Mount Kenya University

SCHOOL OF PURE AND APLIED SCIENCES

DEPARTMENT OF INFORMATION TECHNOLOGY

UNIT CODE: BIT 2103

UNIT NAME: HARDWARE AND SOFTWARE INSTALLATION AND SUPPORT

Table of Contents

Purpose v

Objectives v

Course Content v

Required text books vii

Text books for further reading vii

Basic introduction 1

Chapter 1: Installation of operating systems 2

1.1 System Requirements 4

1.2 Preparation of hard disk 5

1.2.1 Types of hard disks 5

1.2.2 Installing operating system on hard disk 6

1.3 Disc start up 8

1.4 Installation of software in the network 9

1.5 Safety procedures .... **Error! Bookmark not defined.**

Chapter 2: Installation and customization of various hardware devices 11

2.1 Installation 11

2.1.1 Power requirements 11

2.1.2 Types of cables 15

2.1.3 Types of connectors and Ports 19

2.1.2 Devices driver 29

2.1.3 Disk partitioning 33

2.1.4 Formatting 34

2.1.5 Disk space 35

2.1.6 Memory capacity 35

2.1.7 Processor speed check 38

2.2 Software customization; 39

2.2.1 Task bar, ... 39

2.2.2 Startup menu, ... 40

2.2.3 Desktop, ... 40

2.2.4 Screen saver, ... 41

2.2.5 Fonts &color, ... 41

2.2.6 Creating shortcuts to program groups 42
2.3 System maintenance; 44
2.3.1 back up restoration, ... 44
2.3.2 Use of hardware diagnostic tools in system software, ... 50
2.4 Antivirus; 53
2.5 diagnostic tools; 55
2.6 Resolving hardware conflicts 57
Chapter 3: Configuration Management: 60
3.1 Basic concepts of configuration management. 60
3.2 The configuration management database (CMDB) 63
Chapter 4: IT Change Management 65
4.1 Introduction to change management 65
4.2 Possible problems 66
4.3 roles and responsibilities, ... 67
4.4 change management procedures 67
4.5 Scope of Change Management 68
4.6 Review and audit 68
Chapter 5: The Help desk 72
5.1 The role of the help desk, ... 72
5.2 Value added functions of the help desk, ... 74
Incident Management 74
Information Centre 74
Supplier relations 75
5.3 Factors influencing help desk design, ... 75
Logical structure 75
Physical structure 76
5.4 Staffing of the help desk 79
Chapter 6: Incident and Problem Management: 81
6.1 The Incident Management Process, ... 81
Logging 87
Classification 87
6.2 First line incident support, ... 92

6.3 Problem control and prevention 92

1. Identification and Logging 93

2. Classification and Allocation of Resources. 94

3. Analysis and Diagnosis: Known error 95

Chapter 7: Service Delivery: 96

7.1 Service Level Management, ... 96

Basic Concepts 96

Service Catalogue 96

Service Level Requirements (SLR) 96

Specification Sheets 97

Service Quality Programme (SQP) 97

Service Level Agreement (SLA) 97

Operation Level Agreement (OLA) 98

Underpinning Contract (UC) 98

Service Improvement Programme (SIP) 98

7.2 Service Capacity Management, ... 98

Introduction and Objectives 98

7.3 Loss of IT service, ... 100

7.4 Risk analysis and management, ... 100

7.5 IT recovery options, ... 101

7.6 Recovery of failed systems 102

7.7 Release management 102

7.7.1 Planning 104

7.7.2 Development 105

7.7.3 Validation 106

7.7.4 Implementation 106

7.7.5 Communication and Training 107

References 110

BST 2101: HARDWARE AND SOFTWARE INSTALLATION AND SUPPORT

Purpose: To introduce the learner to the basics of IT service support and computer installation and customization procedures

Objectives

By the end of the course unit, a learner should:

i. Install operating system

ii. Install various computer hardware devices

iii. Customize the computer software

iv. Maintain the computer

v. Manage a help desk

Course Content;

WEEK 1

Installation of operating systems: system requirements, preparation of hard disk, disc. Start up

WEEK 2

Installation of software in the network, Safety procedures

Installation and customization of various hardware devices: power requirements

WEEK 3

Types of cables, connectors, ports, devices driver, disk partitioning, formatting, disk space, memory capacity, and processor speed check.

WEEK 4

Software customization; task bar, startup menu, desktop, screen saver, fonts, color, creating shortcuts to program groups

WEEK 5

System maintenance; back up, restoration, use of hardware diagnostic tools in system software, scandisk, restoration,

WEEK 6

Use of hardware diagnostic tools in system software, scandisk, defragmentation, Antivirus; diagnostic tools; Resolving hardware conflicts

WEEK 7

Configuration Management: Basic concepts of configuration management. The configuration management database (CMDB)

WEEK 8

Registration of configuration items, benefits to IT service management, and the configuration manager

WEEK 9

IT Change Management: introduction to change management, possible problems, roles and responsibilities, change management procedures, review and audit.

WEEK 10

The help desk: The role of the help desk, value added functions of the help desk, data recording and usage, factors influencing help desk design, types and features of help desks, staffing of the help desk.

WEEK11

Incident and Problem Management: The Incident Management Process

WEEK 12

Problem control and prevention, Service Level Management, Service Capacity Management, Loss of IT service

WEEK 13

Service Capacity Management, Loss of IT service,

Risk analysis and management, IT recovery options, Recovery of failed systems, Release Management.

Course Assessment

Examination	- 70%
Continuous Assessment Test (CATS)	- 20%
Assignments	- 10%
Total	- 100%

Required text books

Andrews J, (2009), A+ Guide to Software: Managing, Maintaining, and Troubleshooting

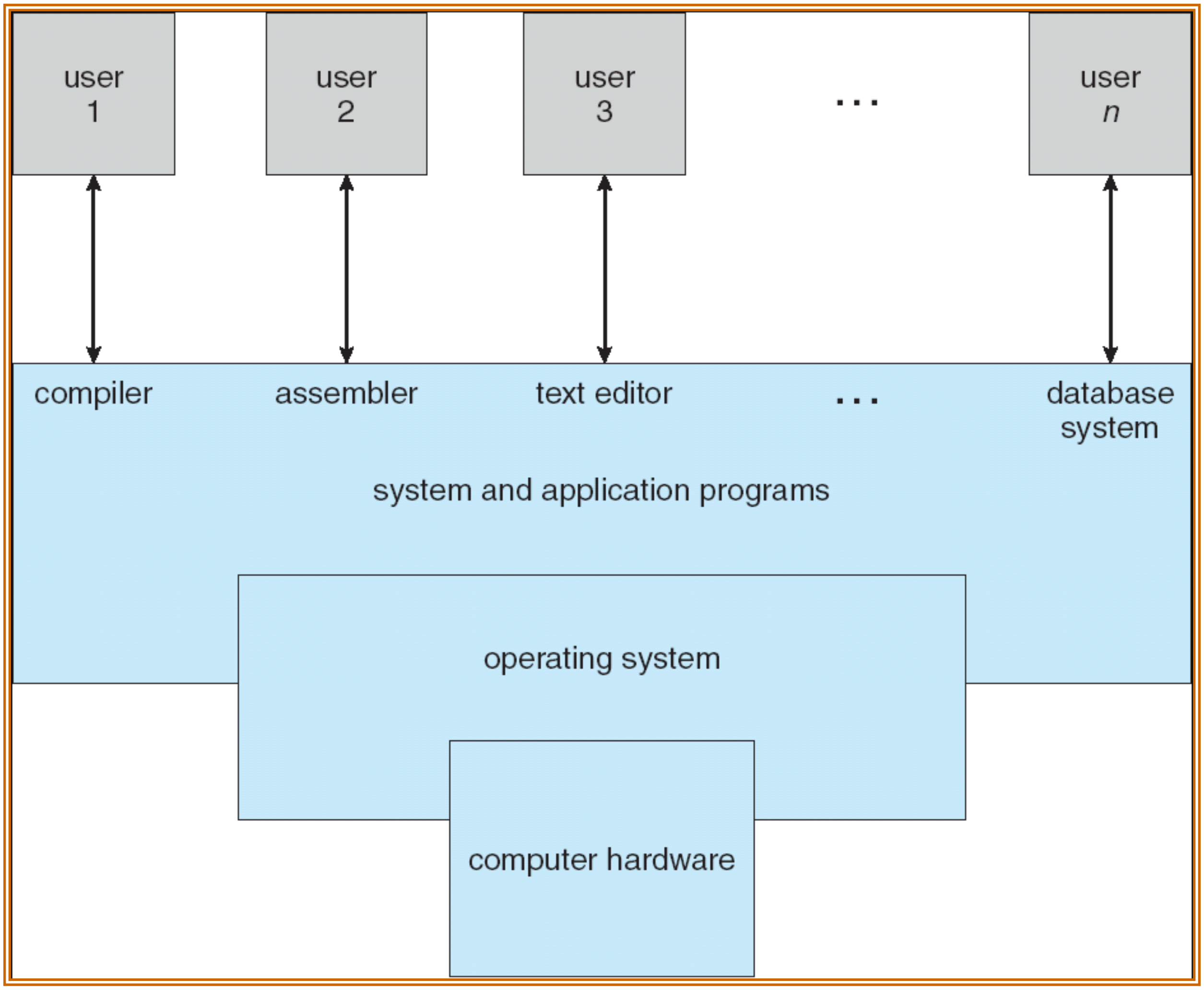
Text books for further reading

Chambers L,(2009) Build Your Own PC Do-It-Yourself For Dummies

Basic introduction:

The computer system can be divided roughly into four components:

1. The hardware
2. The operating system
3. The application software
4. The Users



Chapter 1: Installation of operating systems

***Chapter Learning Objectives:** By the end of this chapter you should appreciate how to install operating systems as well as their various system requirements, preparation of hard disk, disc Start up, Installation of software in the network and Safety procedures to be followed while dealing with various operating systems*

An **operating system (OS)** provides basic programming instructions to the computer hardware. The operating system is program code that makes it possible for you to start the basic functions of a computer, view text on the computer's display, store information, access and modify information, log on to a network, connect to the Internet, and run software applications. An operating system is ideal for providing security because it takes care of the computer's most basic **input/output (I/O)** functions, which enable other programs to easily talk to the computer hardware, and permit the computer user to access a network. It is the task of I/O functions to take requests from the software the user runs and translate them into requests that the hardware can understand and carry out.

WHAT AN OPERATING SYSTEM DOES

Although there are important differences among them, all operating systems share the following four main functions:

Function 1. Provide a user interface

- Performing housekeeping procedures requested by the user, often concerning secondary storage devices, such as reorganizing a hard drive, deleting files, copying files, and changing the system date
- Providing a way for the user to manage the desktop, hardware, applications, and data

Function 2. Manage files

- Managing files on hard drives, DVD drives, CD drives, floppy drives, and other drives
- Creating, storing, retrieving, deleting, and moving files

Function 3. Manage hardware

- Managing the BIOS (programs permanently stored on hardware devices)

- Managing memory, which is a temporary place to store data and instructions as they are being processed
- Diagnosing problems with software and hardware
- Interfacing between hardware and software (that is, interpreting application software needs to the hardware and interpreting hardware needs to application software)

Function 4. Manage applications

- Installing and uninstalling applications
- Running applications and managing the interface to the hardware on behalf of an application

An operating system contains the following basic components:

- The **application programming interface (API)**, software that resides between the application software and the operating system kernel, which is the main program code in the operating system. The API translates requests from the application into code that the kernel can understand and pass on to the hardware device drivers. The API also translates information from the kernel and device drivers so the application can use it. Another function of the API is to provide an interface to the basic input/output system (BIOS).
- The **basic input/output system (BIOS)** , a program that verifies hardware and establishes basic communications with components such as the monitor and disk drives. The BIOS usually loads other operating system components on startup and houses a real-time clock for the date and time.
- The operating system **kernel**, the core of the operating system that coordinates operating system functions, such as control of memory and storage. The kernel communicates with the BIOS, device drivers, and the API to perform these functions. It also interfaces with the resource managers.
- **Resource managers**, programs that manage computer memory and central processor use.
- **Device driver**, programs that take requests from the API via the kernel and translate them into commands to manipulate specific hardware devices, such as keyboards, monitors, disk drives, and printers. The OS also includes optional specialized drivers for other functions and devices, such as sound.

1.1 System Requirements

Every operating system requires its own set of system requirements depending on the particular functionalities of the operating system. In most cases contemporary operating systems require greater system requirements compared to their predecessors. For example,

Windows 8

- Processor: 1 gigahertz (GHz) or faster with support for PAE, NX, and SSE2
- RAM: 1 gigabyte (GB) (32-bit) or 2 GB (64-bit)
- Hard disk space: 16 GB (32-bit) or 20 GB (64-bit)
- Graphics card: Microsoft DirectX 9 graphics device with WDDM driver

Question: - What is PAE, NX, and SSE2 and why does your pc need them in order to support windows 8?

Windows Vista Home Basic

- 1 GHz 32-bit (x86) or 64-bit (x64) processor
- 512 MB of system memory
- 20 GB hard drive with at least 15 GB of available space
- Support for DirectX 9 graphics and 32 MB of graphics memory
- DVD-ROM drive
- Audio Output

MAC OS X 9.5

- Mac computer with an Intel, PowerPC G5, or PowerPC G4 (867MHz or faster) processor
- 512MB of memory
- DVD drive for installation
- 9GB of available disk space

1.2 Preparation of hard disk

1.2.1 Types of hard disks

Hard drive can either be IDE or SATA. As far as Windows is concerned, both types of hard drive are identical, but their *physical* installation needs differ. If you are planning on installing an additional hard drive, you need to know which type you have before continuing.

The simplest and most reliable way to determine whether a hard drive is a Serial ATA or Parallel ATA device is look at the back of the unit where the connections are. A parallel ATA, or IDE drive (still the most common variety) will look like the drive immediately below. Note the 40-pin parallel ATA connector, jumpers, and 4-pin molex power socket. The drive is 3.5" wide, and a little less than 1" thick.

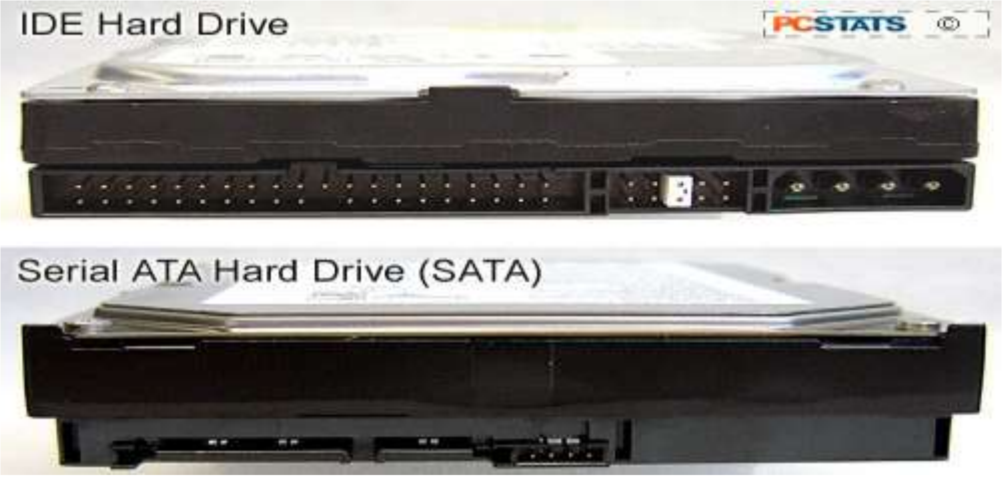


FIG 1.2.1 a

Serial ATA hard drives are physically the same shape and size, and differ only in the type of electrical connectors they require to interface with the motherboard. A Serial ATA drive is pictured directly above. Note the small, flat, keyed power and Serial ATA connectors. Some serial ATA drives also have a 4-pin molex power socket as IDE drive pictured above, so yours may look slightly different from the Seagate SATA drive pictured above.

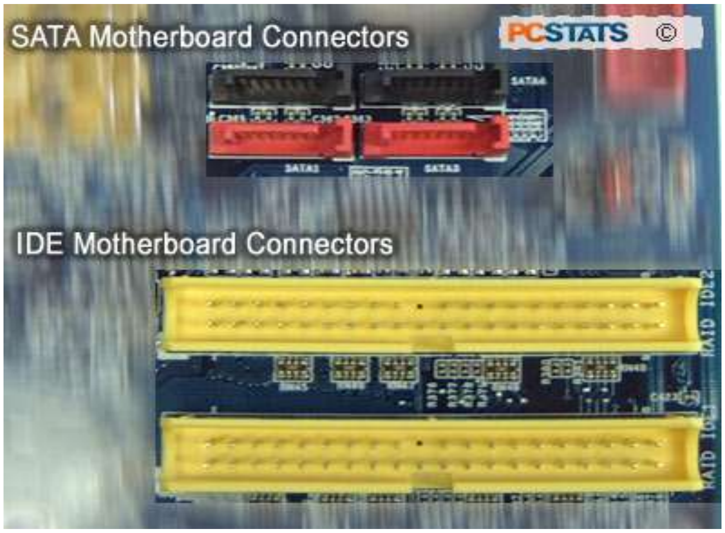


FIG 1.2.1 b

Recently purchased computer motherboards should have both serial ATA and IDE connectors on board, but older boards will have only IDE connectors. Once you have verified which type of hard disk you are using, the next step is to power off your computer and open it up to ensure that you have the necessary connectors free for the new hard drive.

Each SATA port can support a single SATA drive, while each IDE connector can support two IDE hard drives or optical drives (technically, this means a total of two IDE devices per channel). IDE data cables have three connectors; one connects to the motherboard and the other two attaching to the drives.

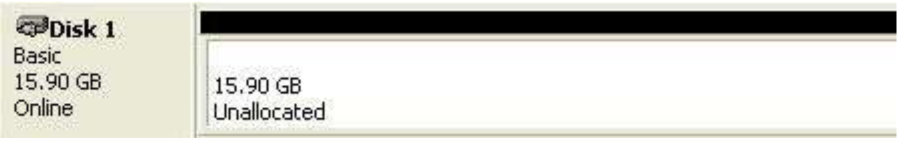
1.2.2 Installing operating system on hard disk

Installing Windows 2000/XP on a new IDE drive

To install Windows 2000/XP on your IDE hard drive, insert the installation CD into your CD/DVD drive and reboot the computer. You should get the option to 'press any key to boot from CD.' If you do not see this, you may have to go into the BIOS setup (by pressing the 'del' key upon rebooting) and make sure that your CD is selected as a boot device. This option is generally found in the 'advanced BIOS setup' menu option in the BIOS screen.

Once you have begun the installation procedure, relax and follow the prompts. You will be shown your available drives and prompted to create, size and format partitions on them as part of the installation process. Nothing outside the install needs to be done unless you opt not to use the full space of your new drive for installing Windows.

If you have left space free on your new drive, once the installation is finished you will need to go into disk manager by right clicking 'my computer' and selecting 'manage.' Once you are in the management screen, select 'disk management.' From here, the unpartitioned space on your hard disk can be seen as the black 'unpartitioned space' section in the graphic display on the bottom pane.



Disk 1
Basic
15.90 GB
Online

15.90 GB
Unallocated

FIG 1.2.2 a

Simply right click the unused space and select 'new partition' to use this space. The wizard will walk you through creating, sizing and formatting the partition with NTFS or FAT32.

QUE?

What does NTFS and FAT stand for?

NTFS is a high-performance and self-healing file system proprietary to Windows XP Vista 2008 2003 2000 NT & Windows 7, Windows 8, which supports file-level security, compression and auditing. It also supports large volumes and powerful storage solution such as RAID. The most important features of NTFS are data integrity and the ability to encrypt files and folders to protect your sensitive data.

FAT- File Allocation Table (FAT) file system is a simple file system originally designed for small disks and simple folder structures. The FAT file system is named for its method of organization, the file allocation table, which resides at the beginning of the volume. To protect the volume, two copies of the table are kept, in case one becomes damaged. In addition, the file allocation tables and the root folder must be stored in a fixed location so that the files needed to start the system can be correctly located.

1.3 Disc start up

What is a startup disk?

A boot disk (sometimes called a startup disk) is a type of removable media, such as a floppy disk or a CD that contains startup files that your computer can use to start Windows. The startup files are also stored on your computer's hard disk, but if those startup files become damaged, you can use the files on a boot disk to start Windows.

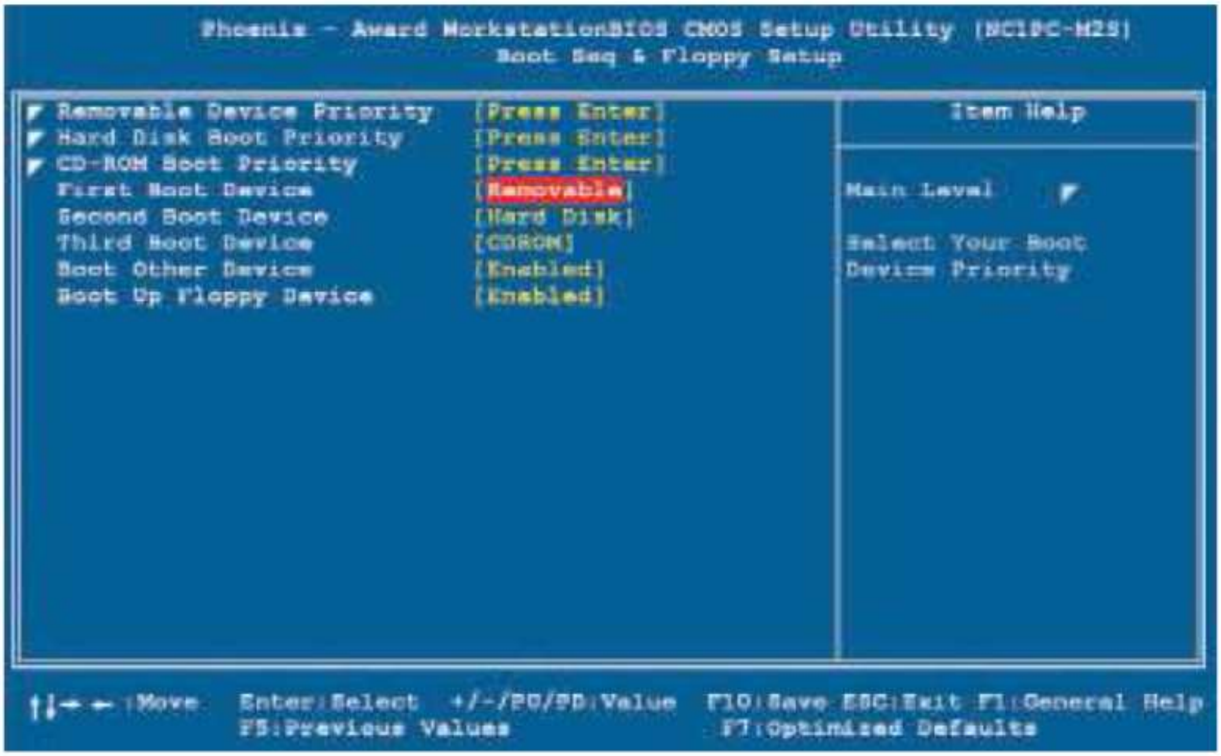
In earlier operating systems that used the FAT or FAT32 file systems, such as Windows 95 and Windows 98, a boot disk was especially useful because it allowed a person to access files on a hard disk even if Windows was unable to start. This ability also represented a security risk, because anyone with a boot disk and access to the computer could start the computer and access any file. Hard disks formatted with NTFS have built-in security features that prevent using a boot disk to access files.

