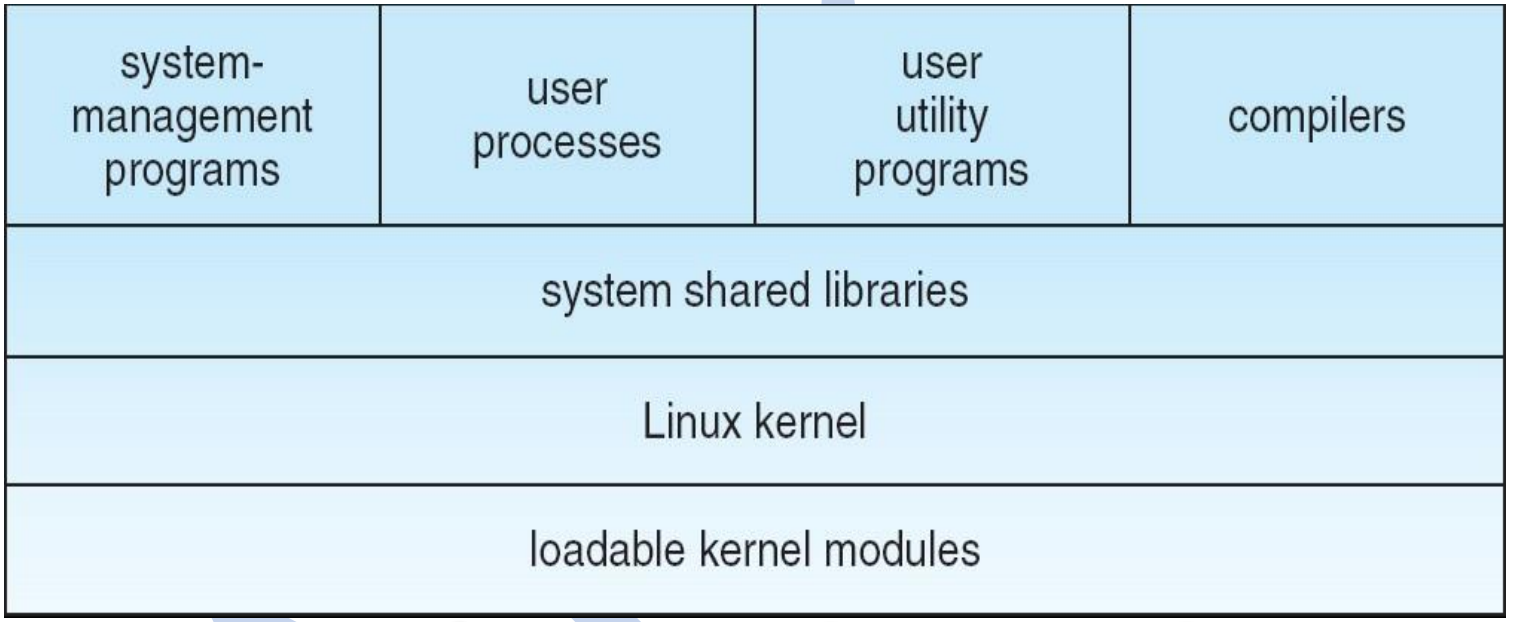
- Its file system adheres to traditional UNIX semantics, and it fully implements the standard UNIX networking model
- Main design goals are speed, efficiency, and standardization
- The Linux kernel is distributed under the GNU General Public License (GPL), as defined by the Free Software Foundation
- “Anyone using Linux, or creating their own derivative of Linux, may not make the derived product proprietary; software released under the GPL must include its source code”

AEC

System Administration

APEC

Components of a Linux System



Components of a Linux System (Cont)

- Linux is composed of three main bodies of code;

- The **kernel** is responsible for maintaining the important abstractions of the operating system
- Kernel code executes in *kernel mode*
- All kernel code are kept in the same single address space

- The **system libraries** define a standard set of functions through which applications interact with the kernel

- The **system utilities** perform individual specialized management tasks

APEC

Monolithic kernel

- Interfaces between different components are simple C calls
- Not messages or inter-process communication, as in micro-kernels

APEC

Kernel Modules

- Sections of kernel code that can be compiled, loaded, and unloaded independent of the rest of the kernel
- A kernel module may typically implement a device driver, a file system, or a networking protocol
- Kernel modules allow a Linux system to be set up with a standard, minimal kernel, without any extra device drivers built in

APEC

Components of module support

- Module management system:
  - allows modules to be loaded into memory and communicate with the rest of the kernel
- Module loader and unloader:
  - User mode utilities, work with the module management system to load and unload modules
- Driver registration system:
  - Allows the modules to tell the rest of the kernel that a new driver is available
- Conflict-resolution mechanisms:
  - Reserving hardware resources and protecting them from accidental use by another driver.

Module Management

- Supports loading modules into memory
- Module loading is split into two separate sections:
- Managing sections of module code in kernel memory
- Handling various modules that are allowed to reference

APEC

Driver Registration

- Allows modules to inform the kernel that a new driver has become available
- The kernel maintains dynamic tables of all known drivers, and provides a set of routines to allow drivers to be added to or removed from these tables at any time
- Registration tables include the following items:
- Device drivers
- File systems

APEC

- Network protocols
- Binary format

Conflict Resolution

- A mechanism that allows different device drivers to reserve hardware resources and to protect those resources from accidental use by another driver

- The conflict resolution module aims to:
- Resolve conflicts with multiple drivers trying to access the same hardware

