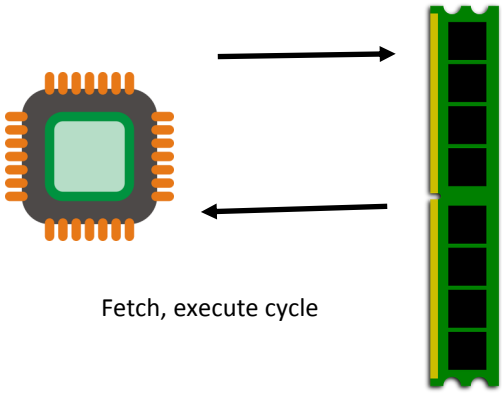
learncomputing

GCSE Computer Science
Component 01

Revision

System Architecture

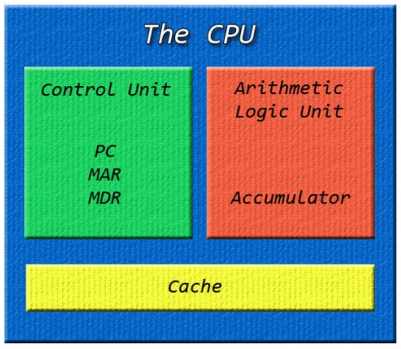
A CPU is the part of the computer that completes the processing. It can be said to **fetch** and **execute** instructions from main memory. This is called the **fetch execute cycle.**



Fetch, execute cycle

Some CPUs are better than others. Factors that affect the speed include:

1. **Clock speed**—the number of fetch execute **cycles per second**. This is measured in Hz. 2GHz is the same as 2,000,000,000 cycles per second.
2. **Number of cores**—most modern CPUs have more than one CPU core. This is like splitting the CPU up into several mini-CPUs. The more cores the more **instructions can be processed at once**. e.g. a quad core processor has four cores and can process four instructions at once.
3. **Cache**—fetching instructions from memory takes time. A good idea is to put the most **commonly used instructions** in some super fast memory located on the CPU itself. This is called cache. The bigger the cache, the more instructions can be stored there and the faster the CPU will run.



The CPU has two main parts:

1. **Control Unit (CU)** —Provides **control signals** so data goes to the place it is supposed to. Controls **timing signals** including the clock speed. Sends signals to memory, the ALU and I/O devices.
2. **Arithmetic Logic Unit (ALU)** - performs any **maths** (arithmetic) calculations, performs **logic** calculations (e.g. is x < y).

An **embedded system** is a computer that is fully **contained within the device it controls**.

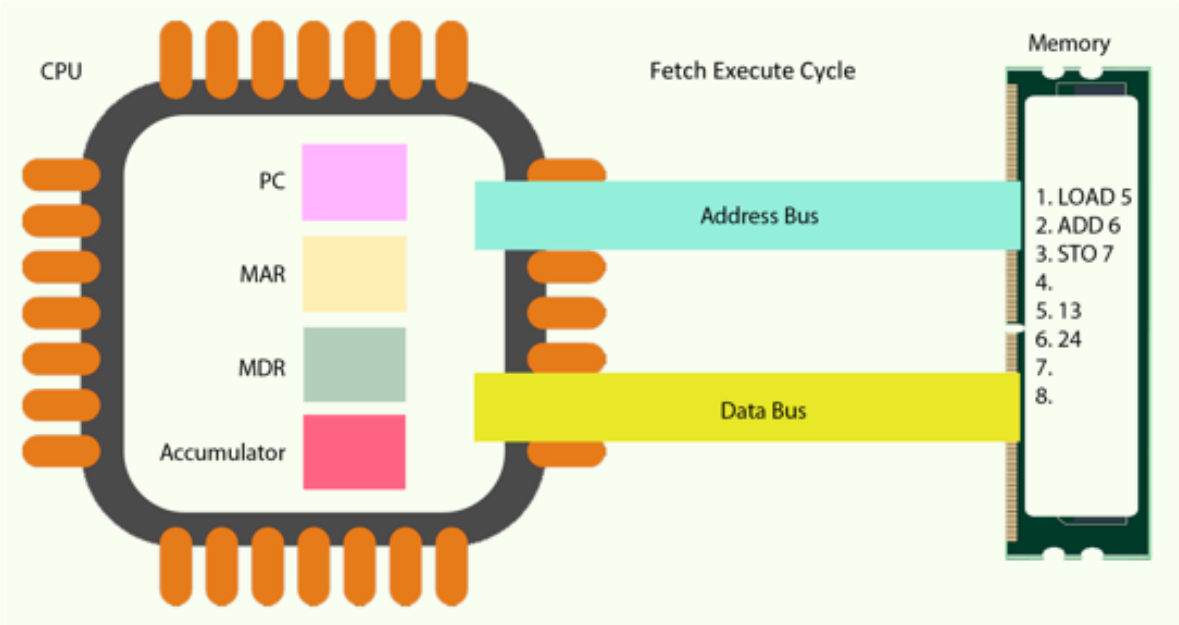
However it still has all the features of the other computers we have been learning about! e.g. a CPU fetches instructions from memory