The Windows installation disc contains the files necessary to start Windows, so it is itself a boot disk. If a problem is preventing Windows from starting, you can use the installation CD to start Windows. The installation CD also contains Startup Repair, which you can use to repair Windows if a problem prevents it from starting correctly. Startup Repair can automatically fix many of the problems that in the past required a boot disk to fix.

Depending on the circumstances and the available hardware, you have options as to the method used for the installation. Choices are the boot device you will use, how you might choose to use the network, and options involving installations from a hard drive image, recovery CDs, factory recovery partitions, and repairs to the existing installation. All these options are discussed next.

BOOT MEDIA USED FOR THE INSTALLATION

If an OS is not already installed on the hard drive, you must boot using the device from which you will install the OS. The boot device most likely will be the DVD or CD drive. However, you can use any device that the PC is capable of booting from. For example, suppose you want to install Windows Vista from the Vista setup DVD, but the system has a CD drive. You can use an external DVD drive that connects to the PC by way of a USB port. Access BIOS setup and set the boot order for USB as the first boot device. You can then boot from the external DVD drive and install Vista. The boot order is the order of devices that startup BIOS looks to for an OS. To change the boot order, enter BIOS setup and look for the appropriate screen. To enter BIOS setup, you press a key, such as F2 or Del, as the computer is booting and before the OS begins to load. To know which key to press, look for a message on-screen during the boot, such as “Press Del to enter setup.” The BIOS setup screen shown in Figure 3-4 shows a removable device as the first boot device.



```
          Phoenix - Award WorkstationBIOS CMOS Setup Utility (NC1PC-M2S)
                              Boot Seq & Floppy Setup

 ▸ Removable Device Priority   [Press Enter]          Item Help
 ▸ Hard Disk Boot Priority     [Press Enter]
 ▸ CD-ROM Boot Priority        [Press Enter]
   First Boot Device           [Removable]     Main Level   ▸
   Second Boot Device          [Hard Disk]
   Third Boot Device           [CDROM]         Select Your Boot
   Boot Other Device           [Enabled]       Device Priority
   Boot Up Floppy Device       [Enabled]

 ↑↓→ ←:Move  Enter:Select  +/-/PU/PD:Value  F10:Save ESC:Exit F1:General Help
             F5:Previous Values              F7:Optimized Defaults
```

Fig 1.3A

1.4 Installation of software in the network

You can copy the setup files on the Windows CD or DVD to a file server on the network. If you will be doing multiple installations, this method might save you some time. Copy the files from the CD or DVD to a folder on the server and share the folder.

Then at each PC, you can execute the Setup program on the server. A server used in this way is called a **distribution server.**

Chapter Review Questions

1. What are the functions of an operating system?
2. Compare and contrast the different types of hard disks?
3. What does APM stand for and what are its functionalities?
4. What are the advantages of fiber optic cables of other transmission mediums?
5. Discuss the various types of fiber optic cables?
6. Differentiate between straight through and crossover cables and state where each is used?
7. What is a startup disk and what is it used for?

Research question: what are the safety procedures involved in computer operating system installation?

Chapter 2: Installation and customization of various hardware devices

Chapter Learning Objectives: *By the end of this chapter you should appreciate Installation and customization of various hardware devices their power requirements, types of cables used in a computer setup, connectors, ports, devices driver, how to perform disk partitioning, formatting, disk space check, memory capacity, processor speed check. You should also be able to utilize various* Software customization tools such as task bar, startup menu, desktop, screen saver, fonts, color, creating shortcuts to program groups. You should also be able to perform System maintenance including back up restoration, use of hardware diagnostic tools in system software, scandisk, restoration.

Computer hardware refers to the physical components of a computer such as the monitor, Keyboard, Mouse, system unit etc

Hardware units (Devices) of a computer can be categorized into five units;

I. Input unit
II. Output
III. Central processing unit (CPU) or processor
IV. Main Memory
V. Secondary storage/Backing Storage

2.1 Installation

2.1.1 Power requirements

If there is any one component that is absolutely vital to the operation of a computer, it is the power supply. Without it, a computer is just an inert box full of plastic and metal. The power supply converts the alternating current (AC) line from your socket to the direct current (DC) needed by the personal computer.

In a personal computer (PC), the power supply is the metal box usually found in a corner of the case. The power supply is visible from the back of many systems because it contains the power-cord receptacle and the cooling fan.

Power supplies, often referred to as "switching power supplies", use switcher technology to convert the AC input to lower DC voltages. The typical voltages supplied are:

- 3.3 volts
- 5 volts
- 12 volts

The 3.3- and 5-volts are typically used by digital circuits, while the 12-volt is used to run motors in disk drives and fans. The main specification of a power supply is in **watts**. A watt is the product of the **voltage** in volts and the **current** in amperes or amps

Today you turn on the power with a little push button, and you turn off the machine with a menu option. These capabilities were added to standard power supplies several years ago. The operating system can send a signal to the power supply to tell it to turn off. The push button sends a 5-volt signal to the power supply to tell it when to turn on. The power supply also has a circuit that supplies 5 volts, called VSB for "standby voltage" even when it is officially "off", so that the button will work.

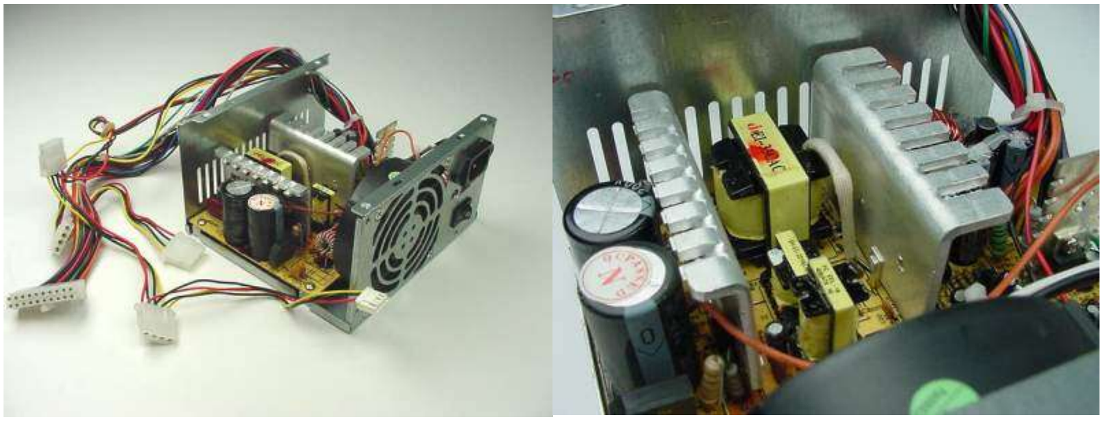


FIG 2.1.1 a

power supply .source: www.howstuffworks.com

The switching power supplies used today are much smaller and lighter. They convert the 60-Hertz (Hz, or cycles per second) current to a much higher frequency, meaning more cycles per second. This conversion enables a small, lightweight transformer in the power supply to do the actual voltage step-down from 110 volts (or 220 in certain countries) to the voltage needed by the particular computer component. The higher-frequency AC current provided by a switcher supply is also easier to rectify and filter compared to the original 60-Hz AC line voltage, reducing the variances in voltage for the sensitive electronic components in the computer.

A switcher power supply draws only the power it needs from the AC line. The typical voltages and current provided by a power supply are shown on the label on a power supply.

Switcher technology is also used to make AC from DC, as found in many of the automobile power inverters used to run AC appliances in an automobile and in uninterruptible power supplies.

Power Supply Standardization

Over time, there have been at least six different standard power supplies for personal computers. Recently, the industry has settled on using ATX-based power supplies. ATX is an industry specification that means the power supply has the physical characteristics to fit a standard ATX case and the electrical characteristics to work with an ATX motherboard.

PC power-supply cables use standardized, keyed connectors that make it difficult to connect the wrong ones. Also, fan manufacturers often use the same connectors as the power cables for disk drives, allowing a fan to easily obtain the 12 volts it needs. Color-coded wires and industry standard connectors make it possible for the consumer to have many choices for a replacement power supply.

Advanced Power Management (APM) offers a set of five different states that your system can be in. It was developed by Microsoft and Intel for PC users who wish to conserve power. Each system component, including the operating system, basic input/output system (BIOS), motherboard and attached devices all need to be APM-compliant to be able to use this feature. Should you wish to disable APM because you suspect it is using up system resources or causing a conflict, the best way to do this is in the BIOS. That way, the operating system won't try to reinstall it, which could happen if it were disabled only in the software.

Some power consumption values (in watts) for common items in a personal computer are:

- Accelerated Graphics Port (AGP) card = 20 to 30W
- Peripheral Component Interconnect (PCI) card = 5W
- small computer system interface (SCSI) PCI card = 20 to 25W
- network interface card = 4W
- 50X CD-ROM drive = 10 to 25W
- RAM = 10W per 128M
- 5200 RPM Integrated Drive Electronics (IDE) hard disk drive = 5 to 11W
- 7200 RPM IDE hard disk drive = 5-15W
- Motherboard (without CPU or RAM) = 20 to 30W
- 550 MHz Pentium III = 30W
- 733 MHz Pentium III = 23.5W
- 300 MHz Celeron = 18W
- 600 MHz Athlon = 45W

Power supply problems

The PC power supply is probably the most failure-prone item in a personal computer. It heats and cools each time it is used and receives the first in-rush of AC current when the PC is switched on. Typically, a stalled cooling fan is a predictor of a power supply failure due to subsequent overheated components. All devices in a PC receive their DC power via the power supply.

A typical failure of a PC power supply is often noticed as a burning smell just before the computer shuts down. Another problem could be the failure of the vital cooling fan, which allows components in the power supply to overheat. Failure symptoms include random rebooting or failure in Windows for no apparent reason.

2.1.2 Types of cables

Fiber-Optic Cable

Optical fiber is usually used for longer, high bandwidth, point-to-point transmission. The fiber-optic cable uses light to transmit data through thin glass or plastic fiber. Electrical signals cause a fiber-optic transmitter to generate the light signals sent down the fiber. The receiving host receives the light signals and converts them to electrical signals. The glass used in fiber-optic cable acts as an electrical insulator. No electricity is used in the fiber-optic cable.

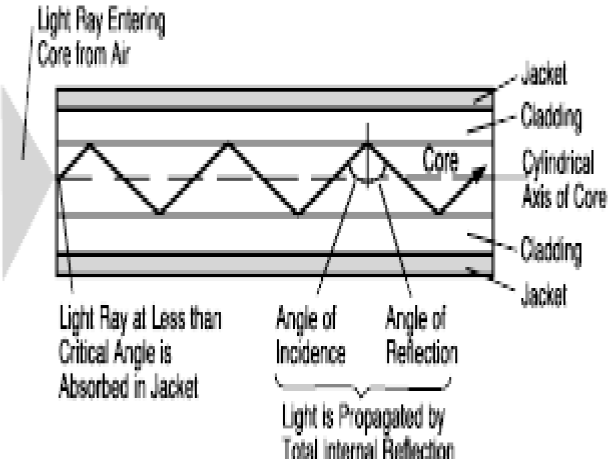
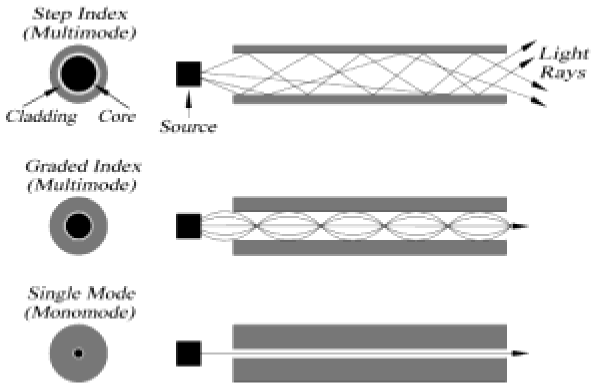

Light Ray Entering Core from Air
Jacket
Cladding
Core
Cylindrical Axis of Core
Cladding
Jacket
Light Ray at Less than Critical Angle is Absorbed in Jacket
Angle of Incidence
Angle of Reflection
Light is Propagated by Total Internal Reflection

FIG 2.1.2 a



<u>Advantages</u>:

- It operate at high speeds
- It has a large carrying capacity
- The signals can be transmitted further without being strengthened.
- It is immune to interference caused by electromagnetic noise such as radios, motors, or other nearby cables.
- It is cheaper to maintain.
- You do not have to worry about grounding[1] the cable.

<u>Disadvantages</u>:

- The cable is more expensive than copper cables.
- It is difficult to install.

Coaxial Cable

Description

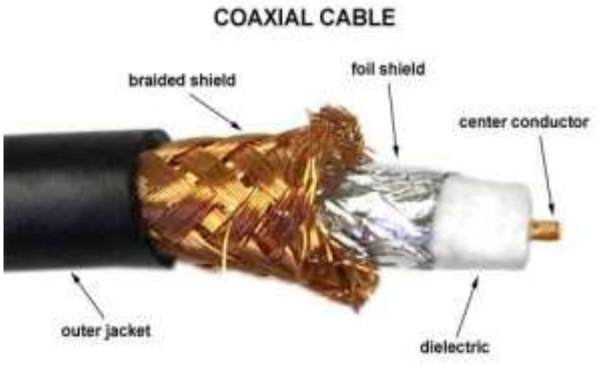


FIG 2.1.2 b

Coaxial cable is made up of a copper conductor surrounded by a layer of flexible insulation. The center conductor can also be made of tin plated aluminum cable allowing for the cable to be manufactured inexpensively.

Over this insulating material is a woven copper braid or metallic foil that acts as the second wire in the circuit and as a shield for the inner conductor. This second layer or shield also reduces the amount of outside electromagnetic interference. Covering this shield is the cable jacket. Cable television uses coaxial cable.

Advantages:

- It can be run longer distances than shielded twisted pair cables and unshielded twisted pair cables without the need for repeaters[2].
- Coaxial cable is less expensive than fiber-optic cable.
- It is cheap to install.
- It has a greater capacity than UTP cables.

Disadvantages:

- Coaxial cable is more expensive to install than twisted-pair cable.
- It is limited in its distance.
- It has a limited number of connections that can be made to it.

Shielded Twisted Pair (STP)

Description:

STP cable uses cancellation, shielding, and twisted wires. The twisted wires and shielded twisted-pair cables allow for more cancellation of electrical interference than the unshielded twisted-pair cables. Each pair of wires is wrapped in metallic foil and those four pairs of wires are wrapped in an overall metallic foil.

Advantages:

- The shielding provides more protection from all types of incoming external interference.
- The shielding minimizes outgoing radiated electromagnetic waves that could potentially cause noise in other devices.

Disadvantages:

- It is more expensive and difficult to install than UTP.
- It cannot be run as far as coaxial cable or optical fiber without the signal being repeated.
- The metallic shielding materials in STP need to be grounded[1] at both ends. If improperly grounded[1] or if there are any breaks in the shielding of the cable it can suffer from noise problems. The shield will act like an antenna picking up unwanted signals in the case that it is not properly grounded or the shielding has breaks in it.

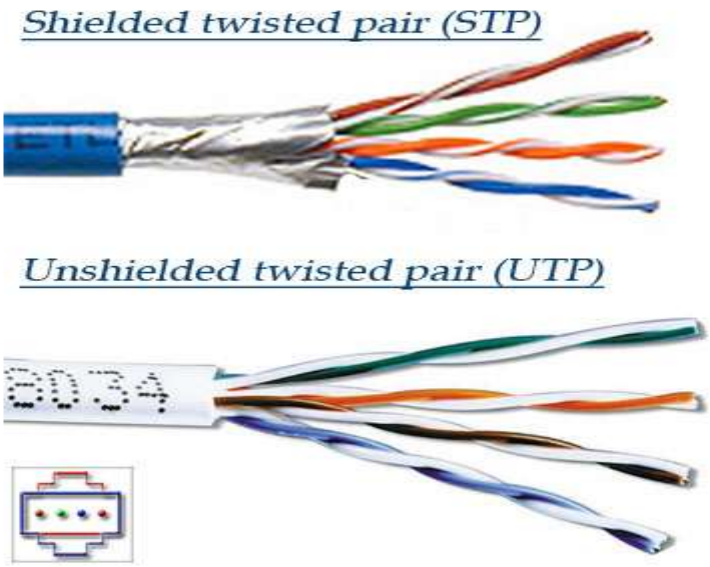


FIG 2.1.2 c :Network Troubleshooting and Resource Site for School IT Staff | Network Cables. (n.d.). Retrieved from http://webpage.pace.edu/ms16182p/networking/cables.html

Unshielded Twisted Pair (UTP)

Description:

UTP is a four-pair wire medium used in a variety of networks. Each of the eight copper wires in the UTP cable is covered by insulating material. In addition, each pair of wires is twisted around each other. This type of cable relies on the cancellation effect produced by the twisted wire pairs to limit attenuation[3] caused by electromagnetic interference and radio frequency interference.

Advantages:

- It is easy to install and is less expensive than other types of cables.
- The cable has a small external diameter and does not fill up wiring ducts as fast as the other types of cable.
- It is easy to terminate.
- It is used most often.

Disadvantages:

- It is more likely to pick up interference than other types of cables.
- The distance between signal boosts is shorter for UTP than it is for coaxial and fiber optic cables. This means that you must strengthen the signal more often.

There are 5 different types of categories of UTP cables as listed below.

Type	**Data Rates**	**Use**
Category 1	-------	*Voice Only (Telephone Cable)*
Category 2	*Data to 4 Mbps*	*LocalTalk*
Category 3	*Data to 10 Mbps*	*Ethernet*
Category 4	*Data to 20 Mbps*	*Some Token Rings*
Category 5	*Data to 100 Mbps*	*Ethernet and Fast Ethernet*

Table 2.1.2 a

Terms

---

1. Ground - a return path for current. Its purpose is to close the current loop.

2. Repeaters - a device used to regenerate the signals in a network so that they can cover greater distances.

3. Attenuation - the loss of signal strength which begins to occur as the signal travels further along a cable.

2.1.3 Types of connectors and Ports

1. VGA Cable

Also known as D-sub cable, analog video cable

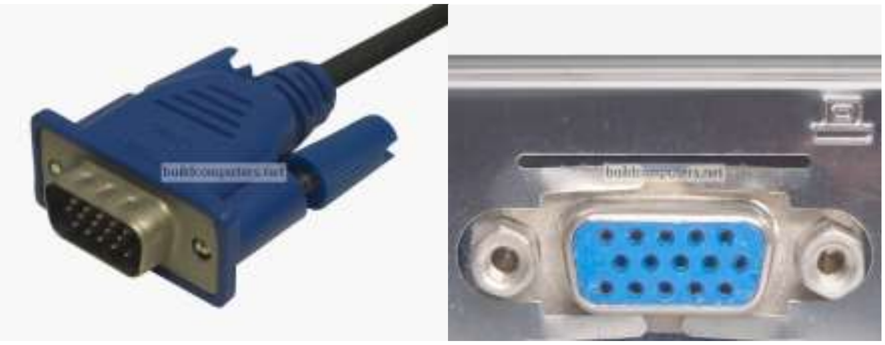


FIG 2.1.3 a

Connect one end to: computer monitor, television (PC input port)

Connect other end to: VGA port on computer

A VGA cable is a lead used for transmitting video signals, and it is most commonly used to link computers with monitors. Some high definition televisions use this type of cable as well. VGA stands for video graphics array, and it was a graphics standard used by IBM in its early PCs sold in the 1980s. Today, all PCs support VGA, but most of them use a more advanced system depending on the actual monitor used. The Windows® loading screen appears using VGA as it is seen before the computer loads the relevant information about the monitor to use.

In most cases, the term "VGA" refers to the type of cable used to carry the display signals, regardless of the actual graphics system being used. It’s characterized by 15 pins on the plug in three rows of five. The plug also has two screws, one either side of the pins, that secure it into place in the socket. These screws have ridged edges, meaning they can be tightened and loosened by hand rather than needing a screwdriver.

2. DVI Cable

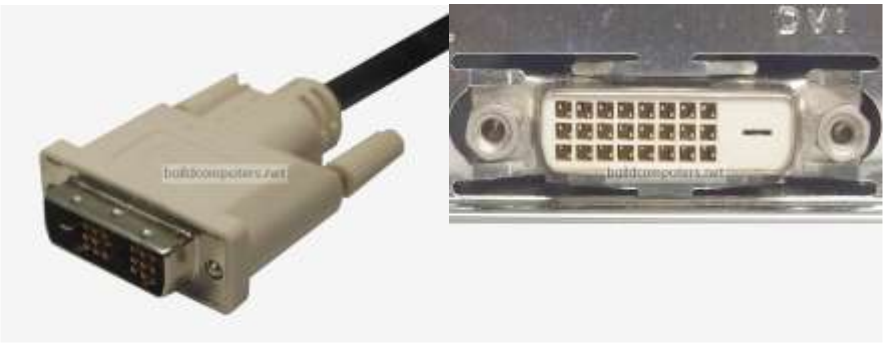


FIG 2.1.3 b

Connect one end to: computer monitor

Connect other end to: DVI port on computer

DVI cables are used with DVI-enabled graphics cards to utilize the *Digital Visual Interface*, (sometimes called *Digital Video Interface*), in order to maximize the benefit of flat panel digital displays.

The traditional Video Graphics Array (VGA) interface was designed for use with analog CRT (cathode ray tube) monitors. It converts digital signals received from the graphics card into analog signals which it sends to the monitor. This conversion to analog creates minute distortions in the integrity of the signal. While necessary for CRT monitors, flat panel displays are themselves digital. With a DVI interface on the video or graphics card, pure digital output can be achieved using DVI cables, resulting in a sharper picture.

There are several types of DVI cables or connectors. Some transfer both analog and digital signals to accommodate intermixed components, as this digital interface acted as a bridge between the market transition from VGA and CRT monitors to digital monitors. The main types of DVI cables are:

DVI-D (Digital, for use with digital displays): These cables link DVI-graphics cards to digital displays. They transfer **digital-to-digital** signals, eliminate analog conversion and cannot accommodate CRT displays.

DVI-A (Analog, for use with analog displays): These DVI cables run from the DVI graphics card to an analog CRT display, converting **digital-to-analog**. Although some purity is lost in the conversion from digital to analog, using a DVI card and DVI-A cable with a CRT monitor delivers superior performance to using a VGA interface.