APEC

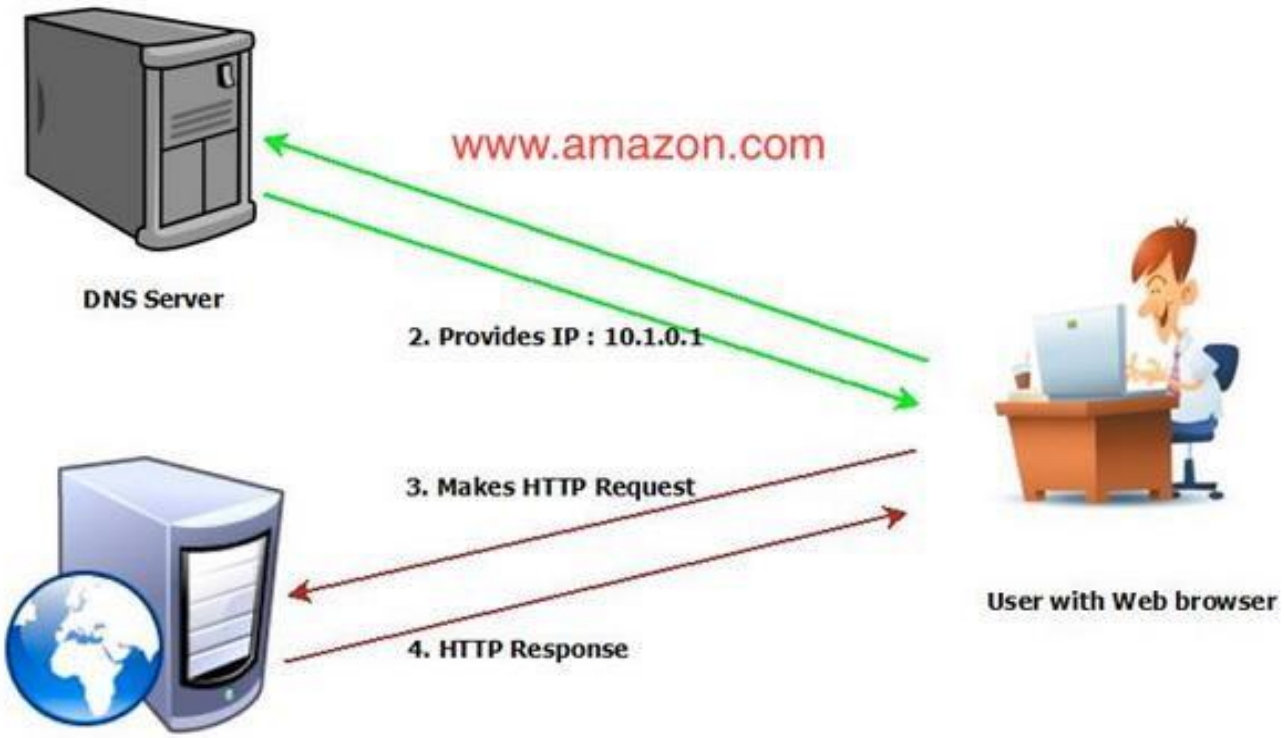
Domain Name System

APEC

Domain Name system

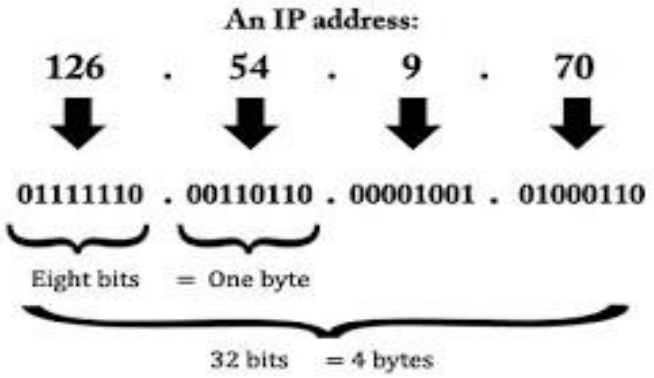
- DNS is a system for naming computers and network services that is organized into a hierarchy of domains.

APEC

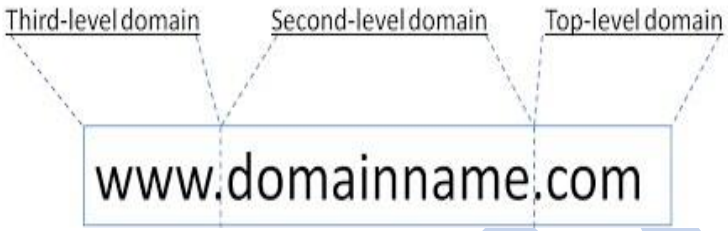

www.amazon.com
DNS Server
2. Provides IP : 10.1.0.1
3. Makes HTTP Request
4. HTTP Response
User with Web browser

DNS contd...

- IP Address: set of numbers separated by full stops that identifies each computer over the network.



- Domain Name:
- A domain name is the information that you enter into a web browser in order to reach a specific website.



DNS contd...

- Translating Domain Names into IP Addresses
  - DNS's job, then, is to take domain names and translate them into

- Translating Domain Names into IP Addresses

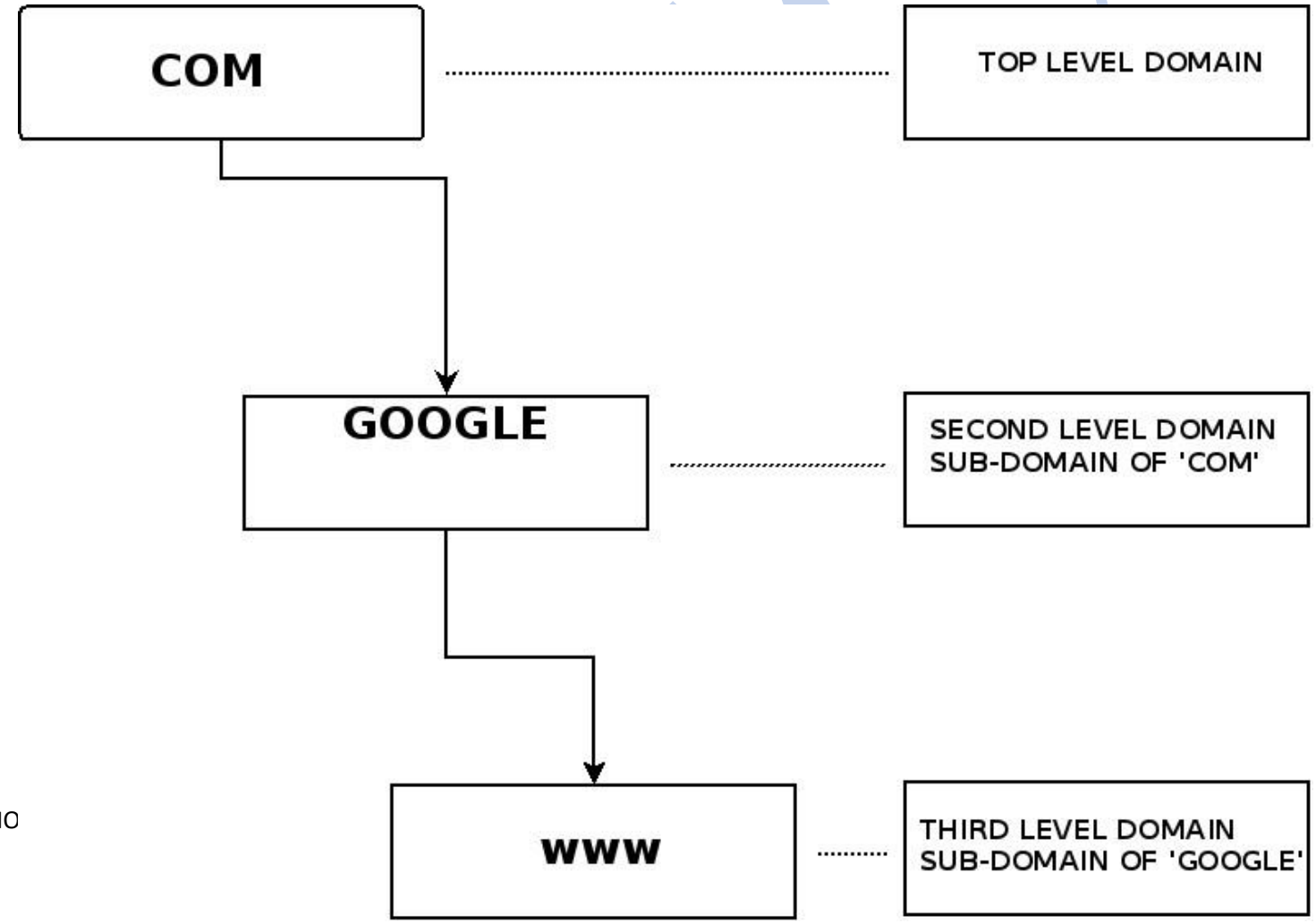
the IP addresses that allow machines to communicate with one another.