Examples:

- Microwave
- Plane
- Washing machine

VON NEUMANN ARCHITECTURE

Modern CPUs still follow a design made decades ago by John von Neumann. They have a series of registers which are small storage locations on the CPU. These registers are used in the fetch execute cycle.



The Program Counter (PC) -

1. points to the next instruction **in memory**
2. copies its value (which is a **memory address**) to the MAR
3. gets **incremented** by 1 (1 is added to it) so that it points to the next instruction

The Memory Address Register (MAR) -

1. receives a **memory address** from the PC
2. sends the memory address along the **address bus** to the correct location in memory

The Memory Data Register (MDR) -

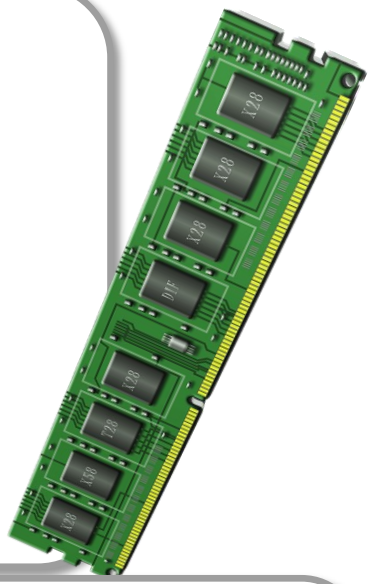
1. the instruction and data is sent along the **data bus** and stored in the MDR

Accumulator -

1. when the instruction is executed the **results are stored** here. Holds a running total of the operation currently happening.

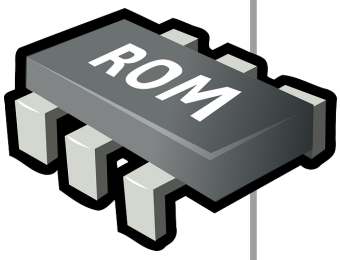
Memory

RAM

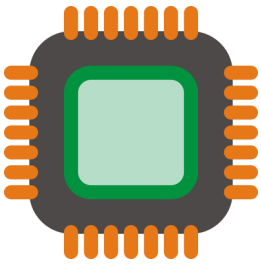


1. Stands for **Random Access Memory**
2. Stores **instructions and data** for **programs that are currently in use**
3. **Volatile**—when the power is switched off all its contents are lost
4. Two types:
   - **DRAM (dynamic RAM)**—less expensive, not as fast, needs constant refreshing. Used for the main RAM in your computer.
   - **SRAM (static RAM)** - much more expensive, faster, doesn't need lots of refreshing. Used for cache (see below).

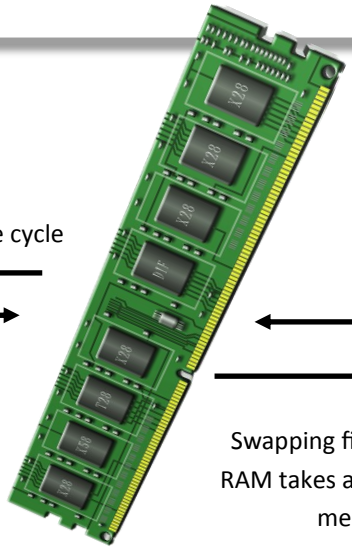
ROM



1. Stands for **Read Only Memory.**
2. Stores **instructions needed to boot up the computer** including the **BIOS.**
3. **Non-volatile**—keeps its contents when the power is switched off.
4. Originally Read Only meaning data could not be written to by the user—however over the years different types of ROM have been developed that allow the user to write some data PROM, EPROM, EEPROM.