3. HDMI Cable

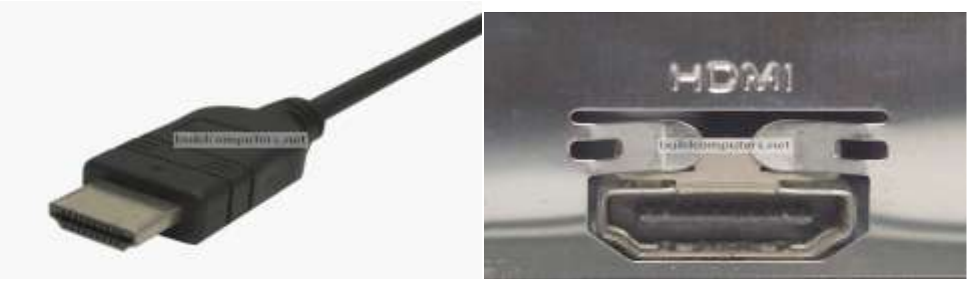


FIG 2.1.3 C

Connect one end to: computer monitor, television

Connect other end to: HDMI port on computer

Note: If you're hooking up a television to your computer, then we would recommend that you use a HDMI cable as your PC cable connection since it is able to transmit both display and sound - So you can not only use your TV screen as a monitor, but also make use of your TV speakers to play PC audio.

HDMI® (High-Definition Multimedia Interface) is an interface standard used for audiovisual equipment, such as high-definition television and home theater systems. With 19 wires wrapped in a single cable that resembles a USB wire, the cable is able to carry a bandwidth of 5 gigabits per second (Gbps). This is more than twice the bandwidth needed to transmit multi-channel audio and video, future-proofing the interface for some time to come. This and several other factors make HDMI® much more desirable than its predecessors, component video, S-Video, and composite video.

Signals that travel through the HDMI® interface are uncompressed and all-digital, while the previous interfaces were all analog. With an analog interface, a clean digital source is translated into less precise analog, sent to the television, then converted back to a digital signal to display on screen. At each translation, the digital signal loses integrity, resulting in some distortion of picture quality. HDMI® preserves the source signal, eliminating analog conversion to deliver the sharpest, richest picture possible.

Previous video interfaces required separate audio cables, with the vast majority of people using standard RCA L/R analog audio jacks. HDMI®, with its abundant bandwidth and speed, carries not only video but also up to eight digital audio channels for uncompromised surround-sound. It replaces the tangle of wires behind the system with a single cable, greatly simplifying the entire setup process of the home theater system while delivering top tier performance.

4. PS/2 Cable

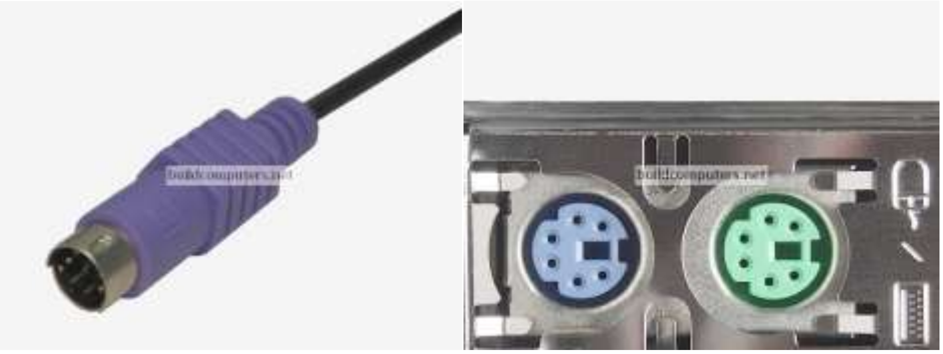


FIG 2.1.3 d

Connect one end to: PS/2 keyboard, PS/2 mouse

Connect other end to: PS/2 ports on computer (see image below)

- Purple PS/2 port: keyboard
- Green PS/2 port: mouse

A PS/2 connector is a plug and socket system used for connecting keyboards and mice to PC computers. It has largely been superseded by Universal Serial Bus (USB) connectors, but is still used on some machines. Relatively cheap adaptors can allow an input device with a PS/2connector to work on a computer that only has USB sockets.

The PS/2 connector system consists of a plug with six circular pins and one flat pin, arranged roughly in a circle. Although the physical design of the connector and socket is the same for both keyboards and mice, the commands sent to the computer mean sockets and plugs for each are not necessarily interchangeable. To avoid conflicts, both sockets and plugs are color-coded: green for mice and purple for keyboards. This color system was introduced several years after the connectors debuted, as a response to customer confusion. It was part of the same color coding system by which analog monitors are connected with a blue plug and socket.

5. Ethernet Cable

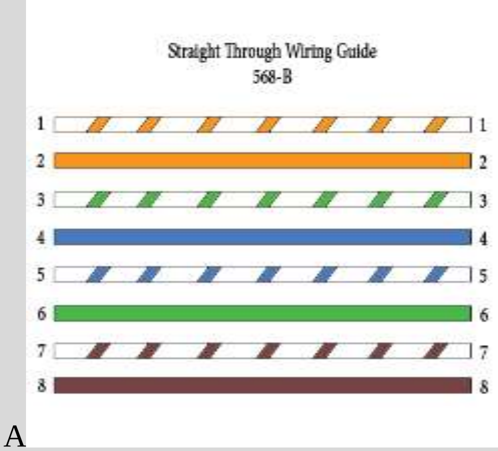
Also known as RJ-45 cable

Connect one end to: router, network switch

Connect other end to: Ethernet port on computer.

Straight-Through Wired Cables

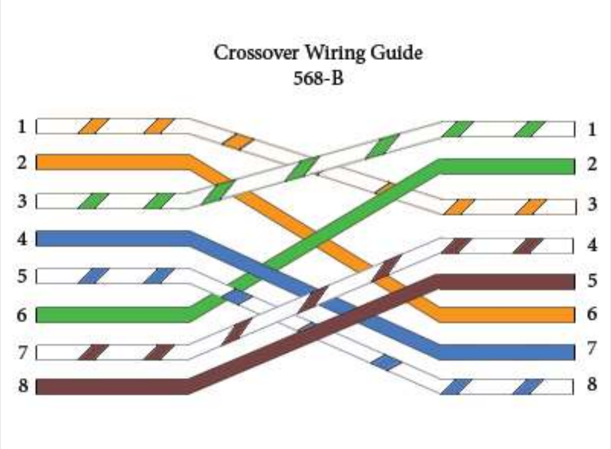
Straight-Through refers to cables that have the pin assignments on each end of the cable. In other words Pin 1 connector A goes to Pin 1 on connector B, Pin 2 to Pin 2 etc. Straight-Through wired cables are most commonly used to connect a host to client. When we talk about cat5e patch cables, the Straight-Through wired cat5e patch cable is used to connect computers, printers and other network client devices to the router switch or hub (the host device in this instance).



A B

Crossover Wired Cables

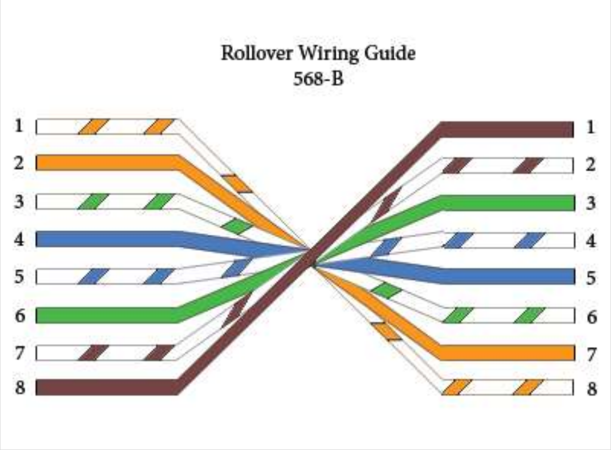
Crossover wired cables (commonly called crossover cables) are very much like Straight-Through cables with the exception that TX and RX lines are crossed (they are at opposite positions on either end of the cable. Using the 568-B standard as an example below you will see that Pin 1 on connector A goes to Pin 3 on connector B. Pin 2 on connector A goes to Pin 6 on connector B ect. Crossover cables are most commonly used to connect two hosts directly. Examples would be connecting a computer directly to another computer, connecting a switch directly to another switch, or connecting a router to a router.*Note: While in the past when connecting two host devices directly a crossover cable was required. Now days most devices have auto sensing technology that detects the cable and device and crosses pairs when needed.*



A B

Rollover Wired Cables

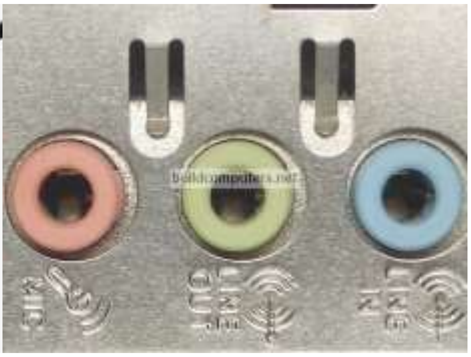
Rollover wired cables most commonly called rollover cables, have opposite Pin assignments on each end of the cable or in other words it is "rolled over". Pin 1 of connector A would be connected to Pin 8 of connector B. Pin 2 of connector A would be connected to Pin 7 of connector B and so on. Rollover cables, sometimes referred to as Yost cables are most commonly used to connect to a devices console port to make programming changes to the device. Unlike crossover and straight-wired cables, rollover cables are not intended to carry data but instead create an interface with the device.



A B

6. 3.5mm Audio Cable

Also known as phone connector (since 3.5mm jacks are often found on mobile phones too)



Connect one end to: computer speakers, 3.5mm headphones, 3.5mm microphone

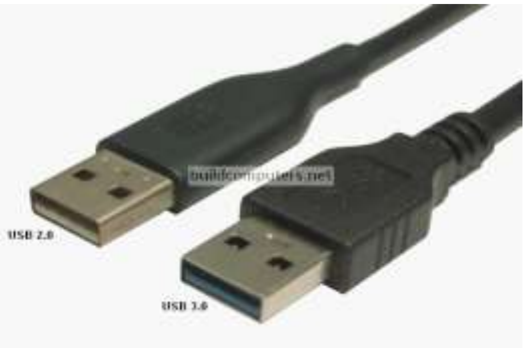
Connect other end to: audio ports on computer (see image below)

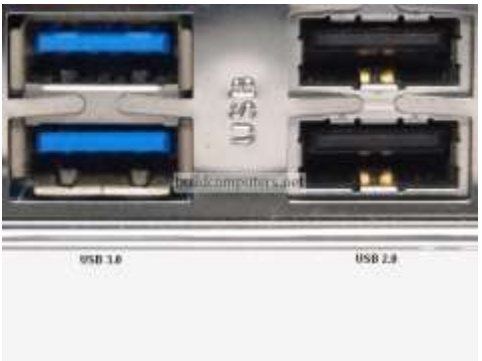
- Green audio port: computer speakers or headphones
- Pink audio port: microphone
- Blue audio port: MP3 player, CD player, DVD player, turntable, electric guitar etc (line-in port to play and record sounds from the above devices)

7. USB Cable

For USB computer cable connections, there are 2 formats that are in popular use: USB 2.0 and the newer USB 3.0

How to tell USB 2.0 and 3.0 cables apart: USB 3.0 cables have a blue tip, and sometimes you can find a SS "Super Speed" label on it. See image below:





Since USB was intended to be the one computer cable connection to replace them all, it's no surprise that the possible uses for a USB port are quite mind-blowing. Its more common uses are listed below:

- Storage devices: USB flash drive, external hard drive, external optical drive
- Input devices: USB keyboard (wired and wireless), USB mouse (wired and wireless), webcam, scanner, gamepad
- Output devices: printer, all-in-one office machine, USB speaker
- Wireless adapters: network (Wi-Fi) adapter, bluetooth adapter, 3G adapter
- Data (and charging) cable for mobile devices such as mobile phone, tablet, MP3 player

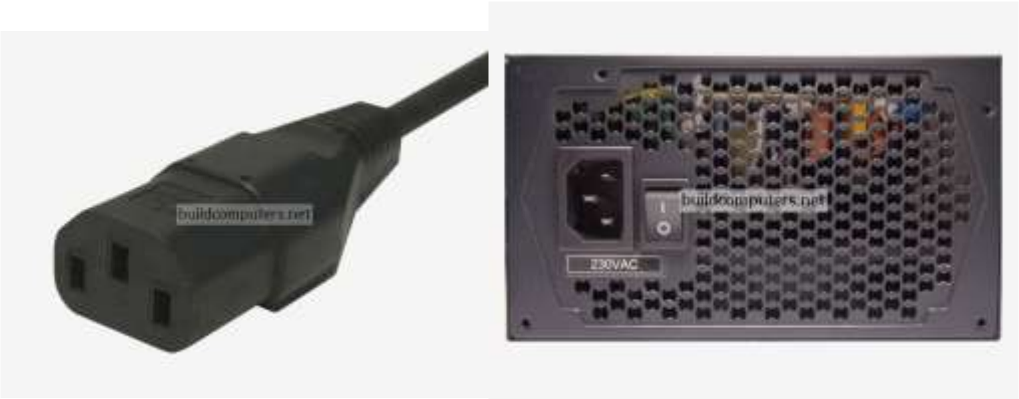
How to tell USB 2.0 and 3.0 ports apart: USB 2.0 ports have black tips while USB 3.0 ports come with blue tips. See image below:

USB 3.0 is backwards-compatible... meaning that you can connect a USB 2.0 device to a USB 3.0 port and vice versa (but the USB 3.0 devices hooked up to a USB 2.0 port will perform at lowered rates).

Que?

What are the advantages of using USB 3.0 over USB 2.0?

8. Computer Power Cord



Connect one end to: AC power socket

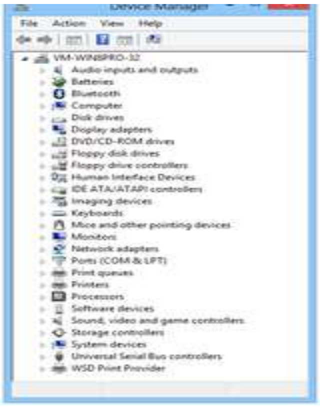
Connect other end to: power supply unit (see image below), computer monitor

Note: Always turn off your power supply unit (with the 1-0 switch at the back) before connecting a power cord to it.

2.1.2 Devices driver

A driver is a small piece of software that tells the operating system and other software how to communicate with a piece of hardware.

For example, all printers come accompanied with drivers to install that tell the operating system exactly how to print information on the page. Sound card drivers tell your software exactly how to translate data into audio signals that the card can output to a set of speakers. The same applies to video cards, keyboards, monitors, etc.
The drivers for each piece of hardware in your Windows computer are centrally managed from device Manager, available in all versions of Microsoft Windows.



Device Manager is an extension of the Microsoft Management Console that provides a central and organized view of all the Microsoft Windows recognized hardware installed in a computer.

Device Manager (What It Is and How To Use It). (n.d.). Retrieved from http://pcsupport.about.com/od/termsd/p/devicemanager.htm

When you boot your computer there is a small utility called setup, which resides in the operating system and is responsible for setting up your devices and making the system ready to use. This setup program loads or installs the device drivers depending upon the need. For example in the initial stage of booting the setup loads only the Keyboard, Mouse, Video adapter, SCSI/Disk, and Machine/HAL. These drivers are very much necessary for the setup to continue booting of the computer. This stage is mainly referred as **text-mode setup**.

Once the text-mode setup is completed, the setup program then boots the operating system and goes on with the GUI (Graphic User Interface) stage of booting. During this stage most of the devices are installed in the computer.

Few devices may not get installed during this stage because may be they are being installed for the first time and needs users interaction for configuration or the setup was not able to find the appropriate device drivers to be loaded.

As soon as the computer is booted up and is in a running state, you can setup the required devices using *Add/Remove Hardware*wizard to install these devices. In order to install these devices, the setup works along with other components both system-supplied and vendor-supplied. The devices are installed by setup once the system boots and when a user adds a Plug and Play device or manually installs a non-plug and play device. Setup ascertains the devices available in the computer, loads them and then calls the drivers for each device. Drivers such as the ACPI driver and other plug and play bus drivers assist setup to determine the devices that are present on the computer.

Now let's have a look at the device installation setup components for windows 2000 and later operating system.

This installation is divided into two parts - kernel mode and user mode.

Kernel-Mode Plug and Play Manager

The kernel-mode plug and play manager informs the user-mode plug and play manager that a new device is present on the machine and needs to be installed. The kernel-mode PNP (Plug And

Play) manager also calls the “**DriverEntry**” and “**AddDevice**” routines of a device driver and sends a request to start the device. All the PNP (Plug And Play) events that take place are reported to PNP (Plug And Play) manager of the user mode by the kernel-mode PNP (Plug And Play). The user mode PNP (Plug And Play) manager sends control requests to the kernel mode PNP (Plug And Play) manager.

Drivers

PNP manager gives directions to PNP (Plug And Play) drivers on how to install devices. These drivers would then execute **DriverEntry** and **AddDevice** routines when called by the PNP (Plug And Play) Manager. Also, Plug and Play drivers are capable of detecting non-Plug and Play devices using “**IoReportDetectedDevice**”.

User-Mode Plug and Play Manager

The ***kernel mode plug and play manager*** sends device installation requests to the ***user mode plug and play Manager*** and also calls other user-mode Setup components to initiate device installation tasks. After this the ***user mode plug*** and play manager sends control requests to the ***kernel mode plug*** and play manager (such as start the device)

The ***user-mode Plug and Play Manager and the kernel-mode Plug and Play Manager*** together maintain the device tree. Incase the ***Plug and Play Manager*** is not able to complete the installation automatically then the installation is aborted. In such a case, the ***Plug and Play Manager*** restarts the device installation when a user logs in by launching the Found New Hardware wizard in the New Device.

Setup API

The Setup API consists of the **Setup**Xxx and the **SetupDi**Xxx functions. Many device installation jobs such as looking for INF files, building a potential list of drivers for a device, copying driver files, writing information to the registry, registering device co-installers etc. are performed by Setupxxx and SetupDixxx functions. **CfgMgr API**

The Configuration Manager API provides basic installation and configuration operations that are not provided by Setup API. The Configuration Manager function performs low level tasks such as managing resource descriptors. Setup API is responsible for calling these functions. However, they can also be called by the other Setup components.

Co-installers and Class Installers

Class installers perform the installation steps relevant to devices in a particular device setup class. For instance, the ports class installer is responsible for assigning a COM port name to a device in the ports setup class.

Co-installer is responsible for installing a particular device or to setup class of devices.

INF files and catalog files

INF files and catalog files give information about the devices and the drivers that are to be installed.

Device Manager

The *Device Manager* provides interface to a user to view and manage the devices on a computer. For example, a user can view device status and set device properties. In case a user requests to update a driver, the *Device Manager* gives a call to the *Update Driver wizard* in the New Device DLL.

Add/Remove Hardware Wizard

The *Add/Remove Hardware* Wizard lets a user to add, remove, unplug, and troubleshoot devices.

New Device DLL

The New Device DLL has the *Found New Hardware* wizard, the *Update Driver* wizard, and the "**UpdateDriverForPlugAndPlayDevices**" functions.

In order to start the installation of a new device, the user-mode Plug and Play Manager calls the*Found New Hardware* wizard. When a user selects the "*Update Driver...*" button on a Device's Driver property page, then the *Device Manager* calls the *Update Driver* wizard. Finally, the Found New Hardware and Update Driver wizards call Setup APIs and Configuration Manager APIs to complete their respective tasks.

2.1.3 Disk partitioning

A *partition* is a segment of the hard disk, created by dividing the disk logically into discrete units. You create partitions for a number of reasons: say, to organize your applications and operating system on drive C while storing your data on drive D. You might also partition a disk for more technical reasons, such as to run multiple OSes on the same machine.

Before creating your partitions, you may need to initialize the disk in Windows Disk Management. When you initialize the disk you choose which partition table format you wish to use:

- *Master Boot Record* (**MBR):** The default partition table type. This is limited to four partitions per disk and volumes up to two terabytes (TB) in size.
- *GUID Partition Table* (**GPT):** The GPT partition table style supports up to 128 partitions and volume sizes up to 18 exabytes (EB) in size.

Operating systems such as Windows XP and Windows 7/Vista, which use basic disks can create two types of partitions: primary partitions and extended partitions.

Primary partition

The *primary partition* is the partition that the computer boots from; the OS's boot files are loaded from here. You are allowed to have four primary partitions per disk. Because you may have multiple primary partitions (say, if you are running several OSes on the same computer), you must designate one primary partition as the *active partition* — the partition from which your normal operating system loads.

Extended partition

An extended partition allows you to extend beyond the four-partition barrier by being a partition that contains one or more *logical drives*, which are blocks of disk space assigned a drive letter.

As an example on how you could use extended partitions, you could set up three primary partitions and then decide that you would like to divide the last chunk of free space into three additional parts (for a total of six partitions). If you create another primary partition from some of the free space, you will have four parts — and that is your limit, four partitions per disk. What you can do instead is create an extended partition from the remaining space after the three primary partitions have been created and then create three logical drives inside the extended partition. Logical drives are not partitions, so you are not limited to four. This will give you your six desired parts.

An *extended partition* is, in effect, the space that remains after the primary partitions are defined. The extended partition does not have an actual drive letter assigned to it; it's simply a container that holds all the logical drives that you build. A *logical drive* is a logical division of the hard disk that the computer treats as if it were a separate disk drive; it is the actual area of the extended partition to which documents are saved.

2.1.4 Formatting

There are many reasons why you might want to format a hard drive, including a clean installation of Windows, to get rid of a virus or malware or simply because you're giving the drive to someone else or throwing it away.

You cannot format the hard drive on which Windows is running. In order to format the disk and reinstall Windows (or another operating system) you will need to boot your PC from a Windows installation disc, a USB flash drive or another bootable disc.

Formatting is the process of deleting all the data on the hard drive, but beware of 'Quick Format' which leaves all your data in place and makes the drive appear to be empty. A quick format is ok if you have a brand new hard drive, or you want to reinstall Windows, but not if you are disposing of the disk or giving it to someone else.

It is important to understand about partitions before you start. A hard drive's storage can be divided up into smaller sections, called partitions. It is possible to format one partition while leaving the others untouched. This is useful in certain situations, but if you want to format the entire hard drive and use the entire capacity in one block, you will also need to delete the partition information.

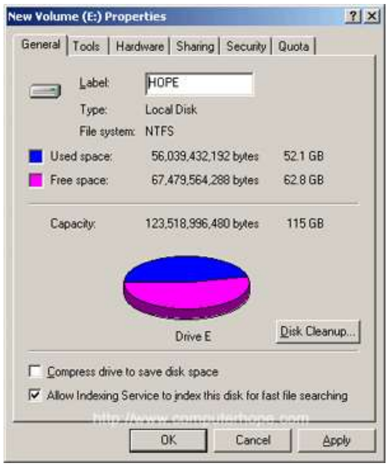
When formatting is performed, the surface of the hard drive platter is briefly scanned to find any possible bad spots, and the areas surrounding a bad spot are marked as bad sectors. Then magnetic tracks are laid down in concentric circles. These tracks are where information is eventually encoded. These tracks, in turn, are split into pieces of 512 bytes called *sectors*. Some space is reserved in between the sectors for error-correction information, referred to as cyclic redundancy check (CRC) information. The OS may use CRC information to re-create data that has been partially lost from a sector. An operating system boot record is created along with the root directory. Finally, the File Allocation Table (FAT) or Master File Table (MFT) is created. This table contains information about the location of files as they are placed onto the harddrive.