Human Readable Domain	Machine Readable IP Address
Hover.com	64.99.80.27
Yahoo.com	209.191.122.70
Microsoft.com	207.46.197.32
Apple.com	17.112.152.57
Dell.ca	143.166.83.38

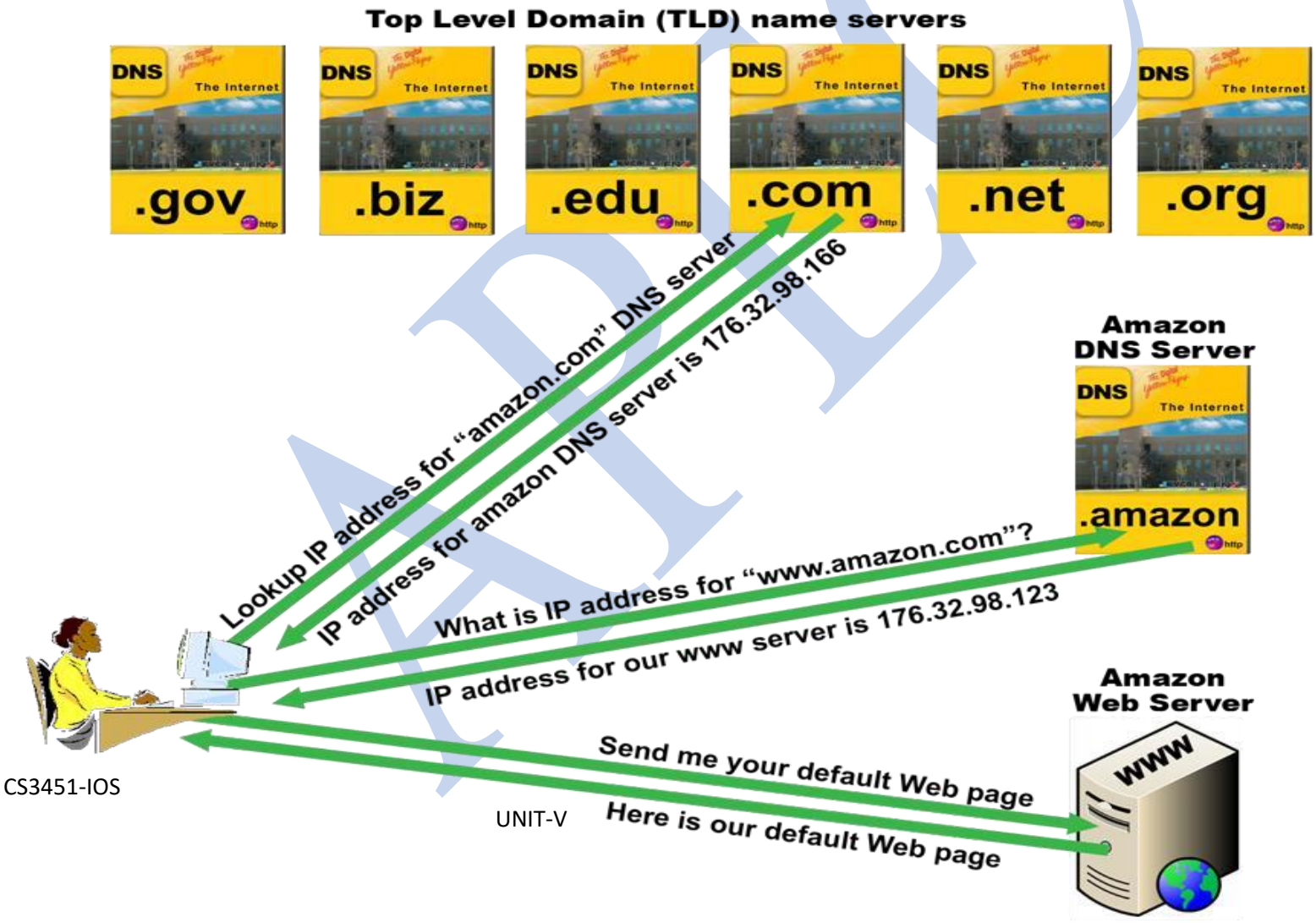


APL

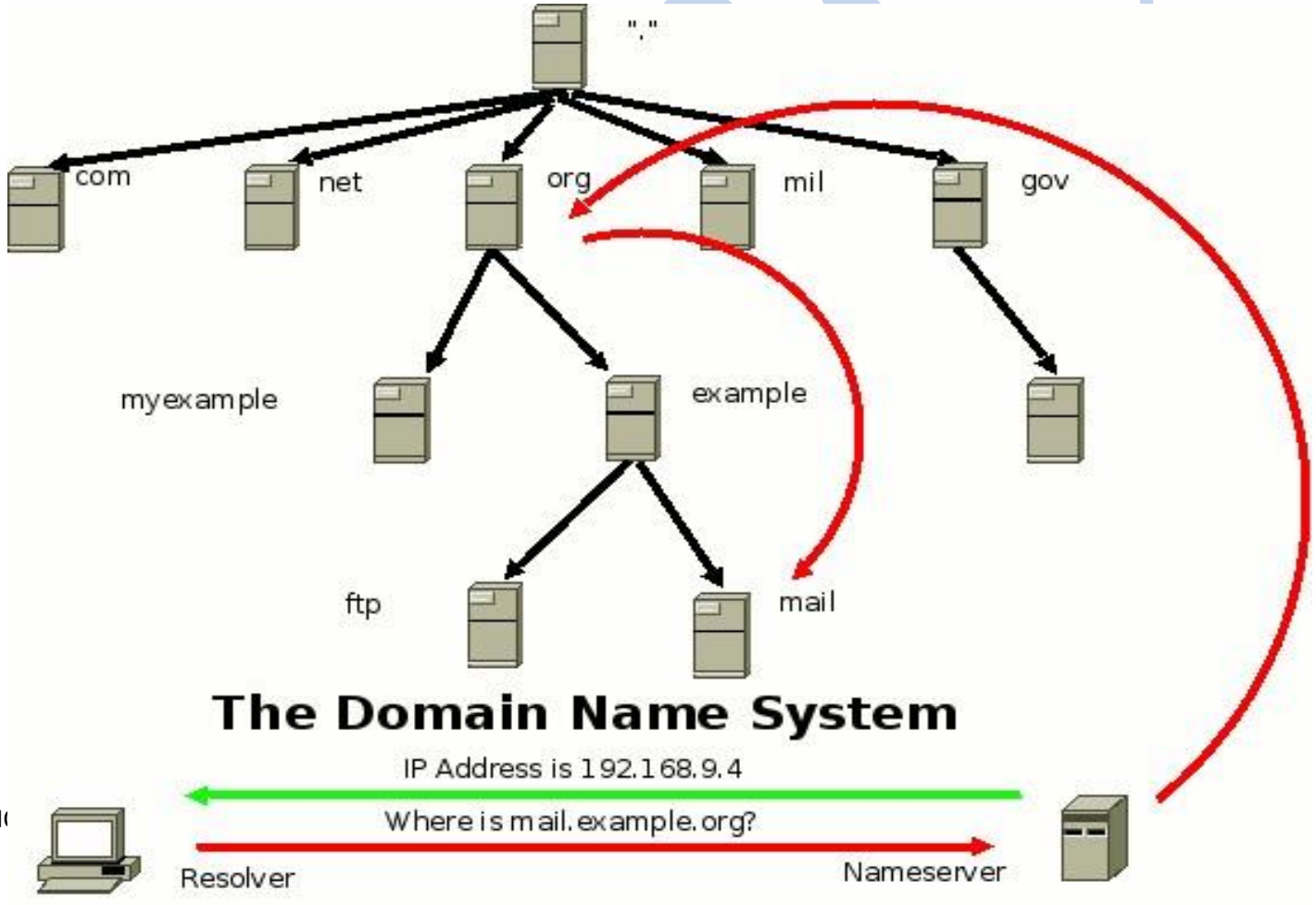
DNS contd...


COM
TOP LEVEL DOMAIN
GOOGLE
SECOND LEVEL DOMAIN
SUB-DOMAIN OF 'COM'
www
THIRD LEVEL DOMAIN
SUB-DOMAIN OF 'GOOGLE'

DNS contd...


Top Level Domain (TLD) name servers
DNS
The Internet
.gov
.biz
.edu
.com
.net
.org
Amazon
DNS Server
.amazon
Lookup IP address for "amazon.com" DNS server
IP address for amazon DNS server is 176.32.98.166
What is IP address for "www.amazon.com"?
IP address for our www server is 176.32.98.123
Amazon
Web Server
WWW
Send me your default Web page
Here is our default Web page

DNS contd...


"."
com
net
org
mil
gov
myexample
example
ftp
mail
The Domain Name System
IP Address is 192.168.9.4
Where is mail.example.org?
Resolver
Nameserver

Top level domain (TLD)

- There are only a limited number of such domains. For example:
- gov - Government agencies
- edu - Educational institutions
- org - Organizations (nonprofit)
- mil - Military
- com - commercial business
- net - Network organizations