Fetch, execute cycle



Items swapped in and out of RAM as needed.

The CPU fetches and executes instruction from RAM only. It can't access the hard disk directly.

Swapping files from the hard drive to RAM takes a lot of time so using virtual memory is very slow.

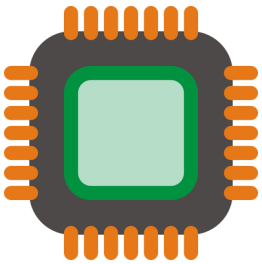
VIRTUAL MEMORY

Often there isn't enough space in RAM for all the programs that are currently being run.

The operating system can use a special section of the hard drive to deal with the overflow if necessary. This is called a **page file** and the process is known as **virtual memory**.

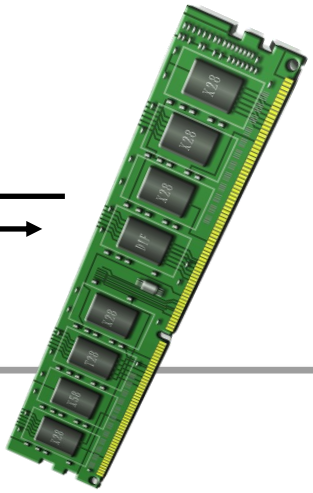
Data and instructions **must be in RAM** to be processed by the CPU so they need to be swapped in and out from the hard drive before they can be processed.

This means that although there is more overall space, using virtual memory is **much slower** than using RAM.



Fetch, execute cycle

Cache—stores the most commonly used instructions for quick retrieval



CACHE MEMORY

One of the problems with the fetch execute cycle is that it can take a relatively **long time** for the data and instructions to be fetched from RAM.

Modern CPUs combat this by using cache memory. This is **super fast** memory that is very **close to the CPU**. It stores the **most commonly used instructions** so that they can be **retrieved much faster** than if they were in RAM. This increases the speed of the computer. The **more cache** you have, the more instructions can be stored, and the **better the performance** of your computer.

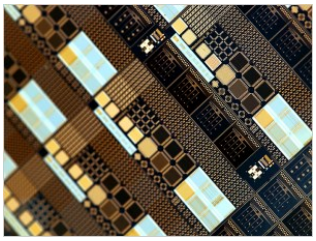
FLASH MEMORY

Advances in ROM technology now mean that ROM can be made to be fully rewritable. This is called flash memory.

Flash memory is useful as it is very fast compared to a hard disk drive and can be used as secondary storage in USB memory sticks, SD cards and solid state drives.

Mobile computing devices like modern laptops and smart phones rely on flash memory for their secondary storage needs. This is fast and isn't affected by being moved around.

Technology is moving fast and there are many up and coming memory innovations that are set to transform the state of modern computer science.



MEMORY INNOVATIONS

Using flash memory has led to new computer designs. Ultra fast solid state drives are now appearing regularly in laptops making them smaller, quieter and quicker.

Mobile phone technology has rapidly advanced and now the quaint iPhone boasts tons of storage!

The future holds many more potential technologies about the be released including:

- A memory bit that is only 12-atoms big! Think how small our storage could become!
- ReRAM—non volatile RAM.
- Memresitor technology—memory so fast scientists can't even measure the speed.

Secondary Storage

Magnetic Storage

A type of storage that uses lasers a magnet to make a magnetised segment on a disk platter.

Includes hard disk drives and the outdated floppy disk.

Hard disk drives feature in most modern computers as they offer a lot of storage at a cheap price and are relatively fast.

Optical Storage

A type of storage that uses lasers to burn marks in a reflective disc.

There are three types: CD-ROM, DVD-ROM and Blu-Ray ROM.

Often used whenever something cheap to produce and portable is needed. Also, most people have access to the equipment to read the discs.

Flash Storage

A type of storage that uses electricity to open and close gates on a circuit board.