2.1.5 Disk space

Alternatively referred to as **disk capacity, disk space** is the total amount of bytes that a disk drive or disc is capable of holding. Typically, the storage device is the computer's hard drive, but it can also be a USB thumb drive, a CD or DVD, a memory stick/card, or a Floppy disk.

Disk space is usually measured in kilobytes (KB), megabytes (MB), gigabytes (GB), or terabytes (TB). For example, a hard drive that is 500GB is capable of holding 500 Gigabytes of information.

As shown in the figure, when viewing the properties of a storage device, it will usually display Used disk space and Free (Unused) disk space. Used space is what is already taken up by existing data/files on the computer and free space is what is available to use.



Label: HOPE

Type: Local Disk

File system: NTFS

■	Used space:	56,039,432,192 bytes	52.1 GB
■	Free space:	67,479,564,288 bytes	62.8 GB
	Capacity:	123,518,996,480 bytes	115 GB

□ Compress drive to save disk space

☑ Allow Indexing Service to index this disk for fast file searching

2.1.6 Memory capacity

RAM is an acronym for ***r**andom **a**ccess **m**emory*, a type of computer memory that can be accessed randomly; that is, any byte of memory can be accessed without touching the preceding bytes. RAM is the most common type of memory found in computers and other devices, such as printers.

When you’re selecting RAM for a memory upgrade, it is important to buy the right kind. On a modern system, you must match the RAM to the motherboard’s needs in the following areas:

Physical Size 168-pin or 184-DIMMs or 184-pin RIMMs and more.

Type SDRAM, Double Data Rate (DDR) SDRAM, or Rambus RAM.

Speed PC100, PC133, and up, as well as the DDR-based speeds discussed in Chapter 1.

Faster RAM than is required will work, but not slower.

Capacity 64MB, 128MB, 1GB, for example.

The characteristics of the chips that make up memory modules lead directly to the overall capacity of the modules.

When you’re shopping for RAM for a system, it’s important to consult the motherboard manual to find out the type of memory you need and any special rules for installation. Without the manual, you must open the case and observe the memory slots or existing memory to determine what is needed. Some motherboards have complex charts showing the combinations and positions of the modules that they allow.

Types of RAM

DRAM

DRAM is dynamic random access memory. (This is what most people are talking about when they mention RAM.) When you expand the memory in a computer, you are adding DRAM chips. You use DRAM to expand the

memory in the computer because it’s cheaper than any other type of memory. Dynamic RAM chips are cheaper to manufacture than other types because they are less complex. *Dynamic* refers to the memory chips’ need for a constant update signal (also called a *refresh* signal) in order to keep the information that is written there. If this signal is not received every so often, the information will cease to exist. Currently, there are four popular implementations of DRAM: SDRAM, DDR, DDR2, and RAMBUS.

SDRAM

The original form of DRAM had an asynchronous interface, meaning that it derived its clocking from the actual inbound signal, paying attention to the electrical aspects of the waveform, such as pulse width, to set its own clock to synchronize on the fly with the transmitter. *Synchronous DRAM (SDRAM)* shares a common clock signal with the transmitter of the data. The computer’s system bus clock provides the common signal that all SDRAM components use for each step to be performed.

This characteristic ties SDRAM to the speed of the FSB and the processor, eliminating the need to configure the CPU to wait for the memory to catch up. Every time the system clock ticks, one bit of data can be transmitted per data pin, limiting the bit rate per pin of SDRAM to the corresponding numerical value of the clock’s frequency. With today’s processors interfacing with memory using a parallel data-bus width of 8 bytes (hence the term 64-bit processor), a 100MHz clock signal produces 800MBps. That’s mega*bytes* per second, not mega*bits*.

Such memory is referred to as *PC100*, because throughput is easily computed as eight times the rating.

DDR

Double Data Rate (DDR) SDRAM earns its name by doubling the transfer rate of ordinary

SDRAM by double-pumping the data, which means transferring it on both the rising and falling edges of the clock signal. This obtains twice the transfer rate at the same FSB clock frequency. It’s the rising clock frequency that generates heating issues with newer components, so keeping the clock the same is an advantage. The same 100MHz clock gives a DDR SDRAM system the impression of a 200MHz clock in comparison to a *single data rate (SDR)* SDRAM system.

You can use this new frequency in your computations or simply remember to double your results for SDR calculations, producing DDR results. For example, with a 100MHz clock, two operations per cycle, and 8 bytes transferred per operation, the data rate is 1600MBps. Now that throughput is becoming a bit tricker to compute, the industry uses this final figure to name the memory modules instead of the frequency, which was used with SDR. This makes the result seem many times better, while it’s really only twice as good. In this example, the module is referred to as *PC1600*. The chips that go into making PC1600 modules are named after the perceived double-clock frequency: DDR-200.

2.1.7 Processor speed check

Your computer's central processing unit (CPU), also known as a processor, can be thought of as the brain of the computer. Fast processors typically offer better performance than slower processors, and they are especially useful for running multimedia programs, such as games or audio and video editing programs.

A computer's processor speed describes the maximum number of calculations per second the processor can perform, and is given in megahertz (MHz) or gigahertz (GHz). Generally, the larger the number, the faster and more powerful the processor.

To check on your processor speed (for Windows PC):-

1. Open System by clicking the Start button ,
2. Click Control Panel,
3. Click System and Maintenance
4. Clicking System.
5. Under System, you can view the processor type and speed, as well as the number of processors installed, if your computer uses multiple processors.

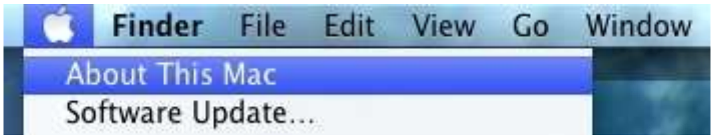
Or

1. Right click on My computer
2. Click on properties

You can check a Macs processor speed a few different ways, but here are two methods: super easy through the GUI, and a more advanced way through the command line.

Check a Mac CPU the Easy Way: GUI

Go up to the Apple menu and select “About This Mac”:



You will then get a window that shows what version of Mac OS X you are running, what your processor and processor speed is, and how much memory your Mac has.

2.2 Software customization;

2.2.1 Task bar,

The Taskbar contains two major items: the Start menu and the System Tray (systray). The Start menu is on the left side of the Taskbar and is easily identifiable: it is a button that has the word *Start* on it. The *System Tray* is located on the right side of the Taskbar and contains only a clock by default, but other Windows utilities (for example, screensavers or virus-protection utilities) may put their icons here to indicate that they are running and to provide the user with a quick way to access their features.

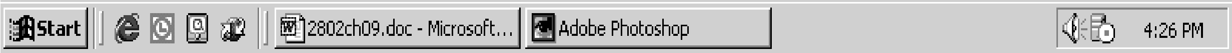


FIG 2.2.1a task bar

Windows also uses the middle area of the Taskbar. When you open a new window or program, it gets a button on the Taskbar with an icon that represents the window or program as well as the name of the window or program. To bring that window or program to the front (or to maximize it if it was minimized), click its button on the Taskbar. As the middle area of the Taskbar fills with buttons, the buttons become smaller so they can all be displayed.

You can increase the size of the Taskbar by moving the mouse pointer to the top of the Taskbar and pausing until the pointer turns into a double-headed arrow. Once this happens, click the mouse and move it up to make the Taskbar bigger. Or move it down to make the Taskbar smaller. You can also move the Taskbar to the top or side of the screen by clicking the Taskbar and dragging it to the new location.

2.2.2 Startup menu,

To display the Start menu, click the Start button in the Taskbar. You will see a Start menu similar to that shown in the Figure above.

Start menu serves the same function (quick access to important features and programs); however, its layout and options have changed. Note that if you change the Desktop's appearance to the Windows Classic look, this changes only the color scheme and so on—the options and layout of the Windows XP Start menu remain different from those in older versions of Windows. However, the way the Start menu works (the principles it applies) is essentially the same in Windows XP as in older versions.

From the Start menu, you can select any of the various options the menu presents. An arrow pointing to the right indicates that a submenu is available. To select a submenu, move the mouse pointer over the submenu title and pause. The submenu will appear; you don't even have to click. (You have to click to choose an option *on* the submenu, though.) One handy feature of the Start menu in pre–Windows XP versions of Windows is that it usually displays the name of the OS type along its side when you activate it. This provides an excellent way to quickly see whether you are on Windows 95, 98, Me, NT, or 2000. In Windows XP you don't see the name of the OS; however, the Start menu looks so different that you'll know you are using Windows XP. The Windows XP Start menu also displays the name of the currently logged-in user at the top.

2.2.3 Desktop,

In addition to the options in your Start menu, a number of icons are placed directly on the Desktop. Three of the most important icons are My Computer, Network Neighborhood/My Network Places, and the Recycle Bin. In Windows XP, the My Computer and My Network

FIG 2.2.3a windows 8 desktop

Places icons no longer display by default on the Desktop; however, you might want to add them. Instructions on how to add My Computer were given earlier in the section "The Start Menu"; you can select My Network Places in the same place you select My Computer to display on the Desktop.

2.2.4 Screen saver,

The screen saver option sets up an automatic screensaver to cover your screen if you have not been active for a certain period of time. Originally it was used to prevent burned monitors. Screen savers are now generally used for entertainment or to password-protect users' Desktops. The Screen Saver tab also gives you access to other power settings.

Windows comes with several screen savers. You can also create your own screen savers from personal pictures that you've saved on your computer, and there are screen savers available to download from the web.

Tip: In Windows press the **Windows key + L** to lock the computer if you're stepping away from the computer. This will still allow the screensaver, but prevents someone from accessing your computer.

To change the screensaver, perform the following steps:

1. Right-click the Desktop.

2. Choose Properties from the context menu.

3. Click the Screen Saver tab.

4. Choose 3D Flower Box. Click Preview to see the new screensaver. Move the mouse to cancel the screensaver and return to the Display Properties dialog box.

5. Click the OK button or the Apply button.

2.2.5 Fonts &color,

You can change the font in any part of Windows (for example, menus). Changing a Windows font does not change your program fonts.

1. Open Appearance Settings by clicking the **Start** button, clicking **Control Panel**, clicking **Appearance and Personalization**, clicking **Personalization**, and then clicking **Window Color and Appearance**. If the Appearance Settings dialog box is not displayed, at the bottom of the page, click **Open classic appearance properties**.

2. Click **Advanced**.

3. In the **Item** list, click the part of Windows where you want to change the font. For example, if you want to change the menu font, click **Menu** in the list.

4. In the **Font** list, click the font you want to use.

5. In the **Size** list, click the font size that you want.

6. In the **Color** list, click the font color you want.

7. Repeat steps 3 through 6 for each part of Windows where you want to change the font, its size, and its color, and then click **OK**.

2.2.6 Creating shortcuts to program groups

A shortcut is a computer desktop icon that enables a user to easily see and select a particular program or data object. The operating system comes with some shortcuts already visible on the desktop. A user can remove these or add new ones.

Creating a Shortcut to a Program or File

To create a shortcut on the desktop to a program or file, there are two possible methods to choose from.

Method 1

1. Right-click an open area on the desktop, point to **New**, and then click **Shortcut**.
2. Click **Browse**.
3. Locate the program or file to which you want to create a shortcut, click the program or file, click **Open**, and then click **Next**.

4. Type a name for the shortcut. If a **Finish** button appears at the bottom of the dialog box, click it. If a **Next** button appears at the bottom of the dialog box, click it, click the icon you want to use for the shortcut, and then click **Finish**.

Method 2

1. Click **Start**, point to **Programs**, and then right-click the program you want to create the shortcut to.
2. Click **Create Shortcut**.
3. The shortcut is now at the end of the Programs list. For example, if you created a shortcut to Microsoft Word, to find that program, click **Start**, and then point to **Programs**. You will find the shortcut, named "Microsoft Word (2)" (without the quotation marks), at the bottom of the Program list.
4. Drag the shortcut to the Desktop.

Creating a Shortcut to a Printer or Dial-Up Networking Connection

To create a shortcut on the desktop to a printer or Dial-Up Networking connection, follow these steps:

1. To create a shortcut to a printer, click **Start**, point to **Settings**, and then click **Printers**. To create a shortcut to a Dial-Up Networking connection, click **Start**, point to **Programs**, point to **Accessories**, and then click **Dial-Up Networking**.
2. Right-click the printer or **Dial-Up Networking** connection icon, drag it to an open area on the desktop, and then click **Create Shortcut(s) Here**.

Creating Shortcuts to Other Objects

To create a shortcut on the desktop to other objects (such as a folder or computer), follow these steps:

1. Use **My Computer** or **Windows Explorer** to locate the object to which you want to create a shortcut.
2. Right-click the object, and then click **Create Shortcut**.
3. Drag the new shortcut to an open area on the desktop.

2.3 System maintenance;

2.3.1 back up restoration,

Ensuring data recoverability involves performing a *backup* (normally to another type of medium) in addition to storing the file on the hard drive. This medium could be (for example) a floppy disk, another hard drive, a tape drive, a Zip drive, or CD-ROM.

If you have lost a single file (or all the files) on your hard drive, you will want to perform a restore. You need to have your backup files or tapes available and use the Windows backup utility to restore your files.

The Windows XP backup software is greatly improved over the old Windows NT backup software, and Windows Vista and Windows 7 have improved this process even more. Windows XP backup software picks up where its predecessor left off, allowing you to schedule regular automatic backups and to back up to nearly any medium you like (including, but not limited to, tape drives). Even though the tool is new, Microsoft has kept the name of ntbackup.exe, and supports all the old command line switches for backward compatibility.

The backup utility allows you to create a backup of all local files on your disk drives, as well as the system state. Open files, such as the Registry and system databases, cannot normally be backed up on your computer, but system state allows you to back up these files by using new file locking methods.

Each organization decides how often it needs to back up each of its computers. This decision is often based on the size and ease of use of the backup media and the value that the organization puts on its files. For example, the loss of a week's worth of invoice records might represent a large amount of revenue to a company, or the loss of a day's worth of rental records at a video store might put a substantial portion of the video store's inventory in jeopardy because they will not have a record of where their movies are. These types of costs are weighed against the cost of decent backup hardware. Some organizations back up important data once a week, once a day, or several times a day, depending on the perceived cost of data loss.

You start a typical backup by launching the Backup utility, which can be done in one of two ways on Windows XP:

- **Run** ntbackup.exe.

TIP: All options for the backup utility are available via the command line interface. To get a complete list of the options and their command line switches, type ntbackup.exe /? at a command prompt.

- **Choose Start >All Programs>Accessories>System Tools>Backup.**

For Windows 7, you can launch the Backup utility by choosing Start>Control Panel>Back Up Your Computer. Either method launches the backup utility.

The first time you launch the Backup utility on Windows XP, it launches in wizard mode, which can be used for backup, and will allow you to back up files using simplified or default settings.

TIP: If you don’t want to launch it in wizard mode, clear the Always Start in Wizard Mode check box in the Backup or Restore Wizard dialog box and then click the Cancel button or the Advanced Mode hyperlink. The next time you launch the backup utility, it will launch in advanced mode instead of in wizard mode. When the utility is in advanced mode, you can run the Backup, Restore, or ASR wizards. You can also choose the appropriate tabs to perform a manual backup or restore. The last tab available in the program is the Schedule Jobs tab, which is used to schedule automated backup jobs.

To schedule a basic backup of your system without using the wizard mode, follow these steps:

1. Choose Start➪All Programs➪Accessories➪System Tools➪Backup.

The Backup Utility dialog box should open.

2. If the Backup or Restore Wizard opens, deselect the Always Start in Wizard mode check box and then click the Advanced Mode link.

3. Click the Backup tab.

4. Select all the drives, folders, or files that you want to back up, as well as the System State, by clicking in the Selection boxes to the left of the names.

Backing up the system state backs up core OS files, including files that are open. For Windows 2000 and newer Windows OSes, this option includes

- COM+ Class Registration database
- Boot files, including the system files
- Registry

If you are backing up a server, the system state may include some or all of the following, depending on what Services are installed on the server:

- Certificate Services database
- Active Directory database
- SYSVOL directory
- Cluster service information
- IIS Metadirectory

System state backups are required to fully restore a computer to its original state and identity on the network. If you are concerned with the data and file system permissions only, you do not need to back up the system state.

5. Select a location to back up to and then click the Start Backup button.

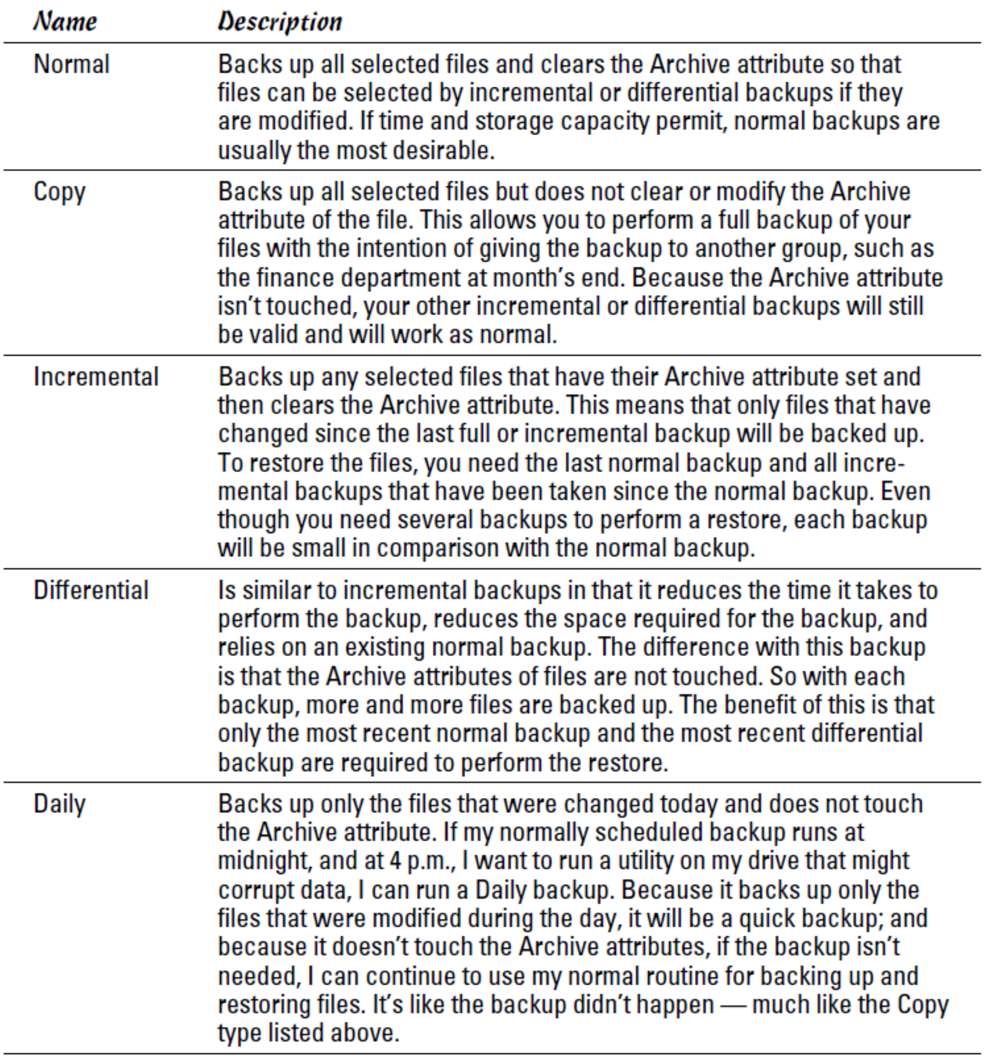
You can back up the files to another local drive or to a tape drive if there is one attached to the computer.

If you are saving to a file on a drive, the default extension for a backup file is .bkf.

6. In the Backup Job Information window, click the Advanced button to set the advanced options for the job.

The main items to be aware of are

- *Verify Data after Backup:* This option rewinds the tape or rereads the backup file and compares its contents with each file that was backed up. You can disable this option if you find that some files managed by third-party applications become corrupted during the verification process. This is not normally the case.
- *Disable Volume Shadow Copy:* Volume Shadow Copy is a service that takes a snapshot of all open files on your drive to allow them to be backed up. Some third-party applications might have problems with the Volume Shadow Copy process, so you have the option of disabling this feature, but disabling the Volume Shadow Copy process will prevent some open files from being backed up because the older file lock mechanisms will be attempted.
- *Backup Type:* You have five options, which are summarized below



Name	*Description*
Normal	Backs up all selected files and clears the Archive attribute so that files can be selected by incremental or differential backups if they are modified. If time and storage capacity permit, normal backups are usually the most desirable.
Copy	Backs up all selected files but does not clear or modify the Archive attribute of the file. This allows you to perform a full backup of your files with the intention of giving the backup to another group, such as the finance department at month's end. Because the Archive attribute isn't touched, your other incremental or differential backups will still be valid and will work as normal.
Incremental	Backs up any selected files that have their Archive attribute set and then clears the Archive attribute. This means that only files that have changed since the last full or incremental backup will be backed up. To restore the files, you need the last normal backup and all incremental backups that have been taken since the normal backup. Even though you need several backups to perform a restore, each backup will be small in comparison with the normal backup.
Differential	Is similar to incremental backups in that it reduces the time it takes to perform the backup, reduces the space required for the backup, and relies on an existing normal backup. The difference with this backup is that the Archive attributes of files are not touched. So with each backup, more and more files are backed up. The benefit of this is that only the most recent normal backup and the most recent differential backup are required to perform the restore.
Daily	Backs up only the files that were changed today and does not touch the Archive attribute. If my normally scheduled backup runs at midnight, and at 4 p.m., I want to run a utility on my drive that might corrupt data, I can run a Daily backup. Because it backs up only the files that were modified during the day, it will be a quick backup; and because it doesn't touch the Archive attributes, if the backup isn't needed, I can continue to use my normal routine for backing up and restoring files. It's like the backup didn't happen — much like the Copy type listed above.

7. Click OK.

8. In the Backup Job Information window that reappears, click the Schedule button.

You are prompted to save your backup selections into a BKS (backup selections) file.

9. Select a location, name the file, and then click Save.

This file can be stored anywhere on your drive, but for organizational purposes, I suggest that you save it in the same location as the BKF file.

Saving the backup selections file allows the utility to know what files are to be copied during each scheduled backup time. The BKS file can be loaded into the backup utility any time you want the same selections for a backup.

The Task Scheduler Service prompts you to enter your credentials.

The default Windows Task Scheduler Service is used when creating the scheduled automatic backup jobs that appear on the Schedule Jobs tab of the Backup Utility.

10. Provide the credentials of a user with the OS rights to perform a backup of the system.

This includes members of the Administrators or Backup Operators groups. The system uses the credentials you supply when it automatically starts the scheduled backup process.

11. Click OK.

You are presented with the standard options for the Scheduling Service.