- ca - Canada
- th - Thailand

APEC

Second Level domains for UK

- .co.uk – intended for UK-based businesses. It is the UK's most widely used second-level domain.
- .org.uk – intended for non-profit organizations.
- .me.uk – available only for personal use.
- .ltd.uk – available only for private limited companies in the UK.
- .plc.uk – available only for public limited companies in the UK.
- .net.uk – available only for Internet providers in the UK.
- .sch.uk – available only for schools in the UK.
- .ac.uk – intended for British academic institutions.
- .gov.uk – available for government agencies.
- .mod.uk and .mil.uk – available for the UK Armed Forces and Ministry of Defence.
- .nhs.uk – registration restricted to the National Health Service only.

- .police.uk – reserved for the UK police forces.

APEC

VIRTUALIZATION

APEC

Introduction to Virtualization

- **Virtualization** is a technology to run multiple operating systems on the same machine (ie. running both Linux & windows operating system on the same machine).

- Its possible with the HYPERVISOR.

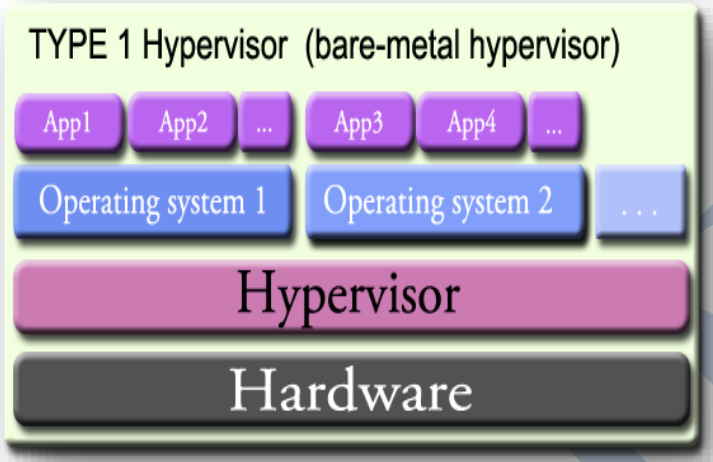
- How it's different from Dual Boot?
- Both operating systems run simultaneously.