Includes USB memory sticks, SD cards and solid state drives.

Very fast, portable and not affected by moving parts. This technology is slowly overtaking the storage world as it becomes cheaper and cheaper.

UNITS OF DATA

Unit	Abbreviation	Number of Bytes	Notes
Bit		1/8	either a 0 or 1
Nibble		1/2	e.g. 1010
Byte		1	e.g. 11001100
Kilobyte	KB	1,000	written as 1KB
Megabyte	MB	1,000,000	or 1000KB
Gigabyte	GB	1,000,000,000	or 1000MB
Terabyte	TB	1,000,000,000,000	or 1000GB
Petabyte	PB	1,000,000,000,000,000	or 1000TB

CAPACITY—how much data the media can store. The higher the capacity the better.

A typical SD card might hold 32GB. A hard drive might be about 2TB. Old floppy disks were 1.44MB.

ACCESS SPEED—how quickly the device can read and write data.

Old floppy disks were very slow as are tape drives.

Optical drives are quite slow.

Hard drives are pretty fast.

Solid state drives are very fast.

PORTABILITY—can the device be carried around easily?

Internal hard disk drives can't be carried around easily. Neither can solid state drives.

Optical disks, flash memory sticks and SD cards are very portable.

DURABILITY—is the device easy to damage?

Internal hard disk drives and optical discs are very fragile.

Flash memory is much more durable.

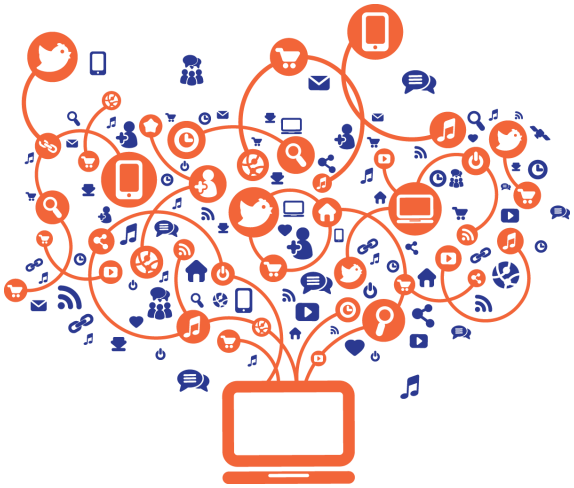
RELIABILITY—how long does it go before it starts to break?

Most storage devices are quite reliable and will suit most uses.

However, flash memory degrades over time and eventually wears out.

Optical discs can't be rewritten forever.

Magnetic storage like hard disks last a very long time.