OS rights are similar to file system permissions, but they grant a username the ability to perform an action that is not directly related to an object, such as a file. You assign rights using the Local Security Policy or an Active Directory Group Policy Object (GPO).

12. Select when you would like the backup to run and then click OK.

By default, backups create a summary log that lists exceptions or the files that were not backed up. After scheduling and running a backup, you can log onto the computer by logging on as the backup user account that was specified when scheduling the job (Step 10 in the previous instructions).You can then open the backup utility and choose Tools➪Report. This allows you to read the last ten backup logs.

Windows Vista has modified the backup process even further by integrating scheduling into it, as well as streamlining the file selection process. This has been done to make the entire process more user friendly

Restoring files from a backup

You should also become familiar with the steps required to restore those files. To restore files on your system without using the wizard mode in the Backup Utility, follow these steps:

1. Choose Start➪All Programs➪Accessories➪System Tools➪Backup.

The Backup Utility dialog box should open.

2. If the Backup or Restore Wizard opens, deselect the Always Start in Wizard ode check box and then click the Advanced Mode link.

3. Click the Restore and Manage Media tab.

This tab has two panes. The left pane is used to select and catalog backup files you want to restore from and to display the directory tree in a backup file; the right pane allows you to view information about backup files that have been cataloged and to select items that you want to restore. This dialog should already have a backup file cataloged, which will be the one that you created in Step 6 of the backup process.

If you need to import or catalog a backup file that was created on another computer, or that you have manually deleted from this window, right-click File in the left pane and choose Catalog File, locate and select the backup file that you want to work with, and then click OK.

4. Double-click the Backup Identification Label of the backup file that you want to work with.

5. Using the navigation controls in both panes, navigate through the list of files and folders that are found in the backup and select the files that you want to restore.

6. Select one of the three options for the Restore files to drop down menu.

• *Original location:* Restores folders and files to the same locations from which they were backed up.

• *Alternate location:* Restores folders and files to an alternate location, creating a duplicate of the directory structure that was used during the backup, but places the restored files in the directory specified in the Alternate Location text box. This option is useful when you do not want the current copies of the files overwritten.

• *Single folder:* Restores folders and files to the location specified in the Alternate Location text box. Does not maintain the original directory structure, but rather places all the files restored into the specified directory. This option is useful when you are looking for a few specific files that are buried or lost in a complicated directory structure.

7. Click Start Restore.

This opens the Confirm Restore dialog box, where you can modify advanced options. I will not explore these options in this book.

8. Click OK to start the restore.

The Restore Progress dialog box opens, displaying the status of the file restore. When this process is complete, Close and Report buttons (topright of the dialog box) appear.

9. Click Close.

The Restore process is now complete, and you can close the Backup Utility.

As with the backup process, the restore process of Windows Vista has been streamlined to make this process more user friendly.

Restoring your computer to a previous state

Minor and major disasters can require you to access a restore point to return your computer to working condition. The following instructions guide you through restoring your computer to a previous state by accessing a system restore point:

1. **Choose Start➪All Programs➪Accessories➪System Tools➪System Restore.**

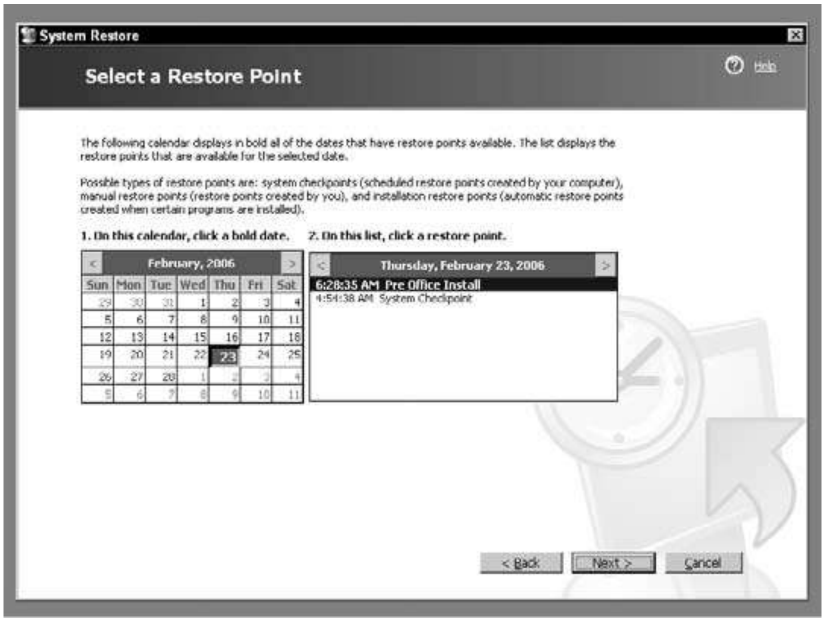
The System Restore Wizard (refer to Figure 3-3) gives you two options:

• Restore My Computer to an Earlier Time

• Create a Restore Point

2. **Select Restore My Computer to an Earlier Time and then click Next.**

The wizard presents you with a list of restore points, as shown in the fig below.



Select a Restore Point

The following calendar displays in bold all of the dates that have restore points available. The list displays the restore points that are available for the selected date.

Possible types of restore points are: system checkpoints (scheduled restore points created by your computer), manual restore points (restore points created by you), and installation restore points (automatic restore points created when certain programs are installed).

1. On this calendar, click a bold date.

February, 2006

Sun	Mon	Tue	Wed	Thu	Fri	Sat
29	30	31	1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	1	2	3	4
5	6	7	8	9	10	11

2. On this list, click a restore point.

Thursday, February 23, 2006

6:28:35 AM Pre Office Install
4:54:38 AM System Checkpoint

fig 2.3.1 a

3. **Select the appropriate restore point and then click Next.**

You see a warning you that you will lose recent changes on your system if you choose to restore.

4. **Click Next.**

Your system reverts to how it was configured at the restore point you chose, and your computer reboots.

2.3.2 Use of hardware diagnostic tools in system software,

Hard drives are complex mechanical and electrical devices. With platters spinning at thousands of rotations per minute, they also generate heat and vibration. All of these factors make hard drives susceptible to failure. In this section, you will learn some basic maintenance tasks that will keep your hard drives healthy, and for those inevitable instances when a hard drive fails, you will also learn what you can do to repair them.

Maintenance

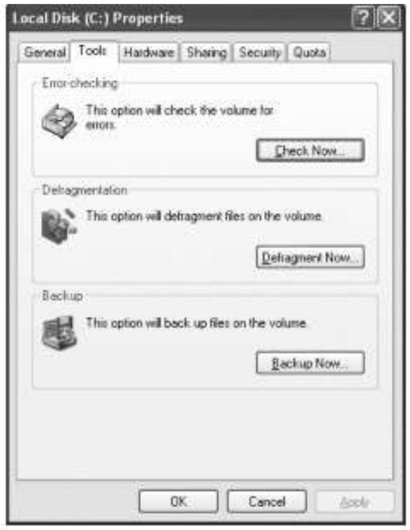
Hard drive maintenance can be broken down into two distinct functions: checking the disk occasionally for failed clusters, and keeping data organized on the drive so it can be accessed quickly.

2.3.2.1 Scandisk restoration

Individual clusters on hard drives sometimes go bad. There's nothing you can do to prevent this from happening, so it is important that you check occasionally for bad clusters on drives. The Tools used to perform this checking are generically called error-checking utilities, although the terms for two older Microsoft tools—ScanDisk and *CHKDSK* (pronounced "Checkdisk")—are often used. Microsoft calls the tool *Error-checking* in Windows XP/Vista/7. Whatever the name of the utility, each does the same job: when the tool finds bad clusters, it puts the electronic equivalent of orange cones around them so the system won't try to place data in those bad clusters.

Most error-checking tools do far more than just check for bad clusters. They go through all of the drive's filenames, looking for invalid names and attempting to fix them. They look for clusters that have no filenames associated with them (we call these *lost chains*) and erase them. From time to time, the underlying links between parent and child folders are lost, so a good error-checking tool checks every parent and child folder. With a folder such as C:\TEST\DATA, for example, they make sure that the folder DATA is properly associated with its parent folder, C:\TEST, and that C:\TEST is properly associated with its child folder, C:\TEST\DATA.

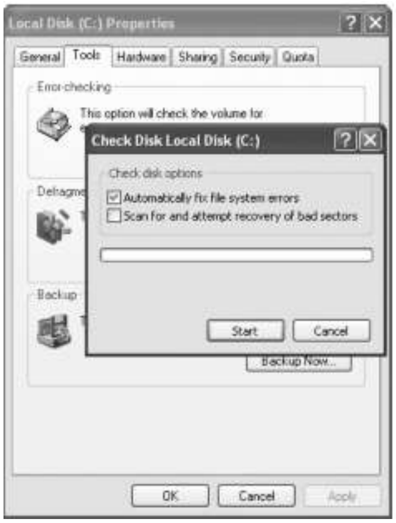
To access Error-checking on a Windows 2000/XP or Windows Vista/7 system, open My Computer/Computer, right-click the drive you want to check, and choose Properties to open the drive's Properties dialog box. Select the Tools tab and click the Check Now button (Figure 2.3.2 a) to display the Check Disk dialog box, which has two options (Figure 2.3.2 b). Check the box next to *automatically fix file system errors*, but save the option to *Scan for and attempt recovery of bad sectors* for times when you actually suspect a problem, because it takes a while on bigger hard drives.



This option will check the volume for errors.

This option will defragment files on the volume.

This option will back up files on the volume.



This option will check the volume for errors

☑ Automatically fix file system errors
☐ Scan for and attempt recovery of bad sectors

fig 2.3.2 b

Fig 2.3.2a

2.3.2.2 Defragmentation

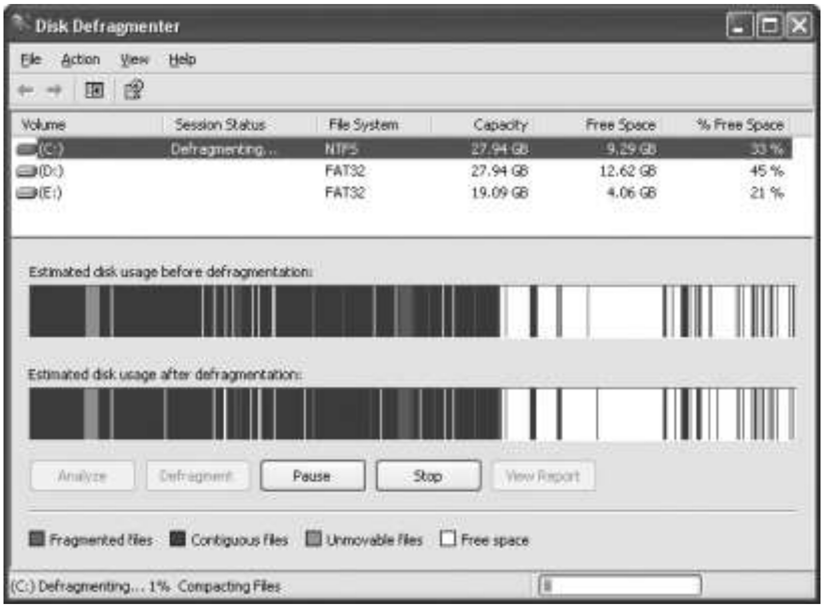
Disk defragmentation is the process of consolidating fragmented data on a volume (such as a hard disk or a storage device) so it will work more efficiently.

Fragmentation happens to a volume over time as you save, change, or delete files. The changes that you save to a file are often stored in a different place on the volume than the original file. This doesn't change where the file appears in Windows—only where the bits of information that make up the file are stored on the actual volume. Over time, both the file and the volume itself become fragmented, and your computer slows down as it has to look in different places to open a single file.

Disk Defragmenter is a tool that rearranges the data on your volume and reunites fragmented data so your computer can run more efficiently. In some versions of Windows, Disk Defragmenter runs on a schedule so you don't have to remember to run it, although you can still run it manually or change the schedule it uses.

Fragmentation of clusters can increase your drive access times dramatically. It is a good idea to *defragment*—or *defrag*—your drives as part of monthly maintenance. You access the defrag tool that runs with Windows 2000, XP, Vista, and 7, called Disk Defragmenter, the same way you access Error-checking—right-click A drive in My Computer/Computer And choose Properties—

except You click the Defragment Now Button on the Tools tab to open the Defragmenter (Figure 2.3.2 c).



Volume	Session Status	File System	Capacity	Free Space	% Free Space
(C:)	Defragmenting...	NTFS	27.94 GB	9.29 GB	33 %
(D:)		FAT32	27.94 GB	12.62 GB	45 %
(E:)		FAT32	19.09 GB	4.06 GB	21 %

(C:) Defragmenting... 1% Compacting Files

fig 2.3.2 c

2.4 Antivirus;

A computer *virus* is a small, deviously ingenious program that replicates itself to other computers, generally causing those computers to behave abnormally. Generally speaking, a virus's main function is to reproduce. A virus attaches itself to files on a hard disk and modifies those files. When the files are accessed by a program, the virus can infect the program with its own code. The program may then, in turn, replicate the virus code to other files and other programs. In this manner, a virus may infect an entire computer. When an infected file is transferred to another computer (via disk or modem download), the process begins on the other computer. Because of the frequency of downloads from the

Internet, viruses can run rampant if left unchecked. For this reason, antivirus programs were developed. They check files and programs for any program code that shouldn't be there and either eradicate it or prevent the virus from replicating. An antivirus program is generally run in the background on a computer, and it examines all the file activity on that computer. When it detects a suspicious activity, it notifies the user of a potential problem and asks the user what to do about it. Some antivirus programs can also make intelligent decisions about what to do.

The process of running an antivirus program on a computer is known as *inoculating* the computer against a virus.

To protect your computers and servers from viruses, it is essential that you have virus protection software installed. Simply, such software knows about the different viruses and can either remove the virus or remove files from your system that contain viruses.

You can choose from many different name brands of virus-protection software, each of which has its own benefits. Some of the popular names in virus protection are

✦ **McAfee:** www.mcafee.com

✦ **Norton/Symantec:** www.symantec.com/norton/index.jsp; www.
symantec.com/index.jsp

✦ **Panda Security:** www.pandasecurity.com

✦ **F-PROT:** www.f-prot.com

Each antivirus software product has its own benefits and features. For example, you might prefer the interface or usability of one product over another. Still, each product should offer similar features. When shopping for antivirus software, you should look for software that offers at least the following features:

✦ **Scheduled virus scans:** This is a great feature because you can have the virus scanning software scan the system in the middle of the night (when the system is not being used), and you do not have to physically perform the scan yourself. You may also choose what happens when a virus is found: say, attempt to remove the virus from the file, place the file in a quarantine area, or delete the file.

✦ **Real-time protection:** The virus protection software runs in memory all the time and scans any file that you open. The benefit of real-time protection is that you are protected from viruses between scan times. Be sure to have software that supports real-time protection and have the feature enabled.

✦ **Scheduled definition updates:** Virus definitions are what virus protection software uses to update its knowledge of viruses. Your virus protection software should have a feature that allows the definitions to be downloaded from its vendor site.

✦ **Scanning e-mail:** Many virus protection software versions support scanning e-mail messages as they arrive in your inbox. This is typical of virus protection software that runs on an e-mail server and you usually pay an annual subscription fee for the service.

When you perform a virus scan, your virus protection software knows only about the viruses as of the creation time of the software. This is a huge problem because new viruses appear every day.

To keep your software valid and to allow it to still be useful years after you purchase it, manufacturers use virus definitions as a way for the software to know the current list of viruses. The virus definitions can be updated online. So, even though your software might be two years old, you can keep it current.

It is critical that you update your virus definitions regularly, or your virus protection software won't know about any new viruses that are developed.

2.5 diagnostic tools;

When you are stumped by a computer problem, where do you turn? Try manuals, the Web, and training.

User/Installation Manuals consult the manuals that came with the hardware and software.

Internet/Web Resources Consult the websites of the companies that make the hardware and software. Updates and patches are often available for download, or the websites may offer knowledge bases of troubleshooting information and downloadable manuals as well as live forums for those with similar problems to discuss their issues.

Training Materials If you have taken a class pertaining to the hardware or software, consult the materials you received for that class.

A big part of being a successful technician is knowing what tools are appropriate to correct which problems. The following **diagnostic tools** and utilities are ones you should be comfortable with:

Task Manager Lets you shut down nonresponsive applications selectively in all Windows versions.

In Windows 2000/XP, it does much more, allowing you to see which processes and applications are using the most system resources. To display Task Manager, press Ctrl+Alt+Delete.

Task Manager appears immediately in Windows 9*x*; in Windows 2000/XP, you must click the Task Manager button to display it after pressing Ctrl+Alt+Delete. Use Task Manager whenever the system seems bogged down by an unresponsive application.

Dr. Watson This tool enables detailed logging of errors. Use it whenever you think an error is likely to occur (for example, when you're trying to reproduce an error).

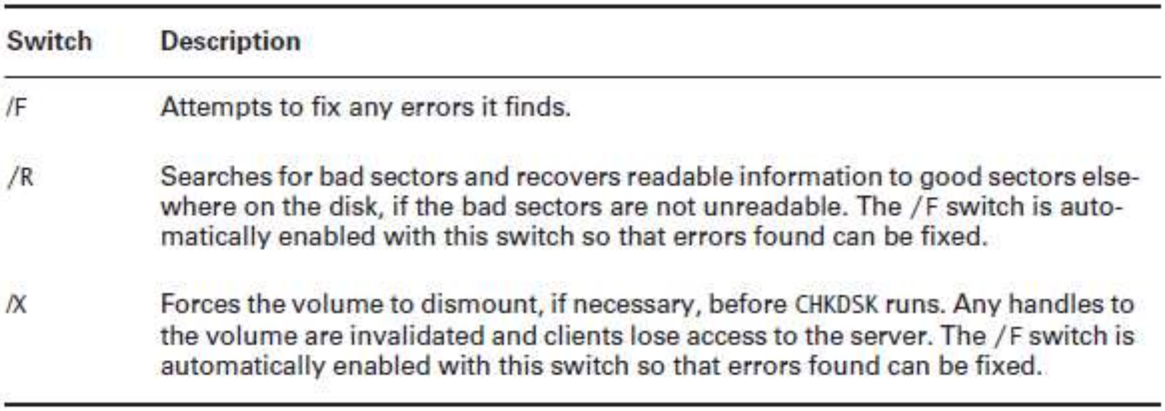
Event Viewer This tool enables you to see what's been going on behind the scenes in Windows NT/2000/XP. Use Event Viewer when you want to gather information about a system or hardware problem.

Device Manager As already mentioned, Device Manager shows you what hardware is installed and lets you check its status. Use this when a device is not functioning and you are trying to figure out why.

WinMSD Another name for System Information, the same utility you can select from the System Tools menu. (Running it at the Run command with WINMSD is an alternative.) WinMSD provides comprehensive information about the system's resource usage, hardware, and software environments. Use it when you need to gather information about the system.

Recovery CD Some computers that come with Windows preinstalled do not come with a full version of Microsoft Windows; instead they come with a Recovery CD that can be used to return the PC to its original factory configuration. The important thing to know about these Recovery CDs is that they wipe out all user data and applications. Use one only when you cannot restore system functionality in any less-drastic way.

CHKDSK One utility for checking the integrity of magnetic media that has been around since the dawn of the PC operating system, DOS that is, is CHKDSK. CHKDSK is run from a command prompt and scrubs the disk to varying degrees for surface-level and filesystem imperfections. The imperfections can even be corrected in many cases, if you request that they be. Table 2.5a lists the primary switches for CHKDSK and their descriptions. Switches can be specified in series and two of the switches imply the third switch without your explicitly specifying it.



Switch	Description
/F	Attempts to fix any errors it finds.
/R	Searches for bad sectors and recovers readable information to good sectors elsewhere on the disk, if the bad sectors are not unreadable. The /F switch is automatically enabled with this switch so that errors found can be fixed.
/X	Forces the volume to dismount, if necessary, before CHKDSK runs. Any handles to the volume are invalidated and clients lose access to the server. The /F switch is automatically enabled with this switch so that errors found can be fixed.

Table 2.5 a

2.6 Resolving hardware conflicts

When you install a new board in you PC (eg. sound card) you can get conflicts between the board and your existing hardware. These can manifest as the following behaviour of your PC:

- It runs noticeably slower
- It spontaneously reboots
- Other hardware stops working properly or at all
- It fails to enter hibernate mode
- It fails to Shutdown
- It will not boot, or
- It crashes.

These are almost never a symptom of a software fault.

There are a number of possible solutions for these issues:

1. **Update the drivers for the new hardware**
   Sometimes the drivers are faulty and can create the issues. We always advise this as it can resolve any possible software issues.
2. **Move the card to a different slot in your PC**
   The card will be installed into a particular PCI slot in your PC. Just move it to a different slot and see if the problems are resolved. No other changes are needed (ie drivers do not need to be reinstalled).

3. **Remove other cards from your PC**
   The issue can be caused by conflicts between two different cards. Try removing other cards and see if this resolves the issue. Sometimes just replacing with a card by a different manufacturer can solve the issue. Also you can try moving the other card to a different slot as 2) above.
4. **Disable On board Devices**
   some computer owners/technicians resolve issues by disabling the on board sound card in their PC. The sound card is not needed for the running of most of our telephony software. You can also try other on board devices.
5. **Update the BIOS on your motherboard**
   The motherboard in all PCs has controlling software called BIOS. The software can have faults and create the problems. The web-site for the manufacturer of your motherboard will normally have downloads for the new BIOS and instructions on the update process. Please note this process can damage your PC so be careful and following the instructions carefully.
6. **Try the card in a different PC and check if it works correctly there.**
   Please note by different we mean a different motherboard and preferably manufacturer of the other components. Most likely PCs from the same shop will use the same components and have the same issue.
7. **Try a different card**
   Exchange the card for a different model/revision or for a totally different card by a different manufacturer.

As you see many of these options require technical expertise so please be careful. Notably when opening your PC be sure to earth yourself to prevent static damage to boards.

Chapter Review Questions

1. Differentiate between AC and DC power and state the advantages and disadvantages of each.
2. What does VGA stand for and where is a VGA cable utilized?
3. Compare and contrast HDMI and co-axial cables.
4. What are the differences between primary and secondary memory?
5. What are computer drivers and what are their functions?
6. What is disk partitioning and what types of partitions exist?
7. Discuss the different types of RAM.
8. What is a screen saver and what are its uses, past and present?
9. What are the procedures for restoring backup on windows XP?
10. What is a computer virus and what are the different types of computer threats?

Chapter 3: Configuration Management:

Chapter Learning Objectives: *By the end of this chapter you should appreciate* Configuration Management, basic concepts of configuration management, the importance of The configuration management database (CMDB), registration of configuration items, benefits to IT service management, and the configuration manager.

3.1 Basic concepts of configuration management.

Configuration management (CM) is the detailed recording and updating of information that describes an enterprise's hardware and software. Such information typically includes the versions and updates that have been applied to installed software packages and the locations and network addresses of hardware devices. Special configuration management software is available. When a system needs hardware or software upgrade, a computer technician can accesses the configuration management program and database to see what is currently installed. The technician can then make a more informed decision about the upgrade needed.