HYPERVISOR

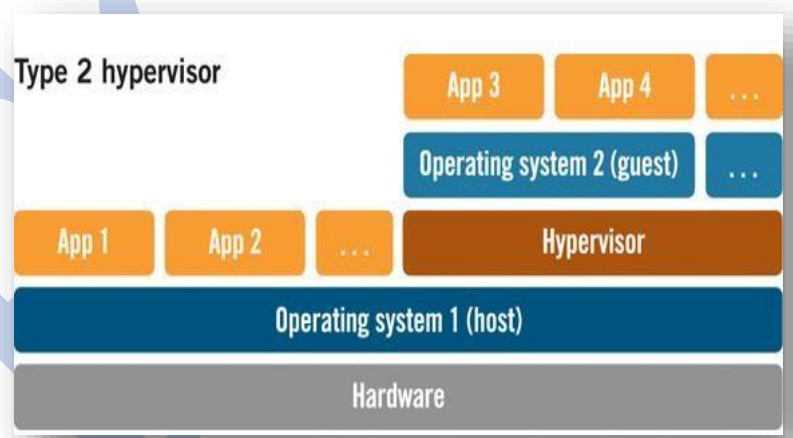
- A hypervisor, also called a **virtual machine manager**, is a program that allows multiple operating systems to share a host.
- Each operating system appears to have the host's processor, memory, and other resources all to itself.

APEC

Types of Hypervisor

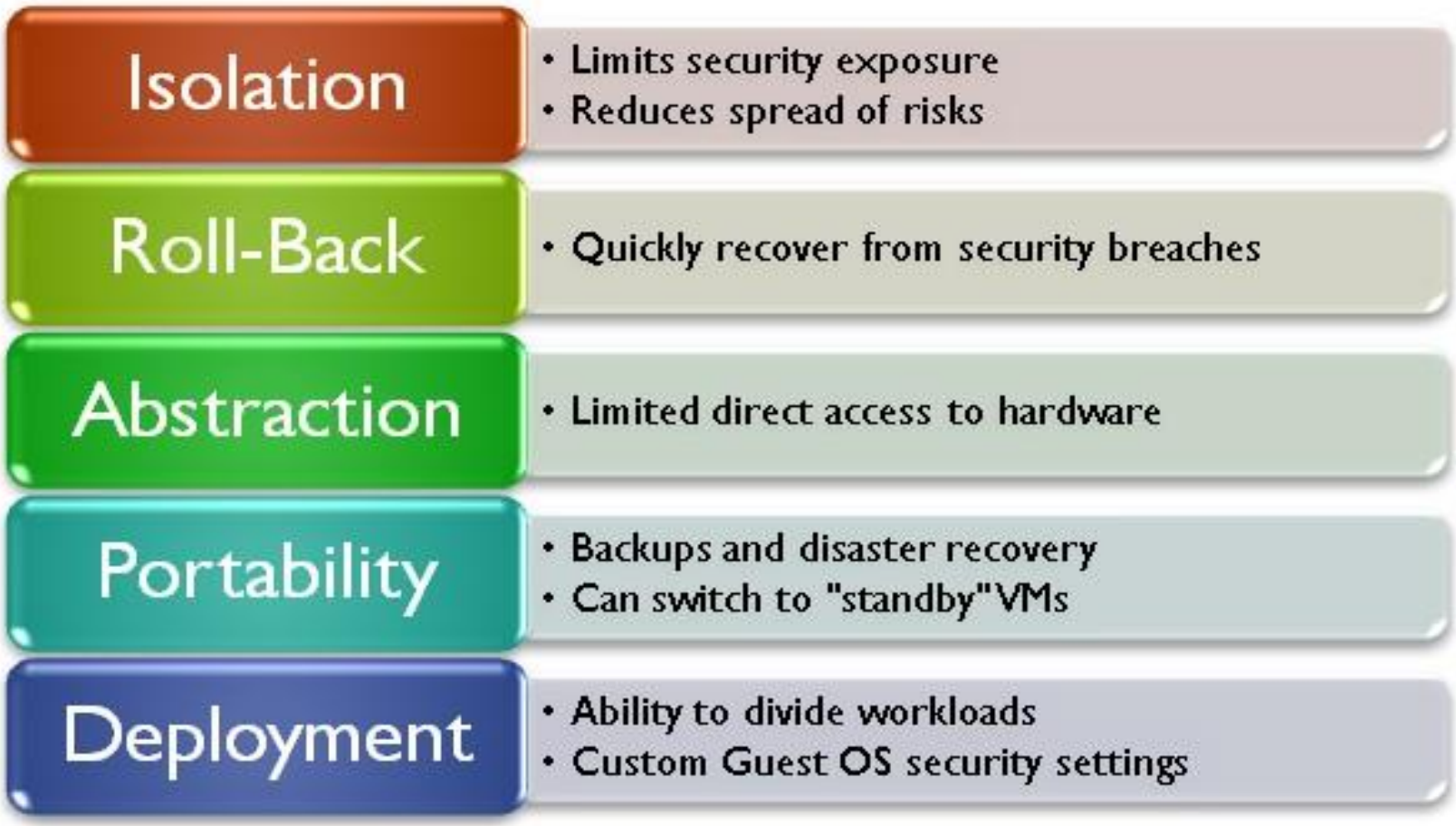


Type 1: Bare-Metal



Type 2: Hosted

Virtualization Benefits



Types of Virtualization

- Hardware Virtualization
- Dividing a part of hardware and sharing resources via virtual Machine.
- Desktop Virtualization
- Cloud computing & server virtualization
- Server Virtualization
- Virtualizing the servers
- Memory Virtualization
- Sharing virtual memory (RAM)
- Storage Virtualization
- Hard drive storage as virtual memory
- Data Virtualization
- Database Virtualization, which lies between storage application.
- Network Virtualization

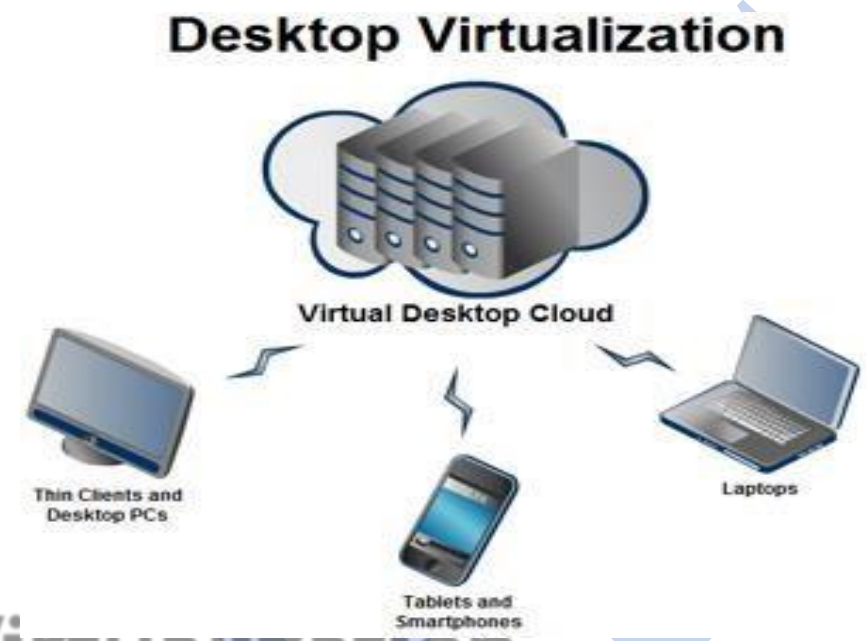
APEC

- Network Virtualization
- Creation of virtualized network addressing space.