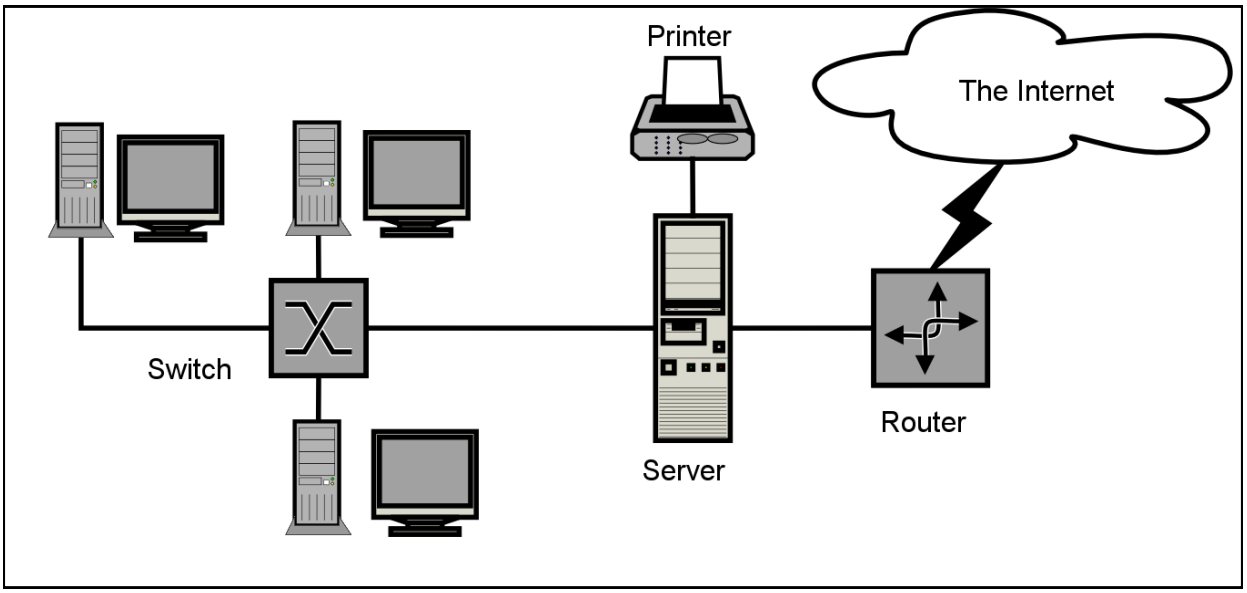


Wired and Wireless Networks

A network is when **two or more computers are connected together**. This is often a good idea because:

- Files can be shared.
- **Resources** like printers and scanners can be shared.
- Buying software for multiple computers is often cheaper (**site license**).
- You can manage **users** and **security centrally.**

However, you can choose to not network your computers. This is called a **standalone environment**. Not having a network is more secure and cheaper to set up but doesn't give you any of the benefits above.



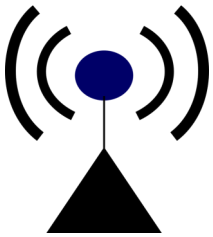
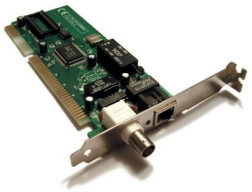
A network can have different sizes.