An advantage of a configuration management application is that the entire collection of systems can be reviewed to make sure any changes made to one system do not adversely affect any of the other systems

Configuration management is also used in software development, where it is called Unified Configuration Management (UCM). Using UCM, developers can keep track of the source code, documentation, problems, changes requested, and changes made.

It is essential to have a detailed knowledge of your organization's IT infrastructure in order to make best use of it. The main task of Configuration Management is to keep an up-to-date record of all the components in the IT infrastructure configuration and the interrelations between them.

This is not a simple task and requires the cooperation of the people managing other processes, in particular **Change Management** and **Release Management**.

The main objectives of **Configuration Management** are:

- Providing accurate and reliable information to the rest of the organization about all the components of the IT infrastructure.

- Keep the **Configurations Database** up-to-date:
  - Up-to-date records of all **CIs**: identification, type, location, status, etc.
  - Interrelations between **CIs**.
  - Services provided by each **CI**.
- Serve as a support to the other processes, in particular to **Incident Management, Problem Management** and **Changes Management**.

The benefits of correct **Configuration Management** include, among other things:

- **Faster problem resolution**, thus giving better quality of service. A common source of problems is the incompatibility between different **CIs**, out-of-date drivers, etc. Having to detect these errors without an up-to-date **CMDB** can considerably lengthen the time taken to solve a problem.
- **More efficient Change Management**. It is essential to know what the prior structure is in order to design changes that do not produce new incompatibilities and/or problems.
- **Cost Reduction**. Detailed knowledge of all the elements of the configuration allows unnecessary duplication to be avoided, for example.
- **Control of licenses**. It is possible to identify illegal copies of software, which could pose risks for the IT infrastructure such as viruses, etc., and non-compliance with legal requirements that may have a negative impact on the organisation.
- **Greater levels of security**. An up-to-date **CMDB** allows vulnerabilities in the infrastructure to be detected, for example.
- **Faster restoration of service**. If you know all the elements of the configuration and how they are interrelated, recovering the live configuration will be much easier and quicker.

The main activities difficulties in **Configuration Management** are:

- **Incorrect planning**: it is essential to programme the necessary activities correctly to avoid duplications or mistakes.
- **Inappropriate CMDB structure**: keeping an excessively detailed and exhaustive configuration database up-to-date can be a time-consuming process requiring too many resources.

- **Inappropriate tools**: it is essential to have the right software to speed up the data entry process and make the best use of the **CMDB**.
- **Lack of Coordination between Change and Release Management** making it impossible to maintain the **CMDB** correctly.
- **Lack of organization**: it is important for there to be a correct assignment of resources and responsibilities. Where possible, it is preferable for **Configuration Management** to be undertaken by independent specialist personnel.
- **Lack of commitment**: the benefits of **Configuration Management** are not immediate and are almost always indirect. This can lead to a lack of interest on the part of management and consequently a lack of motivation among the people involved.

Configuration Items: both the components of IT services and the services these provide are configuration items. For example:

- Hardware devices such as PCs, printers, routers, monitors, etc. and their components: NICs, keyboards, CD drives, etc.
- Software: operating systems, applications, network protocols, etc.
- Documentation: manuals, service level agreements, etc.

In short, all the components that have to be managed by the IT organization.

Configuration Management Database: this database must include:

- Detailed information about each configuration item.
- Interrelations between the different configuration items, such as "parent-child" relationships, or logical and physical interdependencies.

The **CMDB** is not just a list of the stock or parts. It should give a global view of the organization's IT structure.

The main activities involved in **Configuration Management** are:

Planning: to determine the objectives and strategies of **Configuration Management**.

Classification and Recording: the **CIs** have to be recorded according to the predefined scope, depth and naming conventions.

Monitoring and Control: the **CMDB** must be monitored to ensure that all authorised components are correctly recorded and know their current status.

Performing audits: to ensure that the information stored in the **CMDB** matches the real configuration of the organization's IT structure.

Preparing reports: to assess the performance of **Configuration Management** and provide vitally important information to other areas of IT infrastructure.

3.2 The configuration management database (CMDB)

A configuration management database (CMDB) is a database that contains all relevant information about the components of the information system used in an organization's IT services and the relationships between those components. A CMDB provides an organized view of data and a means of examining that data from any desired perspective. Within this context, components of an information system are referred to as *configuration items* (CI). A CI can be any conceivable IT component, including software, hardware, documentation, and personnel, as well as any combination of them. The processes of configuration management seek to specify, control, and track configuration items and any changes made to them in a comprehensive and systematic fashion.

The IT Infrastructure Library (ITIL) best practices standards include specifications for configuration management. According to ITIL specifications, the four major tasks of configuration management are:

- Identification of configuration items to be included in the CMDB
- Control of data to ensure that it can only be changed by authorized individuals
- Status maintenance, which involves ensuring that current status of any CI is consistently recorded and kept updated
- Verification, through audits and reviews of the data to ensure that it is accurate.

A best practice is a technique or methodology that, through experience and research, has proven to reliably lead to a desired result. A commitment to using the best practices in any field is a commitment to using all the knowledge and technology at one's disposal to ensure success. The term is used frequently in the fields of health care, government administration, the education system, project management, hardware and software product development, and elsewhere.

Further reading: *Configuration Management - Overview*. http://itil.osiatis.es/ITIL_course/it_service_management/configuration_management/overview_configuration_management/overview_configuration_management.php

Research topic: discuss the benefits of IT service management and the definition and functions of the configuration manager

Chapter Review Questions

1. What is configuration management and what are its objectives?
2. What is a configuration item?
3. ITIL is the acronym for what organization and what are the functions of the organization?
4. What are the benefits of correct Configuration Management?
5. What is CMDB and what are its functionalities?
6. What is a best practice technique?

Chapter 4: IT Change Management

Chapter Learning Objectives: *By the end of this chapter you should appreciate* IT Change Management, possible problems associated with change management, roles and responsibilities associated with change management procedures and review and audit in change management.

4.1 Introduction to change management

Change management is a formal process used to ensure that changes to a product or system are introduced in a controlled and coordinated manner (as defined by ISO 20000).The objective of Change Management is to ensure that standardized methods and techniques are used for efficient and prompt handling of IT changes, in order to prevent change-related incidents. It is supposed to ensure that changes are made in such a way to minimize negative impact on the delivery of services to users and clients.

The main goal of **Change Management** is for all the changes that need to be made to IT infrastructure and services to be performed and implemented correctly by ensuring standard procedures are followed.

Change Management must work to ensure that changes:

- Are justified.
- Are carried out without jeopardizing IT service quality.
- Are properly recorded, classified and documented.
- Have been carefully tested in a test environment.
- Are recorded in the **CMDB**.
- Can be undone by running back-out plans if the system functions incorrectly after implementation.

The main benefits of proper change management are:

- The number of potential incidents and problems associated with each change is reduced.
- If the change has a negative impact on the IT structure, the process of returning to a stable configuration is relatively quick and simple.

- The number of back-outs needed is reduced.
- Changes are better received and the tendency to resist change is reduced.
- The true costs associated with the change are evaluated and it is therefore easier to assess the true return on the investment.
- The **CMDB** is kept properly up-to-date. This is essential if all other IT processes are to be managed correctly.
- Standard change procedures are developed allowing rapid updates to non-critical systems.

4.2 Possible problems

Implementing an appropriate change management policy can also run into serious difficulties:

- The various departments concerned must accept the authority of **Change Management** over issues relating to the change, independently from whether the change is made to solve a problem, improve a service or adapt the system to legal requirements.
- Established procedures are not followed, and in particular, the information on **CIs** is not updated properly in the **CMDB**.
- The people responsible for **Change Management** lack an in-depth knowledge of the organization's activities, services, needs and IT structure, making them unable to perform their tasks adequately.
- Change management personnel do not have the right software tools to monitor and document the process properly.
- There is insufficient commitment on the part of top management to implement the associated processes rigorously.
- Excessively restrictive procedures are adopted, getting in the way of improvements, or alternatively, the change process is trivialized, resulting in insufficient stability for quality of service to be ensured.

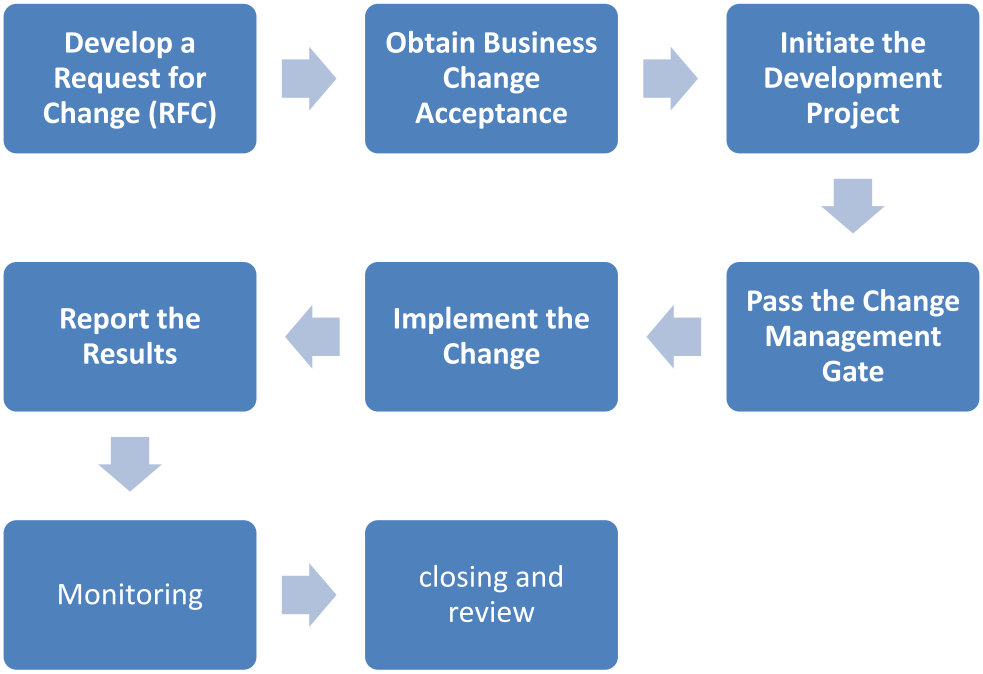
4.3 Roles and responsibilities,

Change Manager: the person responsible for the change process and as such, he/she is the person ultimately responsible for all the tasks assigned to **Change Management**. In large organizations the Change Manager may have a team of specific advisors for each of the various areas.

Change Advisory Board (**CAB**): this is an internal body, chaired by the **Change Manager**. It mainly comprises the representatives of the main IT services management areas. However, in some cases it may also include:

- External consultants.
- Representatives of user groups.
- Representatives of the main hardware and software providers.

4.4 change management procedures


Develop a Request for Change (RFC)
Obtain Business Change Acceptance
Initiate the Development Project
Pass the Change Management Gate
Implement the Change
Report the Results
Monitoring
closing and review

4.5 Scope of Change Management

In principle, all non-standard changes must be considered to fall within the purview of **Change Management**. However, it is sometimes impractical to manage all changes this way.

The scope of **Change Management** must parallel that of **Configuration Management**: all changes affecting **CIs** included in the **CMDB** inventory must be correctly supervised and recorded.

In a similar way to when implementing **Configuration Management**, where it is advisable to establish "reference configurations" as means of simplifying the process (consisting of standard packages of hardware and software, for example, a reference PC with a predefined set of hardware and software components), it is important to create changes processes with protocols defined and authorized in advance, for example, in order to make changes to the reference configurations just alluded to.

These standard change protocols need to be drawn up carefully, but once defined they allow for more rapid and efficient management of small changes or those with a low impact on the IT organization.

4.6 Review and audit

At least once each year an audit of the CMP should be conducted to assure that all change documentation is maintained and available. Every change approval document should be examined to assure that the proper signatures are in place and that the results of the implementation are properly documented.

Further reading: *Change Management - Overview*. (n.d.). Retrieved from http://itil.osiatis.es/ITIL_course/it_service_management/change_management/overview_change_management/overview_change_management.php

Chapter Review Questions

1. What is change management and what are its goals?
2. Discuss the various pitfalls of change management implementation?
3. What are the roles of a change manager and the change advisory board in change management?

CASE STUDY

The customers and suppliers of "Cater Matters" are making increasing use of the company's online services to manage ordering and the supply chain.

Although it basically meets the needs of the business, the currently implemented system was not designed to support a high level of activity. Both Availability Management and Capacity Management have reported inadequacies in the process and the risk of future bottlenecks if the current rate of growth continues.

Moreover, the company's management has decided to bolster its online presence and offer customers higher levels of service in order to build its market share.

This all requires a substantial change in both the hardware and software driving the company's online services, and the connection with the organization's internal management software (ERP-enterprise resource planning).

The company's management therefore raised an RFC and submitted it to Change Management. The objectives of the RFC were:

- To increase the capacity of the company's web servers in order to enhance connectivity and response capacity.
- To develop a series of Web Services permitting:
    - Direct integration of the online ordering system with the company's ERP system.
    - Tracking of the whole ordering process.
    - Management of the whole supply chain remotely in conjunction with suppliers.
- To redesign the website to enhance usability and optimize it for search engine indexing.

After recording the RFC:

- The request is given the "accepted" status and provisionally assigned normal priority and high impact.
- A meeting of the CAB is called, and the people in charge of e-commerce and web programming are asked to attend.

- A preliminary evaluation of the project is requested from the outside consultant who supervised the whole implementation process for the current system.

Prior to the CAB's meeting the Change Manager, in close coordination with Capacity, Availability, Financial and Service Level Management, and top management and project management, prepares:

- An initial evaluation of the costs and necessary resources.
- An evaluation of the impact of the changes on the IT infrastructure.
- A preliminary Gantt chart of the process.
- A survey so that the Service Desk can sound out customers' opinions about the possible changes.

After weighing up the documentation submitted and the organization’s business strategy, the CAB approves the change, and:

- Finalizes the schedule for the change.
- Assigns the internal and external resources needed.
- Develops a plan allowing for the temporary coexistence of both online systems to ensure continuity of service. This will involve:
    - Duplication of the whole web structure: new servers will be bought so that the old ones can continue providing continuous service and are immediately available for a possible back-out.
    - "Translation" applications will be developed so as to enable the old databases to be kept up-to-date in order to avoid the loss of data in the event of a back-out.
- Configuration Management is informed about all the CIs affected by the change.
- The same consultancy that implemented the current system is asked to perform an external audit on the whole process.
- All the information necessary for Version Management to be able to start the testing and implementation process is prepared.

After the change is implemented, in conjunction with "Service Support" and "Service Delivery",Change Management:

- Confirms the change is successful:
    - The new system has sufficient capacity to provide the envisaged levels of service and availability.
    - The new system works without apparent errors.
    - Customers and suppliers perceive the change as an improvement in service delivery.
    - Productivity has improved.
- A check is made to ensure everything has been recorded in the CMDB correctly.
- The process is evaluated.
- The change is closed.

Chapter 5: The Help Desk

Chapter Learning Objectives: By the end of this chapter you should appreciate the role of the help desk, value added functions of the help desk, data recording and usage, factors influencing help desk design, types and features of help desks, staffing of the help desk.

A help desk is a place that a user of information technology can call to get help with a problem. In many companies, a help desk is simply one person with a phone number and a more or less organized idea of how to handle the problems that come in. In larger companies, a help desk may consist of a group of experts using software to help track the status of problems and other special software to help analyze problems (for example, the status of a company's telecommunications network).

Some common names for a help desk include: Computer Support Center, IT Response Center, Customer Support Center, IT Solutions Cetnter, resource Center, Information Center, and Technical Support Center, service desk.

5.1 The role of the help desk,

Successful IT departments ensure not only that they are good at solving problems, but that they provide great customer service to their clients. Skilful customer service is essential to maintain a good impression of your helpdesk, and hence your IT department in general. So, the role of the **IT** Helpdesk is twofold:

1. A means to report, manage and resolve problems and issues identified by customers and
2. A marketing tool for your IT department or business.

How do you get both these roles right in order to provide complete or near complete customer satisfaction?

You need to provide excellent problem management by providing your **IT Helpdesk** with the tools and training required to do their job effectively and efficiently. You also need to equip the *helpdesk* technicians/analysts with the correct technical training and customer service training to carry out their roles to the best of their ability.

Problem Management – You will need to provide the appropriate tools and procedures for your *Helpdesk* personnel: Telephony and ACD (Automatic Call Distributor), CTI (Computer Telephony Integration), ***Helpdesk Software*** (for problem and change management) and documented policies and procedures are just some of the most important areas that need to be implemented and adhered to.

Customer Service – Ensure all Helpdesk personnel have good customer service skills and have appropriate training in how to manage their customer: from efficient call handling, through escalation procedures to dealing with irate customers.

Helpdesk Training

This should involve the use of a combination of in-house training, computer based training and classroom training for both new members of your **Helpdesk** team, and also for ongoing training requirements identified from particular circumstances or as a result of a performance appraisals or service level reviews.

Specific self-study courses available for the Helpdesk include the following:

- Customer Service Training – Includes training in the following areas: Calming Upset Customers, Customer Satisfaction and Quality Customer Service.
- CRM Training – Customer Relationship Management Training covering Fundamentals of CRM, Implementing CRM and eCRM.
- Call Centre Training – Covers Managing an Inbound Call Centre, Measuring Quality and Performance and Managing and Motivating Your Staff.

For the Helpdesk Manager the following computer based training is available:

- Team Leadership Training – covering Working Together, manage Your Mind, Manage Your Words, Manage the Unspoken and Putting Diversity to Work.
- Team Development Training – includes Effective Meeting Skills, Increasing Employee Productivity, Mentoring, Team Leadership, Team Problem Solving and Working Together.

- Successful Management Training – includes Excellence in Supervision, Project Management, Giving & Receiving Feedback, Managing Disagreement and Supreme Teams.

So, with the right tools and training, your Helpdesk staff will be able to provide a consistent and efficient service to their customers.

5.2 Value added functions of the help desk,

The activities of the **Service Desk** can include almost all aspects of IT Services Management in one way or another. However, its main function is that of managing relationships with customers and users, keeping them informed about all the processes of interest to them.

Some of the key functions a **Service Desk** should offer are:

Incident Management

Although managing incidents in full requires the collaboration of other departments and staff, the **Service Desk** must be able to provide a first line of support to help resolve interruptions to service and/or service requests from customers and users.

Its specific tasks include:

- Logging and monitoring each incident.
- Checking that the support service required is included in the associated **SLA(service level agreement)**.
- Tracking the escalation process.
- Identifying problems.
- Closing the incident and obtaining confirmation from the customer.

Information Centre

The **Service Desk** should be the main source of information for customers and users, informing them about:

- New Services.
- New releases to correct errors.
- Compliance with the **SLAs**.

This direct contact with customers should also be used to identify new business opportunities, and to assess customers' needs and their level of satisfaction with the service they are given.

The **Service Desk** is ideally positioned to provide inside information on all the IT service management processes. For it to do so, however, it is essential that it log all interactions between users and customers properly.

Supplier relations

The **Service Desk** is also responsible for relations with external suppliers providing maintenance services.

In order to offer a high quality service, it is essential that there be close links between external maintenance providers and **Incident Management**. This should be channeled through the **Service Desk**.

5.3 Factors influencing help desk design,

The Service desk is "the" point of contact between the IT organization and customers and users. It is therefore essential that:

- It be readily accessible.
- It offers a uniform service of consistent quality.
- It keeps users regularly informed and logs all interaction with them.
- It provides support for the business.

To achieve these goals an appropriate physical and logical structure is needed.

Logical structure

The members of the **Service Desk** team must:

- Be familiar with the protocols for interaction with customers: scripts, checklists, etc.
- Be equipped with software tools they need to log their interactions with users.
- Know when to escalate incidents to higher levels or contribute to discussions on the compliance with **SLAs**.
- Have the relevant knowledge bases at their fingertips so as to give a better service to users.
- Receive training on the company's products and services.

Physical structure

The structure of the **Service Desk** opted for will vary depending on the service needs (global, local, 24/7, etc.).

There are three basic formats:

- Centralized
- Distributed
- Virtual

The main characteristics of each format are described below:

Centralized Service Desk

In this case all contact with users is channeled through a single central structure.

The main advantages are:

- Costs are reduced.
- Resources are optimized.
- Management is simplified.

However, this approach may have significant drawbacks when:

- Users are spread across several geographical locations, with different languages, products and services.
- Maintenance services need to be delivered on site.

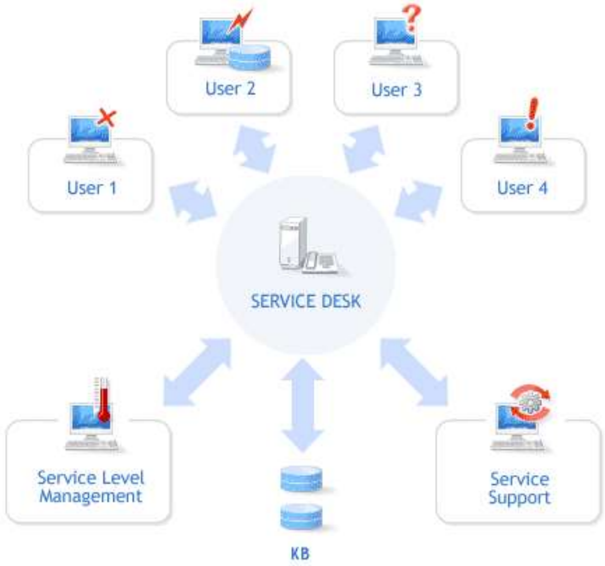


fig 5.4a

Distributed Service Desk

This is the structure traditionally used when the company offers services at different geographical locations (whether these are cities, countries or continents). The advantages are clear in these cases. However, geographically distributing the Service Desks in this way can entail serious difficulties:

- It is generally more expensive.
- Managing and monitoring the service is more complicated.
- It is more difficult for data and knowledge to flow between the different Service Desks.

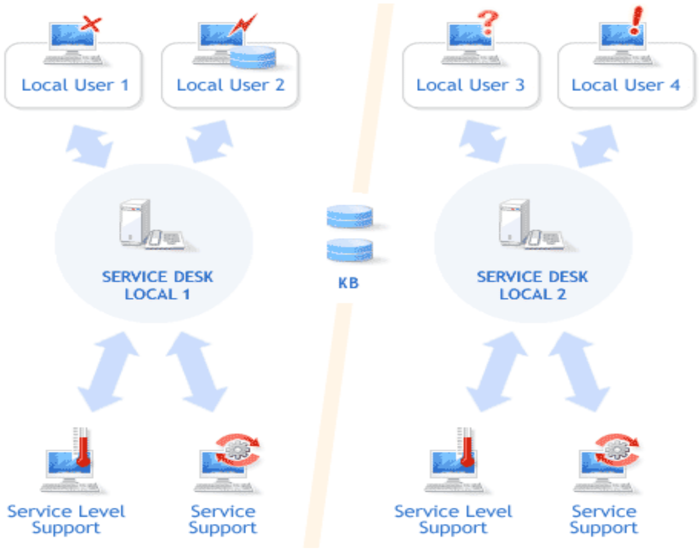


fig5.4b

Virtual Service Desk

Thanks to high speed communications networks, the geographical location of the Service Desk can nowadays be irrelevant.