Desktop Virtualization

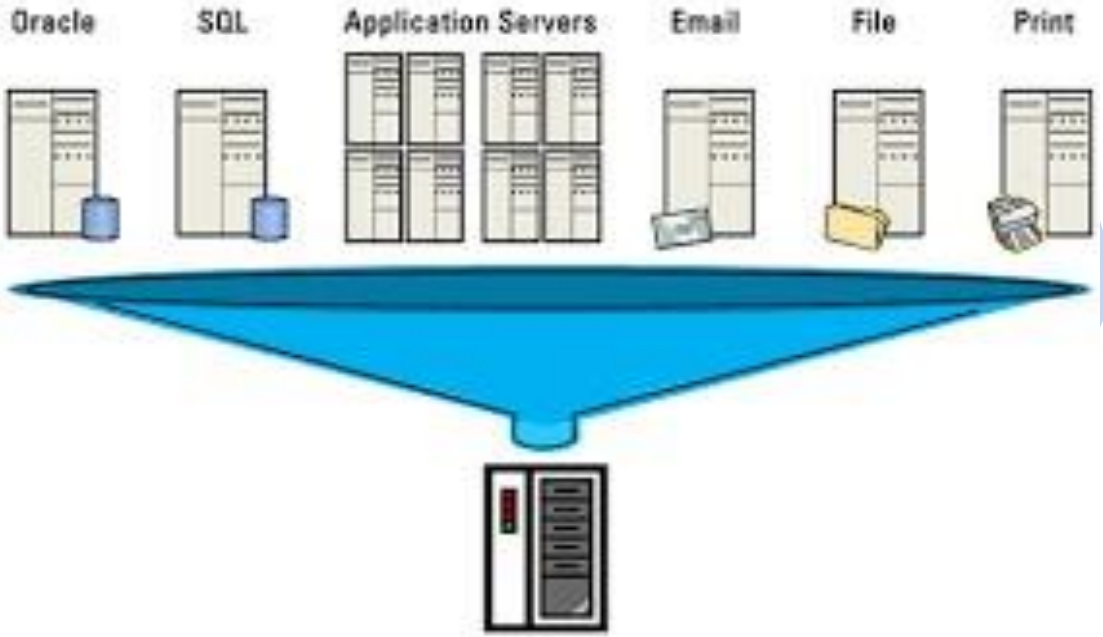
- Desktop virtualization is software technology that separates the desktop environment and associated application software from the physical client device that is used to access it.

APEC



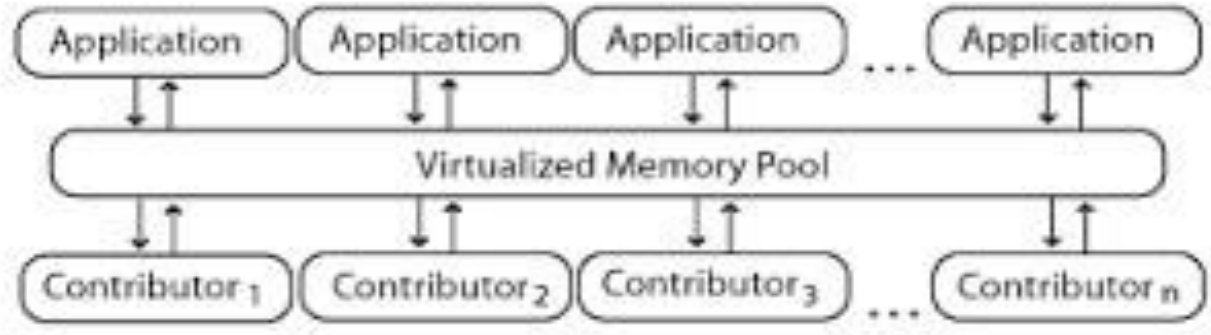
Server Virtualization

- **Server virtualization** is the masking of server resources, including the number and identity of individual physical servers, processors, and operating systems, from server users.



Memory Virtualization

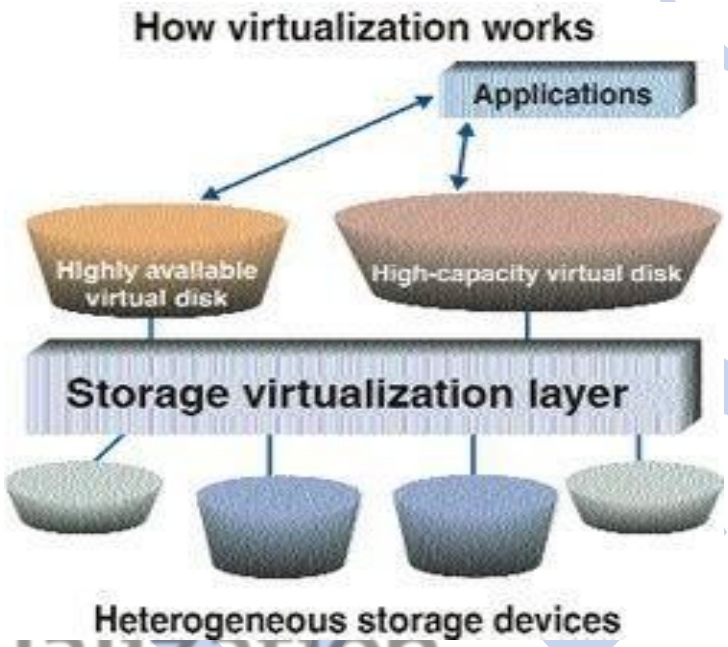
- **Memory virtualization** collects random access memory (RAM) resources from individual systems, and then sum those memory into a virtualized memory pool and give to different applications.



Memory Virtualization: Application Level Implementation

Storage virtualization

- **Storage virtualization** is the pooling of physical storage from multiple network storage devices so that it appears to be a single storage device that is managed from a central console.



Data virtualization

- **Data virtualization** is any approach to data management that allows an application to retrieve and manipulate data without requiring technical details about the data, such as how it is formatted or where it is physically located



Application virtualization

- A fully virtualized application is not installed in the traditional sense, although it is still executed as if it were.