LAN – local area network

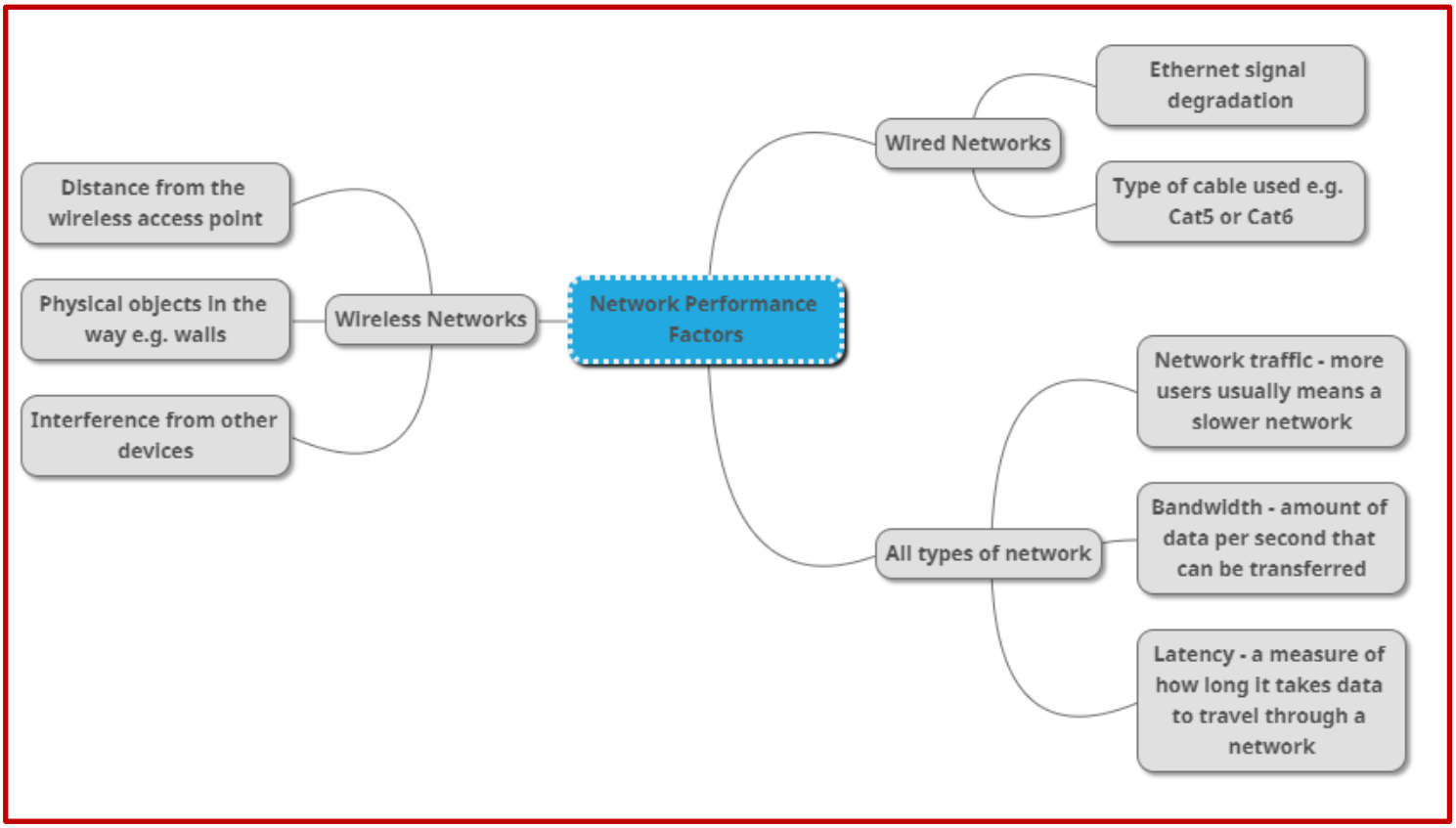
WAN – wide area network

	Advantages	Disadvantages
LAN	Quick and easy to set up	Small area only
	Cheap to set up	Relatively few computers / users
	Cheap to maintain	
	Relatively fast	
WAN	Can be any size – even global	More expensive to set up
	Allows many more computers / much more intricate and detailed	Needs ongoing maintenance
		Needs specialised equipment and expertise
		Slower

NETWORK HARDWARE

				
Wireless Access Point	*Router*	*Switch*	*Network Interface Card (NIC)*	*Transmission Media*
Lets a device connect to a LAN using WiFi.	Connects two networks together, usually a LAN to the internet	Intelligently decides where data travels to in a network so each device gets the data it needs	Lets a computer connect to a network using a wire.	Refers to the cabling used to connect the network together and includes Ethernet cable, coaxial cable and fibre optic cable.