The main aim of a virtual service desk is to utilize the advantages of both centralized and distributed service desks.

In a virtual **Service Desk**:

- Knowledge is centralized.
- Unnecessary duplication is avoided, with the consequent cost savings.
- A "local service" can be offered without incurring extra costs.
- The quality of service is uniform and consistent.

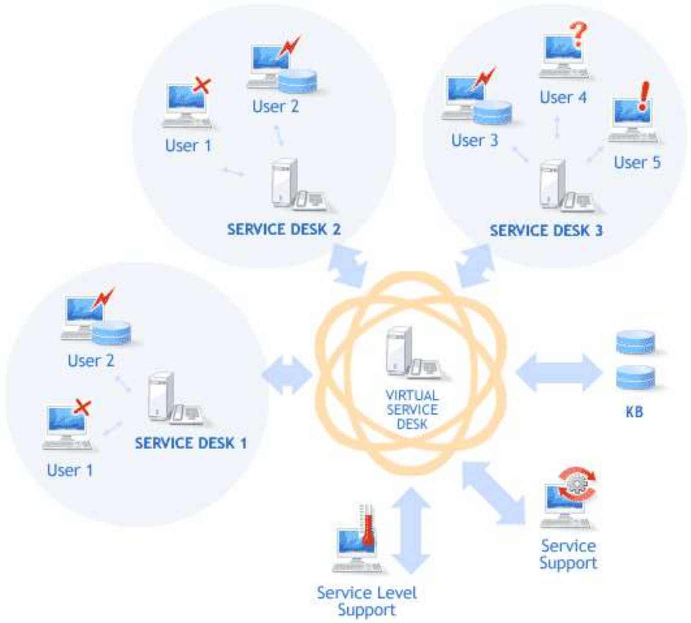


Fig 5.4c

5.4 Staffing of the help desk

A company's brand image can depend to a large extent on the quality of service given by its Service Desk.

We have all endured frustrating experiences dealing with large companies that promise high quality, round the clock support, and when it comes to the crunch, turn out to have a contact center with staff who are poorly trained, if not downright rude.

"Your Service Desk's success is your company's success" and it depends to large degree on the people in the team. It is therefore essential to establish strict selection and training protocols for them.

Ideally, the Service Desk staff should:

- Share the organization’s customer care philosophy.
- Deal with customers in a way that is correct and polite, using language the customer can understand.

- Have an in-depth knowledge of the services and products offered.
- Understand customers' needs and redirect them, if necessary, to the experts in question.
- Control all the technological tools available to them in order to offer a high quality service.
- Be able to work as a team.

The training they are given should relate to all these aspects and not be limited to building their technology skills.

It is also essential for the management to be committed to:

- Close monitoring of the services delivered, particularly as regards their effectiveness and performance.
- Continuous support to the service desk team in its difficult task of dealing directly with customers.
- Team work.

Chapter Review Questions

1. Define the term help desk with respect to the IT sector.
2. What are the roles of a helpdesk?
3. What essential training should a help desk manager go through?
4. Discuss the key functions of a service desk.
5. What are the essential characteristic of a good help desk?
6. Discuss the three basic physical formats of a service desk?
7. What are the essential characteristics of effective service desk staff?

Chapter 6: Incident and Problem Management:

Chapter Learning Objectives: By the end of this chapter you should appreciate the working of Incident and Problem Management, the Incident Management Process, First line incident support, Problem control and prevention

6.1 The Incident Management Process,

The aim of **Incident Management** is to resolve any incidents causing an interruption of service in the quickest and most effective way possible.

Incident Management should not be confused with **Problem Management**, as unlike the latter, it is not concerned with finding and analyzing the underlying causes of a particular incident but solely with restoring service. Nevertheless, there is obviously a strong interrelationship between them.

The main objectives of **Incident Management** are:

- Detecting any alterations in IT services.
- Logging and classifying these alterations.
- Assigning personnel charged with restoring service, as defined in the relevant **SLA**.

This activity requires close contact with users, which means that the **Service Desk** needs to play a central role.

The diagram below summarizes the incident management process:

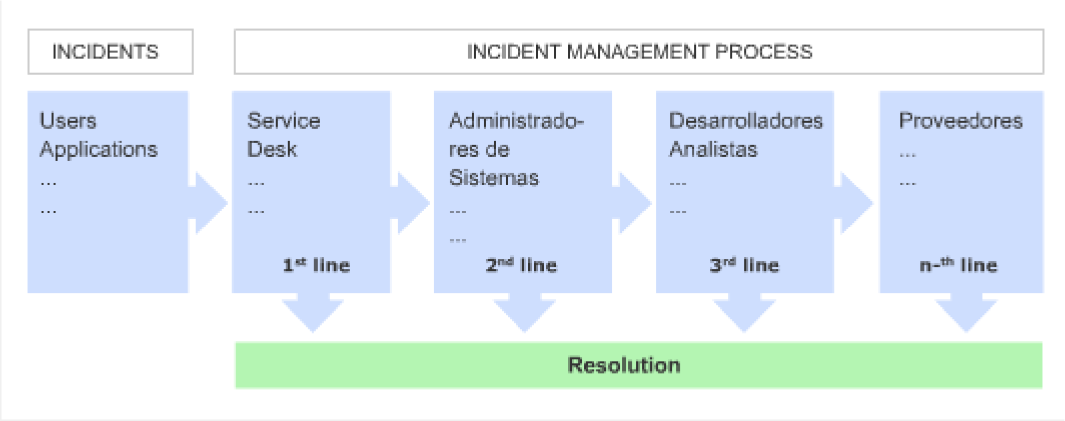


Fig 6.1a

Although the concept of an incident is naturally associated with a malfunctioning of the hardware and software systems, the ITIL® Service Support book defines an incident as:

“*Any event which does not form part of the standard operation of a service and which causes, or may cause, an interruption or a reduction in service quality*."

Thus, almost any call to the **Service Desk** may be classified as an incident. This includes **Service Requests**, such as asking for new licenses, changing access to information, etc. provided these services are considered standard.

Any change requiring a modification to the infrastructure is considered **not** to be a standard service and requires the initiation of a Request for Change**(RFC)**, which should be handled in accordance with the principles of **Change Management**.

The main benefits of correct **Incident Management** include:

- Improved user productivity.
- Fulfillment of the levels of service agreed in the **SLA**.
- Greater process control and service monitoring.
- Optimization of the resources available.
- A more accurate **CMDB**, as incidents affecting configuration items are logged.
- And, in particular: improved general customer and user satisfaction.

On the other hand, incorrect **Incident Management** may have adverse effects, such as:

- Reduced Service Level.
- Valuable resources are squandered: too many people, or people of the wrong level, working simultaneously on resolving the incident.
- Valuable information on the causes and effects of incidents of use for future restructuring or upgrades is lost.
- Customers and users are unsatisfied as a result of the poor and/or slow resolution of their incidents.

The main difficulties when implementing **Incident Management** may be summarized as:

- The envisaged procedures are not followed and incidents are resolved without logging or are escalated unnecessarily and/or the pre-defined protocols are omitted.
- There is no operating margin allowing peaks in incidents to be managed, so they are not adequately recorded and the correct operation of the classification and escalation protocols is hindered.
- The service quality levels and products supported are not well defined. This can mean that requests not included in the services agreed beforehand with the customer are processed.

Classifying the Incident

It is commonplace for multiple incidents to exist in parallel, making it necessary to define levels of priority when resolving them.

The level of priority is essentially based on two parameters:

- **Impact:** this determines the importance of the incident depending on how it affects business processes and/or the number of users affected.
- **Urgency:** depends on the maximum delay the customer will accept for the resolution of the incident and/or the level of service agreed in the SLA.

Secondary factors, such as the expected resolution time and the resources necessary, also need to be taken into account: "simple" incidents will be dealt with as soon as possible.

Depending on the priority, the necessary resources will be assigned to resolve the incident.

The incident's priority may change during its lifecycle. For example, a temporary solution may be found which restores acceptable levels of service and allows the closure of the incident to be delayed without serious repercussions.

It is worth establishing a protocol to determine the incident's priority in the first instance. The graphic below shows a possible "priority chart" depending on the urgency and impact of the incident:

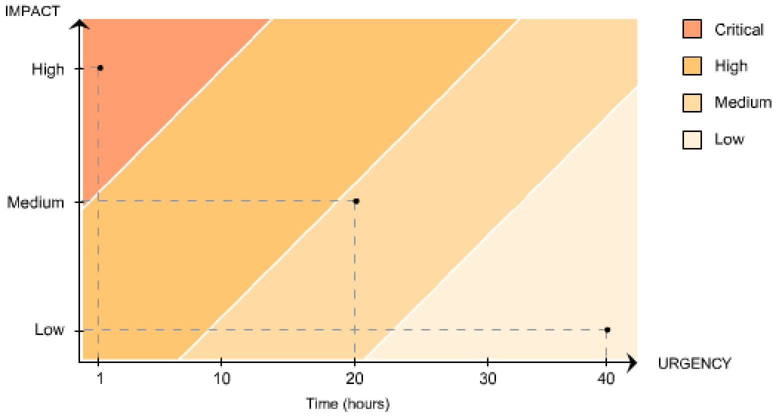


fig 6.1b

Escalation and Support

It frequently happens that the **Service Desk** is unable to resolve the incident in the first instance and so has to turn to a specialist or superior who can make decisions that are outside the Service Desk's area of responsibility. This process is referred to as **escalation**.

Basically there are two different types of escalation:

- **Functional escalation**: The support of a higher level specialist is needed to resolve the problem.
- **Hierarchical escalation:** A manager with more authority needs to be consulted in order to take decisions that are beyond the competencies assigned to this level, for example, to assign more resources in order to resolve a specific incident.

The escalation process can be summarized graphically as follows:

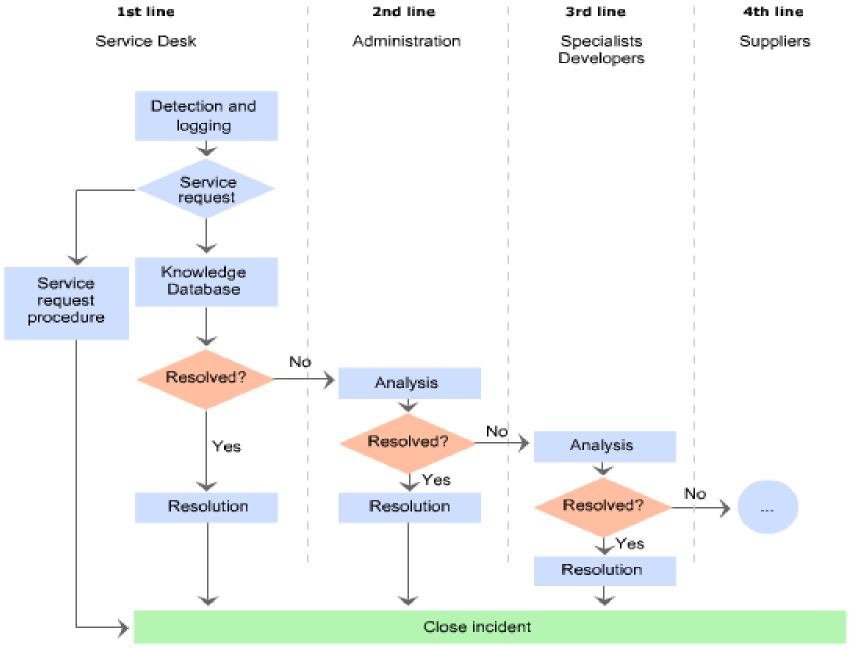


Fig 6.1 c

* Escalation may include more levels in larger organizations, or alternatively, consist of different levels in SMEs.

Incident Management

Process

The diagram below shows the processes involved in proper **Incident Management**:

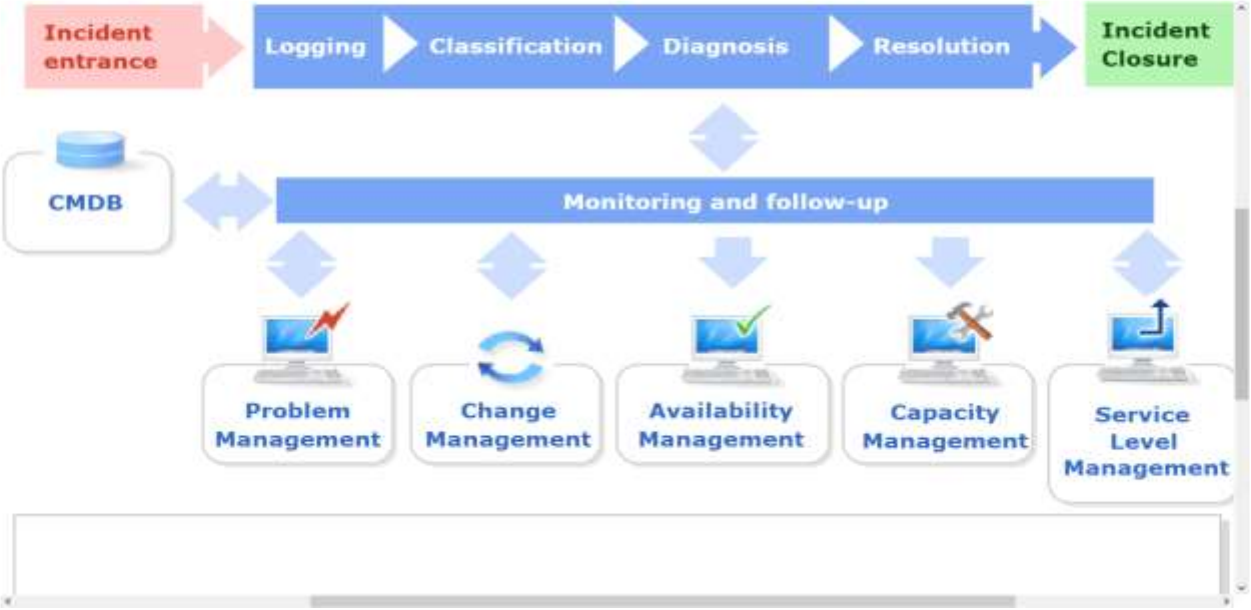


fig6.1 d

CMDB plays a key role in resolving incidents. For example, it gives information about who is responsible for configuration items involved. It makes it possible to ascertain all the implications the malfunctioning of a particular CI may have on other services. The CMDB must be updated when an incident is resolved if it was necessary to change or modify any configuration items.

Problem management helps incident management by reporting on known errors and possible workarounds. It also checks the quality of the information recorded in incident management so it can be useful in detecting and potentially solving problems.

Change management: resolving ab incident may require a request for change (RFC), which will be sent to change management. Implementing a given change incorrectly could cause multiple incidents, so change management must keep incident management informed about possible incidents that the changes made might cause to the service.

Availability management uses the information stored on the duration, impact and development over time of incidents in order to prepare reports on the real availability of the system.

Capacity management is concerned with incidents caused by insufficient IT infrastructure (Insufficient bandwidth, processing capacity, etc.)

Service level management: incident management must have access to the SLAs agreed with the customer in order to be able to determine the course of action to be taken in each case. Incident management must also provide regular reports on the fulfilment of the SLAs contracted.

Incident Logging and Classification

Logging

The essential first step in managing incidents correctly is to receive and log them.

Incidents may be reported from various sources, such as users, application managers, the **Service Desk** or technical support, among others.

Incidents should be logged immediately as it is much more difficult to log them later and there is a risk of new incidents emerging, causing the process to be postponed indefinitely.

- Commencing handling of the incident: the **Service Desk** must be able to evaluate whether the service required is included in the customer's **SLA** in the first instance and if not, forward it to a competent authority.
- Checking that the incident has not already been logged: it is commonplace for more than one user to report an incident, so it is necessary to check to avoid unnecessary duplication.
- **Assigning a reference**: the incident will be assigned a reference number to uniquely identify it in both internal processes and when communicating with the customer.
- **Initial logging**: the basic information needed to process the incident (time, description of the incident, systems affected, etc.) has to be entered on the associated database.
- **Supporting information**: any relevant information for the resolution of the incident that may be asked for from the customer using a specific form, or which may be obtained from the CMDB (interrelated hardware), etc.
- **Incident notification**: in those cases where the incident may affect other users, these should be notified so that they are aware of how the incident may impact their usual workflow.

Classification

The main aim of incident classification is to collect all the information that may be used to resolve it.

The classification process should implement at least the following steps:

- **Categorization**: a category is assigned (this may in turn be subdivided into several levels) depending on the type of incident and the workgroup responsible for resolving it. The services affected by the incident are identified.
- **Establishing the level of priority**: the incident is assigned a level of priority, based on predefined criteria, depending on its impact and urgency.
- **Allocation of resources**: if the **Service Desk** cannot resolve the incident in the first instance, it will designate the technical support personnel responsible for resolving it (second level).
- **Monitoring the status and the expected response time**: an incident is associated with the incident (for example, logged, active, suspended, resolved, closed) and the resolution time **for the incident is estimated based on the relevant SLA and the priority.**

Incident Analysis, Resolution and Closure

In the first instance the incident is examined with the aid of the **KB (**knowledge base) to determine if it can be matched with any incident that has already been resolved and the assigned procedure applied.

If the **Service Desk** is unable to resolve the incident it will forward it to a higher level for the experts assigned to investigate. If these experts are unable to resolve the incident, the predefined escalation protocols will be followed.

Throughout the lifecycle of the incident, the various agents involved must update the information stored in the databases so that all the levels involved have complete information on the incident's status.

If necessary, a **Request for Change (RFC)** may be raised. If the incident is recurrent and no definitive solution is found, **Problem Management** should also be informed so it can study the underlying causes in detail.

Once the incident is solved the following steps should be taken:

- Confirm with users that the solution is satisfactory.
- The resolution process should be added to the **KB**.

- The incident should be reclassified if necessary.
- The information on the **CMDB** about the configuration items **(CI)** involved in the incident should be updated.
- The incident should be closed.

Process Control

Preparing reports correctly is an essential part of the **Incident Management** process.

These reports must provide essential information, for example, for:

- **Service Level Management**: it is essential that customers have timely information about the level of compliance with **SLAs** and that corrective measures are taken in the event of non-compliance.
- Monitoring the performance of the **Service Desk**: determining the degree of satisfaction of the customer from the service delivered and supervising proper functioning of the first line of support and customer care.
- Optimizing the allocation of resources: managers need to know if the escalation process has followed the established protocols faithfully and if duplication has been avoided in the management process.
- Identifying mistakes: it may happen that the specified protocols are not right for the organization’s structure or the customer's needs, meaning that corrective measures need to be taken.
- Availability of Statistical Information: which may be used to make future projections about the assignment of resources, additional costs associated with the service, etc

Also, proper **Incident Management** requires infrastructure enabling it to be implemented correctly. This includes:

- A proper automated system to handle relationships with customers and for logging incidents.
- A knowledge base **(KB)** allowing new incidents to be compared with logged and resolved incidents. An up-to-date **(KB)** allows:
  - Unnecessary escalation to be avoided.

    - Engineers' know-how to be turned into a lasting asset for the company.
    - Some or all of this data to be made directly available to customers (in the form of a **FAQ**) on the Extranet. This can mean that sometimes the user does not even need to report the incident.
- A **CMDB** allowing all the current configurations and the impact these can have on resolving the incident to be determined.

To monitor the process correctly it is indispensable to use metrics allowing the functioning of the service to be evaluated as objectively as possible. Some of the key aspects to consider are:

- Number of provisionally classified incidents and their priorities.
- Resolution times classified according to the incidents' impact and urgency.
- Level of compliance with the **SLA**.
- Associated costs.
- Use of available resources in the **Service Desk**.
- Percentage of incidents, classified by priorities, resolved in the first instance by the**Service Desk**.
- The customer's level of satisfaction.

CASE STUDY

The "Cater Matters" **Service Desk** has just received a call from the person in charge of supplies at one of its customer's canteens.

He says that although he had ordered a new batch of ice-creams a few days ago over the web, they had not yet arrived and the stock in the fridge was running low.

The **Service Desk** operator looks in the orders database and confirms that the order was made several days ago, but he also notices that it was incorrectly stored.

He tries to repeat the order on his computer, but the system continues to malfunction.

Following the established protocols, the operator then takes the following decisions:

- He evaluates its priority: although the impact is low, the incident is urgent as the customer needs the delivery urgently.
- He logs the details of the incident.
- He consults the **Knowledge Base** to investigate whether the incident is the result of a **known error**, and if there are any possible work-arounds.
- A temporary solution is proposed to the customer: he is pointed in the direction of a reserved area of the website where he can place "urgent" orders by email.
- He contacts the systems department to warn that the incident may be repeated throughout the morning.
- Using the application that monitors warehouse stock, he checks the availability of the ice-creams ordered.
- He reassures the customer that he will receive the ice-creams before midday via the company's express service.

Meanwhile, the systems department:

- Runs a series of tests and confirms that, in general, the system is functioning correctly.
- Are unable to identify the cause of the incident.
- They contact **Service Desk** and suggest that the problem be forwarded to **Problem Management** with a preliminary classification of low priority.

Service Desk receives the information and decides that:

- Given the low impact of the incident and the fact that the customer has been given a satisfactory work-around, it does not need to be escalated.
- They log the work-around for the incident together with the information provided by the systems department.
- The incident is closed.

6.2 First line incident support,

The service desk is the single point of contact for users when there is a service disruption, for service requests, and for some categories of request for change. The service desk provides a point of communication with the users and a point of coordination for several IT groups and processes. To enable the service desk to perform these actions effectively, it is usually separate from the other service operation functions. In some cases, e.g. where detailed technical support is offered to users on the first call, it may be necessary for technical or application management staff to be on the service desk.

In summary the following are the functions of the 1st level support

- To register and classify received Incidents and to undertake an immediate effort in order to restore a failed IT service as quickly as possible.
- If no ad-hoc solution can be achieved, 1st Level Support will transfer the Incident to expert technical support groups (2nd Level Support).
- It also processes Service Requests and keeps users informed about their Incidents' status at agreed intervals.

6.3 Problem control and prevention

The main objective of **Problem Control** is to turn problems into **Known Errors** so that **Error Control** can propose the relevant solutions.