Application virtualization
Applications
Operating System & Applications
Operating System & Applications

REQUIREMENTS FOR LINUX SYSTEM ADMINISTRATOR

APEC

The Linux System Administrator

- Installing & configuring servers
- Installing & configuring application software
- Creating & Maintaining user accounts
- Backing up & restoring files
- Monitoring & Tuning performance
- Configuring a secure system
- Using tools to monitor security

Installing & configuring servers

- Server → offers some type of service to clients.
- Services:

- Services:
- File or printer sharing
- File transfer protocol (FTP)
- Web access or email- processing tasks.

- Server is not a standalone workstation, but it's a computer that specifically performs these services for many users.
- Red Hat graphical user interface (GUI) requires a graphical layer called XFree86. This is a server. It runs even on a standalone machine with one user account. It must be configured.

- Likewise, printing in Linux takes place only after you configure a print server.

- In certain areas the client-server nomenclature can be confusing, though. While you cannot have a graphical desktop without an X server, you can have remote web access without running a local web server, remote FTP access without running a local FTP server, and email capabilities without ever starting a local mail server. You may well want to use these servers, all of which are included in Red Hat; then again maybe not. Whenever a server is connected to other machines outsider. You want your users to have easy access to the things they need, but you don't want to open up the system you're administering to the whole wide world.

Installing and Configuring Application Software

- Although it is possible for individual users to install some applications in their home directories—drive space set aside for their own files and customizations — these applications may not be available to other users with-out the intervention of the user who installed the program or the system administrator. Besides, if an application is to be used by more than one user, it probably needs to be installed higher up in the Linux file hierarchy, which is a job that only the system administrator can perform

- New software packages might be installed in /opt if they are likely to be upgraded separately from the Red Hat distribution itself. Doing this makes it simple to retain the old version until you are certain that the new version works and meets your expectations. Some packages may need to go in /usr / src or even usr if they are upgrades of packages installed as part of upgrades Red Hat. (For instance, there are sometimes security s of existing packages.) The location of the installation usually matters only if you compile the application from sourced code; if you use a Red Hat Package Manager (RPM) application package, it automatically goes where it should.

- Configuration and customization ac age of applications is to some extent at the user's discretion, but not entirely, "Skeleton" configurations — administrator-determined default configurations — set the baseline for user employment of applications. If there are particular forms, for example, that is used through. out an enterprise, the system administrator would set them up or at least make them available by adding them to the skeleton configuration. The same applies to configuring user desktops and in even deciding what applications should appear on user desktop menus. For instance, your company may not want to grant users access to the games that ship with modern Linux desktops. You may also want to add menu items for newly installed or custom applications. The system administrator brings all this to pass.

Creating & Maintaining user accounts

- Not just anyone can show up and log on to a Linux machine. An account must be created for each user and—you guessed it—no one but the system administrator can do this. That's simple enough. But there's more. It involves decisions that either you or your company must make. You might want to let users select their own passwords, which would no doubt make them easier to remember but which probably would be easier for a malefactor to crack. You might want to assign passwords, which is more secure in

theory but increases the likelihood that users will write them down on a conveniently located scrap of paper — a risk if many people have access to the area where the machine(s) is located.

- You might decide that users must change their passwords periodically — something you can configure Red Hat Enterprise Linux to prompt users about.
- What happens to old accounts? Suppose that someone leaves the company. You probably don't want that person to gain access to the company's network, but you also don't want to delete the account wholesale, only to discover later that essential data resided nowhere else.
- To what may specific users have access? It might be that there are aspects of your business that make Web access desirable, but you don't want everyone spending their working hours surfing the Web. If your system is at home, you may wish to limit your children's access to certain Web sites.
- These and other issues are part of the system administrator's duties in man- aging user accounts. Whether the administrator or his or her employer establishes policies governing accounts, these policies should be delineated—preferably in writing for a company — for the protection of all concerned.

Backing Up and Restoring Files

- Until computer equipment becomes infallible, until people lose the desire to harm others' property, and — truth be told — until system administrators become perfect, there is considerable need to back up important files so that the system can be u and running again with minimal disruption in the event of hardware, security, or administration failure. Only the system administrator may do this. (Because of its built-in security features, Linux doesn't allow even user to back up their own to removable disks.)
- It's not enough to know that performing backups is your job. You need to formulate a strategy for making sure your system is not vulnerable to catastrophic disruption. This is not always obvious. If you have a high-capacity tape drive and several good sets of restore disks, you might make a full system backup every few days. If you are managing a system with scores of users, you might find it more sensible to back up user accounts and system configuration files, figuring that reinstallation from the distribution CDs would be quicker and easier than getting the basics off a tape archive. (Don't forget about applications you install separately from your Red Hat distribution, especially those involving heavy customization.)

- Once you decide what to back up, you need to decide how frequently to perform backups, whether to maintain a series of incremental backups – adding only files that have changed since the last backup- or multiple full backups, and when these backups should be performed. Do you trust an automated, unattended process? If you help determine which equipment to use, do you go with a redundant array of independent disks (RAID), which is to say multiple hard drives all containing the same data as insurance against the failure of any one of them, in addition to other backup system? (A RAID is not enough because hard drive failure is not the only means by which a system can be brought to a halt.)

- You don't want to become complacent or foster a lackadaisical attitude among users. Part of your strategy should be to maintain perfect backups without ever needing to resort to them. This means encouraging users to keep multiple copies of their important files in their important files in their home directories so that you won't be asked to mount a backup to restore a file that a user corrupted. (If your system is a standalone on then, as your won system administrator, you should make a habit of backing up your configuration and other important files.)

- Restoring files from your backup media is no less important than backing them up in the first place. Be certain you can restore your files if the need arises by testing your restore process at least once during a noncritical time. Periodically testing your backup media is also good idea.

- Chances are good that even if you work for a company, you'll be the one making these decisions. Your boss just wants a system that runs perfectly, all the time. Backing up is only part of the story, however. You need to formulate a plan for bringing the system back up after a failure. A system failure could be caused by any number of problems, either related to hardware of software (application, system configuration) trouble, and could range from a minor inconvenience to complete shutdown.

- Hardware failures caused by improper configuration can be corrected by properly configuring the device. Sometimes hardware failures are caused by the device itself, which typically requires replacing the device. Software failures caused by improperly configured system files are usually corrected by properly configuring those files. An application can cause the system to fail for many reasons, and finding the root of the problem may require a lot of research on the part of the administrator.

- If you are the administrator of servers and workstations for a business, you should have a disaster recovery plan in place. Such a plan takes into account the type of data and services provided and how much fault tolerance your systems require, that is, how long your systems could be down and what effect that would have on your company's ability to conduct business. If you require 100 percent fault tolerance, meaning your systems must be online 24/7, disaster recovery may be unnecessary in some circumstances as your systems never go down and there is no disaster from which to recover. Most organizations, though, cannot afford such a high level of fault tolerance; they are willing to accept less stringent standards.