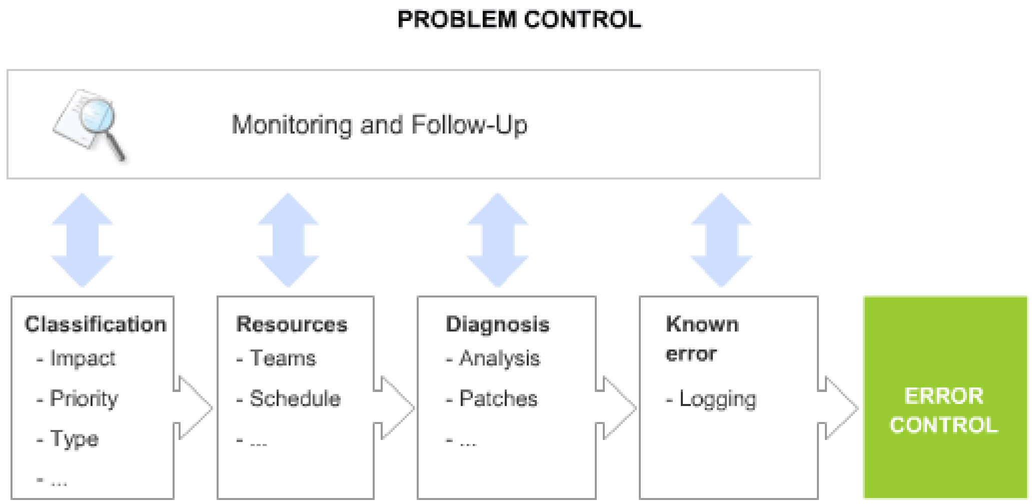


Fig 6.2 a

Problem Control basically consists of three phases:

1. Identification and Logging

One of the main tasks of Problem Management is to identify problems. The main sources of information used are:

- **The incident database:** in principle, any incident of which the cause is unknown and which has been closed by means of some sort of work-around is potentially a problem. However, it will be necessary to examine whether the incident is isolated and assess its impact on the IT structure before raising it to the category of a problem.
- **Analysis of IT infrastructure:** in collaboration with Availability Management and Capacity Management, Problem Management needs to analyse the different processes and determine the aspects in which IT systems and structures need to be bolstered in order to avoid future problems.
- **Service Level Degradation:** a decline in performance may be an indication of underlying problems that have not manifested themselves explicitly as incidents.

All the IT infrastructure areas need to work with **Problem Management** in order to identify real and potential problems and report any symptoms to it that may be a signal of deterioration in the IT service.

The problem log is basically similar to the incident log, except that the emphasis should not be on specific details of associated incidents but on the nature and possible impact of problems.

Among other things, the log should include information about:

- The **CIs** involved.
- Causes of the problem.
- Associated symptoms.
- Temporary solutions.
- Services involved.
- Levels of urgency, priority and impact.
- Status: active, known error, closed.

2. Classification and Allocation of Resources.

Problems are classified according to their general characteristics, such as whether they are hardware or software problems, the functional areas affected and details of the various configuration items (**CIs**) involved.

An essential factor is determining the priority of the problem, which, as in the case of incidents, is based on its urgency (the acceptable delay in solving the problem) and the impact (degree of deterioration in the quality of service).

As in the case of **Incident Management** the priority may change over the course of the life cycle of the problem, for example, if a temporary solution is found that considerably reduces its impact.

Once the problem has been classified and its priority defined, the resources necessary to solve the problem should be assigned. These resources need to be sufficient to ensure that the associated problems are dealt with effectively and the impact on the IT infrastructure minimised.

3. Analysis and Diagnosis: Known error

The main objectives of the process of analysis are:

- Determining the causes of the problem.
- Providing work-arounds for **Incident Management** to minimize the impact of the problem until the necessary changes are made so as to resolve the problem definitively.

It is essential to take into account the fact the the source of a problem is not always a hardware or software fault. It is commonplace for problems to be caused by:

- Errors of procedure.
- Incorrect documentation.
- A lack of coordination between different areas

It is also possible for the cause of the problem to be a well-known bug in one or other of the applications used. It is therefore a good idea to establish direct contact with the development environment, in the case of applications developed in-house, or to look for information on the Internet about known errors applicable to the problem in question.

Once the causes of the problem have been determined, it becomes a **Known Error** and is forwarded to **Error Control** for processing.

Chapter 7: Service Delivery:

Chapter Learning Objectives: By the end of this chapter you should appreciate the working of Service Level Management, Service Capacity Management, Loss of IT service,
Risk analysis and management, IT recovery options, Recovery of failed systems, Release management.

7.1 Service Level Management,

Basic Concepts

Suppliers, customers and users

Customer: the company or organization that contracts the IT services offered.

Users: the people who use the service.

Supplier: the company or organization that provides the services the customer requires.

Service Catalogue

The Service Catalogue is more than just an essential tool in simplifying communication with the customer. It can also be a great help to the internal organization and the external profile of the IT organization.

The Service Catalogue must:

- Describe the services offered in a non-technical way that is accessible to customers and non-specialist staff.
- Be used as a guide to orient and direct customers.
- Include, in general terms, the levels of service associated with each of the services offered.
- Be available to the **Service Desk** and all the staff in direct contact with customers.

Service Level Requirements (SLR)

The **SLR** should include detailed information about the customer's needs and expectations in terms of performance and level of service.

The **SLR** constitutes the basic element for defining the **SLA** and possible related **OLAs**.

Specification Sheets

The specification sheets are primarily technical documents for internal use that delimit and define the services offered to the customer.

The specification sheets should evaluate the resources necessary to offer the service required with a sufficient level of quality and determine whether it is necessary to outsource certain processes, and serve as a base document when drawing up the **OLAs** and **UCs** concerned.

Service Quality Programme (SQP)

The **SQP** needs to incorporate all the information necessary to enable efficient management of the levels of quality of the service:

- Targets for each service.
- Estimate of resources.
- Key performance indicators.
- Supplier monitoring procedures.

In short, **SQP** must contain the information necessary for the IT organisation to know about the processes and procedures involved in supplying the services provided, ensuring that they are aligned with the business processes, and so maintain appropriate quality levels.

Service Level Agreement (SLA)

The **SLA** needs to describe all the details of the services offered, in layman's terms, or at least in language comprehensible to the customer.

After it is signed, the **SLA** must be treated as the reference document for relations with the customer in all aspects of the delivery of the agreed services. It is therefore essential that it clearly define the essential aspects of the service, such as their description, availability, quality levels, recovery times, etc.

Operation Level Agreement (OLA)

The **OLA** is an internal document specifying the responsibilities and commitments of the various departments of the IT organization in the delivery of a particular service.

Underpinning Contract (UC)

The **UC** is an agreement with an external supplier to provide services not covered by the IT organization.

Service Improvement Programme (SIP)

The **SIP** must include corrective measures for faults detected in the service levels and proposals for improvements based on developments of the technology.

The **SIP** must form part of the basic documentation for the renewal of the **SLAs** and must be kept internally so that it is available to the managers of other IT processes.

7.2 Service Capacity Management,

Introduction and Objectives

The fundamental goal of **Capacity Management** is to make the available IT resources that customers, users and the IT department need to carry out their work efficiently, and to do so in a cost effective way.

This means **Capacity Management** has to:

- Stay up-to-date with the current state of the technology and expected future developments.
- Know about the company's business plans and service level agreements in order to forecast the necessary capacity.
- Analyze the performance of the infrastructure in order to monitor the use of existing capacity.
- Run capacity models and simulations for various possible future scenarios.
- Dimension services and applications appropriately, aligning them with business processes and the customer's real needs.

- Manage demand for computing services by rationalizing their use.

Capacity Management aims to avoid situations in which unnecessary investments are made in technologies that do not meet the real needs of the business or which are over-dimensioned, or by contrast, to avoid situations in which productivity is undermined by a shortage of, or inefficient use of, the existing technology.

Both scenarios frequently arise and can often be found coexisting in a single organisation: managers, customers and computer personnel are blinded by technologies they do not really need and buy them while overlooking applications, hardware and services that would genuinely increase the productivity in their working environments.

The main benefits of good **Capacity Management** are:

- The performance of IT resources is optimized.
- The necessary capacity is available when it is needed, avoiding a negative impact on quality of service.
- Unnecessary expenses caused by "last minute" purchases are avoided.
- Growth of the infrastructure is planned, allowing it to be matched to real business needs.
- The cost of maintenance and administration associated with obsolete or unnecessary hardware and applications are reduced.
- Possible incompatibilities and faults in the IT infrastructure are reduced.

In summary: the management of purchases and maintenance of IT services is rationalized, with the consequent reduction in costs and increase in performance.

Implementing an appropriate **Capacity Management** policy can also run into serious difficulties, such as:

- Insufficient information for realistic capacity planning.
- Unrealistic expectations about the cost savings and improvements in performance.
- Inadequate resources to monitor performance properly.
- Distributed and excessively complex IT infrastructure making access to data difficult.

- There is insufficient commitment on the part of top management to implement the associated processes rigorously.
- Rapid technological change makes it necessary to continuously review the plans and scenarios envisaged.
- Correct dimensioning of **Capacity Management** itself: excessive zeal may result in expensive capacity analyses that might have been made unnecessary by buying new hardware or software.

7.3 Loss of IT service,

Incident Management's sole aim is to restore quality of service as quickly as possible. It does not seek to determine the origins or causes of degradation to service quality.

When a type of incident becomes recurrent or has a powerful impact on the IT structure, the role of **Problem Management** is to determine its causes and look for possible solutions.

The following concepts need to be distinguished:

Problem: the as-yet unidentified underlying cause of a series of incidents or an isolated incident of considerable importance.

Known error: A problem becomes a known error when its cause has been identified.

The main concepts involved in the process of **Problem Management** and their relationship with Incident Management are summarized in the following interactive graphic:

7.4 Risk analysis and management,

Unless you know what the real risks facing your IT infrastructure are, it is impossible to set up a prevention and recovery policy that will be at all effective in the event of a disaster.

IT Service Continuity Management must enumerate and assess the various risk factors according to their probability and impact. To do so, **ITSCM** must:

- Have an in-depth knowledge of the IT infrastructure and the configuration items (**CIs**) involved in providing each service, particularly critical and strategic IT services.
- Analyze possible threats and estimate their probability.
- Detect the most vulnerable points of the IT infrastructure.

The results of this detailed analysis will provide sufficient information with which to put forward various different prevention and recovery measures suited to the real needs of the business.

Prevention of generic, highly unlikely risks may be very expensive and not always justified. However, preventive or recovery measures designed to tackle specific risks may be simple, quick to implement and relatively cheap.

For example, if power cuts are frequent where the organization is based, it might opt to relocate certain IT services via **ISPs** with redundant power systems or invest in an uninterruptible power supply (UPS) to run the **CIs** on which the most critical service depend, etc.

7.5 IT recovery options,

Crises often cause panic. This can be counterproductive and may at times be even more damaging than the original incident. It is therefore essential to ensure that staff roles and responsibilities in an emergency, as well as the relevant protocols for action, are clearly defined

Emergency management plans therefore need to take into account aspects such as:

- Evaluating the impact of the contingency on the IT infrastructure.
- Assigning emergency roles to IT service personnel.
- Informing users and customers of a serious interruption or service degradation.
- Procedures for contact and collaboration with the suppliers concerned.
- Protocols for putting the relevant recovery plan into action.

7.6 Recovery of failed systems

When an interruption to service is inevitable the time to put the recovery procedures into action has arrived.

The recovery plan needs to include everything necessary to:

- Reorganize the staff involved.
- Re-establish the hardware and software systems necessary.
- Recover the data and restart the IT service.

The recovery procedures may depend on the importance of the contingency and the associated recovery option (cold or hot stand-by), but in general they involve:

- Assigning personnel and resources.
- Alternative hardware facilities.
- Security plans guaranteeing the integrity of the data.
- Data recovery procedures.
- Cooperation agreements with other organizations.
- Protocols for informing customers.

When a recovery plan is brought into action there is no room for improvisation. Any decisions made can have serious consequences both for the way the organization is perceived by customers and the costs associated with the process.

Although it may seem paradoxical, a "disaster" can be a good opportunity to show your customers the solidity of your IT organization and thus increase their confidence in you. As they say, **"every cloud has a silver lining."**.

7.7 Release management.

A release is a group of new or modified **CIs** which have been validated for installation in the live environment. The functional and technical specifications of a version are defined in the corresponding **RFC**.

Releases may be classified, according to their impact on the IT infrastructure, as:

- **Major releases**: representing a significant roll-out of hardware and software and which introduce important modifications to the functionality, technical characteristics, etc.
- **Minor releases**: these usually entail the correction of one or more specific errors and are often modifications that implement documented emergency solutions correctly.
- **Emergency releases**: modifications repairing a known error quickly.

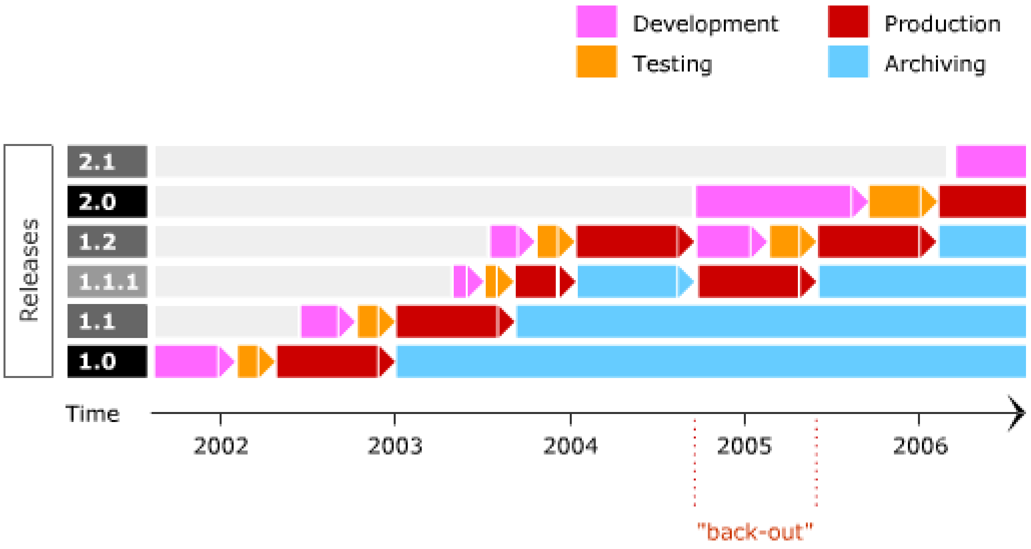
As there may be multiple versions it is worth defining a reference or code unambiguously identifying them. The universally accepted system is:

- **Major releases**: 1.0, 2.0, etc.
- **Minor releases**: 1.1, 1.2, 1.3, etc.
- **Emergency releases**: 1.1.1, 1.1.2, etc

In some cases this classification is further refined. (for example, the help in the version of your browser).

During its life-cycle a release may go through various states: development, testing, live and archived.

The diagram below illustrates the progress of a release over time:



New versions can be rolled out in different ways and it is the responsibility of **Change Management** to decide the most appropriate way of proceeding. The most common options include:

- **Delta release**: only the modified components are tested and installed. This option has the advantage of greatest simplicity, but it entails the risk that problems or incompatibilities may arise in the live environment.
- **Full release**: All the affected components are distributed, whether they have been modified or not. Although this option obviously involves more work, provided the relevant tests have been done, it is less likely that incidents will occur after installation.
- **Package of Releases**: Change Management may opt to distribute different packages of releases in a synchronized way. This offers greater stability in the IT environment. In some cases this option is unavoidable due to incompatibilities between a new version and previously installed hardware or software. Consider, for example, a migration to a new operating system requiring more advanced hardware and/or new versions of office automation programs.

The following are the stages of release management

7.7.1 Planning

It is crucial to establish a general framework for the launch of new versions. This must set out the working methods. This is especially important for small or emergency releases, as in the case of large releases specific plans taking into account the specific features of each case will be drawn up.

In order to plan a new release properly, the following points need to be taken into account:

- How does the new version affect other areas of the IT framework?
- What **CIs** will be directly or indirectly involved during and after the launch of the new version?
- How should the test environment be built so that it is a faithful reflection of the production environment?
- What back-out plans are necessary?

- How and when should back-out plans be implemented in order to minimize the possible negative impact on the service and the integrity of the IT system?
- What are the human and technical resources necessary to ensure the new release is implemented successfully?
- Who will be directly in charge of the various stages of the process?
- What information and/or training plans need to be developed so that users are kept informed and are able to perceive the new version as an improvement?
- What type of deployment is most appropriate (complete, delta, synchronized at all sites, gradual, etc.)?
- What is the expected average useful life of the new version?
- What impact is the release process likely to have on the quality of service?
- Is it possible to establish precise metrics defining the degree of success of the launch of the new version?

7.7.2 Development

Release Management is responsible for designing and building new versions following the guidelines defined in the relevant **RFCs (Request For Change)**.

This development work is sometimes done in-house, but in many cases requires the involvement of external service providers. In this latter case, the role of **Release Management** is to ensure that the hardware or software package or packages offered meet the specifications described in the **RFC**. **Release Management** will also be responsible for the complete configuration process necessary.

This development must include, if necessary or advisable, all the installation scripts needed for the deployment of the version. These scripts must take into account aspects such as:

- Automatic data back-ups.
- Any updates that need to be made to the associated databases.
- Installation of new versions on different systems or at different sites.

- Creating the logs of the installation process.

An integral part of the development work is drawing up the associated back-out plans. These need to take into account the availability agreed with customers in the relevant SLAs.

7.7.3 Validation

A well planned test protocol is absolutely essential if a new version is to be released onto the live system with reasonable certainty of success.

Tests should not be limited to performing merely technical validation (checking for the absence of errors); rather, functional tests with real users must be conducted to ensure that the version meets the set requirements and is reasonably usable (there will always be a degree of resistance to change among users and this should be taken into account).

It is important that the tests include back-out plans to ensure that it is possible to return to the last stable version quickly and in an orderly way without the loss of valuable information.

The main activities performed during the testing process should include:

- Tests of correct functioning of the release in a realistic environment.
- Tests of automatic or manual installation procedures.
- List of bugs or errors detected, if any.
- Tests on back-out plans.
- Documentation for users and service personnel.

Release Management will be responsible for final validation of the version before proceeding with its installation. If the version is not accepted it will be returned to **Release Management** for re-evaluation.

7.7.4 Implementation

The moment of truth has arrived, the distribution of the new version, or rollout.

There are several types of rollout:

- **Complete and synchronized**: a complete rollout takes place simultaneously on all sites.

- **Fragmented**: either in space or time. For example, the new version is released to different work groups or the functionality offered is progressively increased.

The rollout procedure must be carefully documented so that all the parties are aware of their specific tasks and responsibilities. In particular, end users must be informed of the release schedule in advance and told how it might affect their day-to-day activities.

It is essential to clearly define:

- The **CIs** that should be deleted and installed and the order in which this process should take place.
- When this process should be carried out in the case of different work groups and/or geographical locations.
- What metrics determine the implementation of back-out plans and whether these should be complete or partial.

After distributing the new release, **Release Management** must ensure that:

- A copy of the version is included in the **DSL**.
- The **DHS** includes the functional responses of the new **CIs**.
- The **CMDB** is properly updated.
- Users are properly informed about new functionality and have been given the training they need in order to be able to make best use of it.

After the release, **Release Management** must be informed in a timely way by the **Service Desk** of any comments, complaints, incidents, etc. that the new version may have produced. All this information must be analyzed to ensure that future versions incorporate the suggestions received and that the necessary corrective measures are taken to minimize the negative impact that future changes might have.

7.7.5 Communication and Training

It is a frequent, but nonetheless serious, mistake to overlook the human factor when tackling technical issues.

With relatively few exceptions, interaction between users and applications is necessary and this usually represents the weakest link in the chain.

It is useless to have a sophisticated IT service if the users are not able to make use of its advantages because they have insufficient information or training.

This training and information has to be structured on various levels:

- Users should be made aware of the forthcoming launch of a new release and be informed of the planned new functionality or the errors the release aims to solve so they can become involved in the process if they wish.
- Wherever possible functional tests should be carried out by a selected group of end users. During this test process the following will be documented and analyzed:
    - Users' subjective experience.
    - Comments and suggestions on usability and functionality, or the doubts that may have arisen during use of the new version.
    - The documentation that will be provided to end users.
- When considered appropriate, courses on the functioning of the new version should be run, whether classroom-based or online courses using e-learning modules.
- A page of **FAQs** will be written, where users can find answers to their most common queries and can ask for help or technical support using the new version.

References

1. A+ Study Guide: Device Drivers. (n.d.). Retrieved from http://www.proprofs.com/certification/comptia/a-plus/study-guide/wbt16/4001.shtml

2. Andrews, J. (2003). A+ guide to software: Managing, maintaining, and troubleshooting. Cambridge, Mass: Course Technology.

3. Byrne, J. J. (2002). Network+ certification bible. New York, NY [u.a.: Hungry Minds.

4. Chambers, M. L. (2009). Build your own PC for dummies: Do-it-yourself. Hoboken, N.J: Wiley.

5. Coaxial Cables. (n.d.). Retrieved from http://atx2000.altervista.org/English/EN_coax.html

6. Docter, Q., Dulaney, E. A., & Skandier, T. (2009). CompTIA A+ complete study guide. Indianapolis, Ind: Wiley Pub.

7. Driver Definition (Computer Driver, Device Driver). (n.d.). Retrieved from http://pcsupport.about.com/od/termsag/g/term_driver.htm

8. Fiber Optic Communications for the Premises Environment by Dr. Kenneth S. Schneider PhD. Chapter 2. (n.d.). Retrieved from http://www.telebyteusa.com/foprimer/foch2.html

9. How to Check the Mac Processor Speed. (n.d.). Retrieved from http://osxdaily.com/2010/10/23/how-to-check-the-mac-processor-speed/

10. How to Develop an IT Change Management Program: 8 Steps. (n.d.). Retrieved from http://www.wikihow.com/Develop-an-IT-Change-Management-Program

11. HowStuffWorks "How PC Power Supplies Work". (n.d.). Retrieved from http://computer.howstuffworks.com/power-supply3.htm

12. IT Management - Change Control vs. Change Management: Moving Beyond IT. (n.d.). Retrieved from http://www.technologyexecutivesclub.com/Articles/management/artChangeControl.php

13. IT Management - Change Control vs. Change Management: Moving Beyond IT. (n.d.). Retrieved from http://www.technologyexecutivesclub.com/Articles/management/artChangeControl.php

14. Network Troubleshooting and Resource Site for School IT Staff | Network Cables. (n.d.). Retrieved from http://webpage.pace.edu/ms16182p/networking/cables.html

15. NTFS.com: Data Recovery Software, File Systems, Hard Disk Internals, Disk Utilities. (n.d.). Retrieved from http://www.ntfs.com/

16. Palmer, M. (2003). *Guide to Operating Systems Security*. Retrieved from https://ecampus.phoenix.edu/content/eBookLibrary2/

17. The Service Desk - Introduction and Objectives - Activities and Functions. (n.d.). Retrieved from http://itil.osiatis.es/ITIL_course/it_service_management/service_desk/introduction_and_objectives_service_desk/activities_and_functions_service_desk.php#

18. Types of Computer Cable Connections - Computer Cable Guide. (n.d.). Retrieved from http://www.buildcomputers.net/computer-cable-connections.html

19. What are DVI Cables? (n.d.). Retrieved from http://www.wisegeek.com/what-are-dvi-cables.htm

20. What is configuration management database (CMDB)? - Definition from WhatIs.com. (n.d.). Retrieved from http://searchdatacenter.techtarget.com/definition/configuration-management-database

21. Windows 8 system requirements - Microsoft Windows. (n.d.). Retrieved from http://windows.microsoft.com/en-us/windows-8/system-requirements