- Based on the level of fault tolerance you require, Your disaster recovery plan should list as many possible failures as You can anticipate and detail the steps required to restore your systems.

- TIP Backing up is only part of the story. You need to formulate a disaster recovery plan to bring your system back up in the event of a failure.

Monitoring and Tuning Performance

- The default installation of Red Hat Enterprise Linux goes a long way toward capitalizing on existing system resources. There is no “one size fits all” configuration, however. Linux is infinitely configurable, or close to it.
- On a modern standalone system, Linux runs pretty quickly. If it doesn’t, there’s something wrong — something the system administrator can fix. Still, you might want to squeeze one last little bit of performance out of your hardware — or a number of people might be using the same file server, mail server, or other shared machine, in which case seemingly small improvements in system performance add up.
- System tuning is an ongoing process aided by a variety of diagnostic and monitoring tools. Some performance decisions are made at installation time, while others are added or tweaked later. A good example is the use of the hdparm utility, which can increase throughput in IDE drives considerably, but for some high-speed modes a check of system logs shows that faulty or inexpensive cables cam in combination with hdparm, produce an enormity of non-destructive but system-slowing errors.
- Proper monitoring allows you to detect a misbehaving application that consumes more resources than it should or fails to exit completely upon closing. Through the use of system performance tools, you can determine when hard-ware such as memory, added storage, or even something as elaborate as a hardware RAID — should be upgraded for more cost-effective use of a machine in the enterprise or for complicated computational tasks such as three dimensional rendering.
- Possibly most important, careful system monitoring and diagnostic practices give you a heads up when a system component is showing early signs of failure, so that you can minimize any potential downtime. Combined with the resources for determining which components are best supported by Fedora Core and Red Hat Enterprise Linux, performance monitoring can result in replacement components that are far more robust and efficient in some cases.
- In any case, careful system monitoring plus wise use of the built-in configurability of Linux allows you to squeeze the best possible performance from your existing equipment, from customizing video drivers to applying special kernel patches or simply turning off unneeded services to free memory and processor cycles.

- TIP:To squeeze the best performance from your equipment, monitor your system carefully and use Linux's built-in configurability wisely.

Configuring a Secure System

- If there is a common thread in Linux system administration, it is the security of the computer and data integrity.
- What does this mean? Just about everything. The system administrator's task, first and foremost, is to make certain that no data on the machine or network is likely to become corrupted, whether by hardware or power failure, mis-configuration or user error (to the extent that the latter can be avoided), or malicious or inadvertent intrusion from elsewhere. This means doing all the tasks described throughout this chapter, and doing them well, with a full understanding of their implications.
- No one involved in computing has failed to hear of the succession of increasingly serious attacks on machines connected to the Internet. For the most part, these attacks have not targeted Linux systems. That doesn't mean Linux systems have been entirely immune, either to direct attack or to the effects of attacks on machines running other operating systems. In one distributed denial of service (DDoS) attack aimed at several major online companies,
- For instance, many "zombie" machines — those that had been exploited so that the vandals could employ thousands of machines instead of just a few —were *running Linux that had not been patched to guard against a well-known security flaw. In the various Code Red attacks during the summer of 2001, Linux machines themselves were invulnerable, but the huge amount of traffic generated by this worm infection nevertheless prevented many Linux machines from accomplishing much Web-based work for several weeks, so fierce was the storm raging across the Internet. And few email users have been immune from receiving at least some Sir Cam messages — nonsensical messages from strangers with randomly selected files attached from their machines. While this infection did not corrupt Linux machines per se, as it did those running MS Windows, anyone on a dial-up Internet connection who had to endure downloading several megabytes of infected mail each day would scarcely describe himself or herself as unaffected by the attack.
- Depending on how a Linux machine is connected, and to what; the sensitivity of the data it contains; and the uses to which it is put, security can be as simple as turning off unneeded services, monitoring the Red Hat security mailing list to make sure that all security advisories are followed, regularly using system utilities to keep the system up to date, and otherwise engaging in good computing practices to make sure that the system runs robustly. It's almost a full-time job, involving levels of security permissions within the system and systems to which it is connected; elaborate firewalls to protect not just Linux machines but machines that, through their use of nonLinux software, are far more vulnerable; and physical security — making sure that no one steals the machine itself!
- For any machine connected to another machine, security means hardening against attacks and making certain that no one else uses your machine as a platform for launching attacks against others. If you run Web, FTP, or mail servers, it means giving access to only those who are entitled to it, while locking out everyone else. It means making sure that passwords are not easily guessed and not made available to unauthorized persons. It means that disgruntled former employees no longer have access to the system and that no reauthorized person may copy files from your machines.
- Security is an ongoing process. The only really secure computer is one that contains no data, is unplugged from networks and power supplies, has no keyboard attached, and resides in a locked vault. While this is theoretically true, it implies that security diminishes the usefulness of the machine.
- In the chapters that follow, you learn about the many tools that Red Hat pro-ides to help you guard against intrusion, even to help you prevent intrusion do non-Linux machines that may reside on your network. Linux is designed om the beginning with security in mind. In all your tasks you should main-in that same security awareness.

- TIP: Your job as system administrator is to strike the right balance between maximum utility and maximum safety, all the while bearing in mind that confidence in a secure machine nothing about the machine's security tomorrow.

Using Tools to Monitor Security

- People who, for purposes of larceny or to amuse themselves, like to break into computers – they're called crackers – are a clever bunch. If there is vulnerability in a system, they will find it.

- Fortunately, the Linux development community is quick to find potential exploits and to crate ways of slamming the door shut before crackers can enter. Fortunately, too, Red Hat is diligent in making available new, patched versions of packages in which potential exploits have been found. Your first and best security tool, therefore, is making sure that whenever a security advisory is issued, you download and install the repaired package. This line of defense can be annoying but it is nothing compared to rebuilding a compromised system.

- As good as the bug trackers are, sometimes their job is reactive. Preventing the use of your machine for nefarious purpose and guarding against intrusion are, in the end, your responsibility alone. Red Hat equips you with tools to detect and deal with unauthorized access of many kinds.

- As this book unfolds, you'll learn how to install and configure these tools and how to make sense of the warnings they provide. Pay careful attention to those sections and do what they say. If your machine is connected to the Internet, you will be amazed at the number

of attempts made to break into your machine. You'll be struck by how critical the issue of security is.

APEC