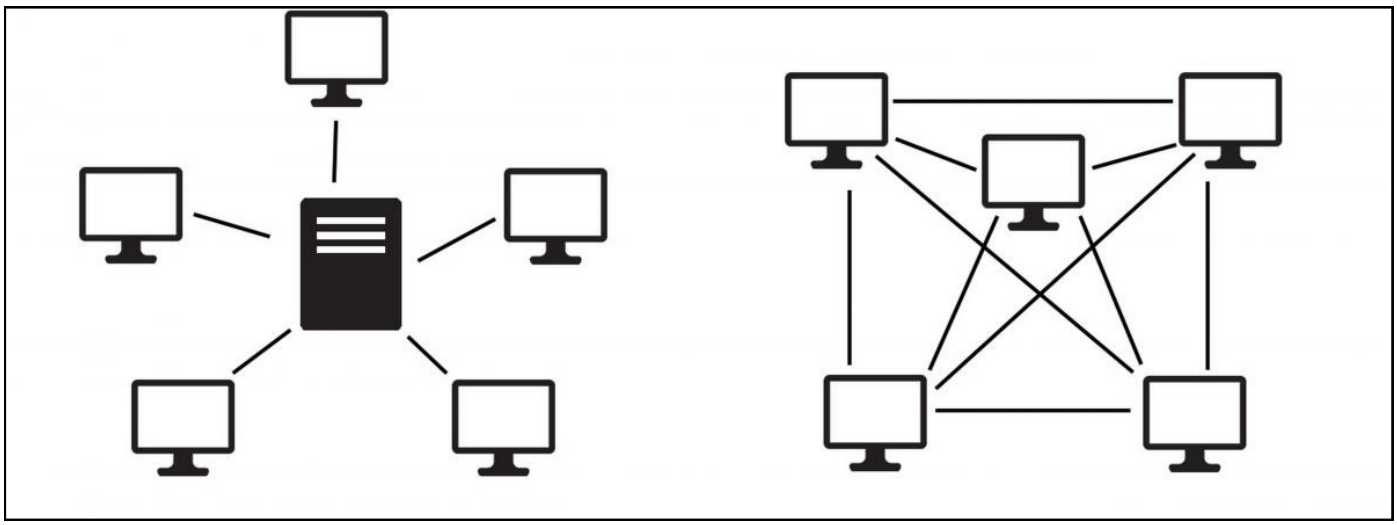
NETWORK PERFORMANCE FACTORS



CLIENT SERVER VS PEER TO PEER

Client server involves having one centralised computer (a server) that does most of the processing and stored most of the data. The client computers connect to the server when needed.

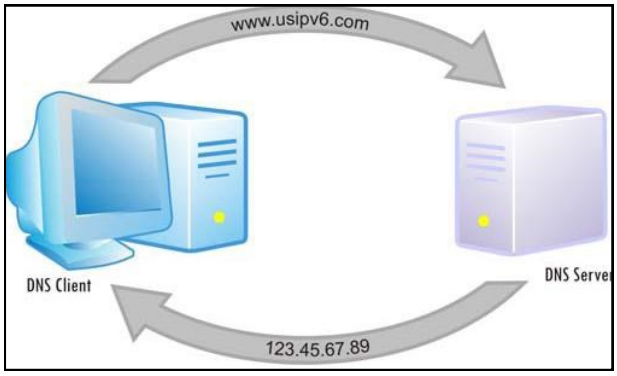
In peer-to-peer all the computers have the same importance and all share processing and storage.



	Advantages	Disadvantages
Client Server	Files are stored centrally – easy to manage.	Needs a specialist network operating system.
	Backups and security controlled centrally – more secure.	You often have to employ a network manager (costs money).
	You can have levels of access to control data.	You need to buy a server and other expensive equipment.
Peer to Peer	No need for a network operating system.	Files are stored on individual computers so it can be harder to find things.
	Much easier to set up – no high-level IT knowledge needed.	Everybody has to be responsible for not bringing a virus in.
	If one computer fails then the network can carry on.	No levels of access – less security.

THE INTERNET

The internet is a very large WAN. In fact it is a collection of networks that span the entire world.



Key terms:

DNS – Domain Name System – the system that converts a web page's name (also know as URL e.g. amazon.co.uk) into its corresponding IP address.

Hosting – the process of storing a web page on a server so that it can be accessed on the World Wide Web.

The Cloud – a term used for storage that can be accessed using the internet.

VIRTUAL NETWORKS

A virtual network is a small subset of a LAN or WAN where only specific computers can see each other.

In the example opposite, the red computers have been made into a virtual network. To the users on those machines it will seem like they are the only computers on the network.

It could be that the red computers are for the network administrators and the others are for normal users.

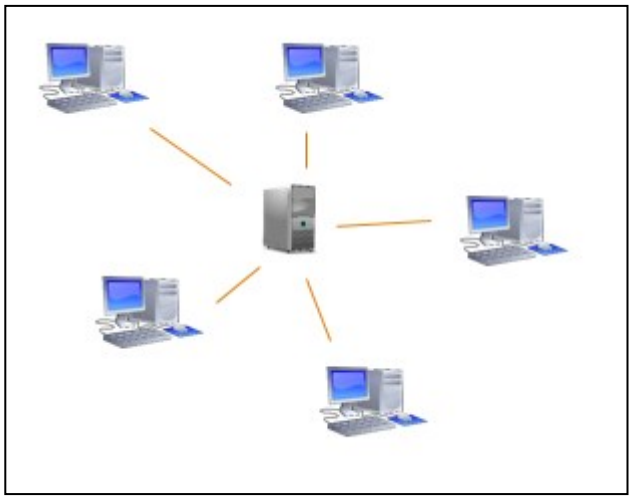
Normal users won't be able to see the admin functions and vice versa.

This is handy as there is no need to rewire the network to do this—it is possible via software and using all the existing physical connections.

Network Topologies, Protocols and Layers

STAR NETWORK

In a star network all computers are connected directly to a central server or to a switch.



Advantages

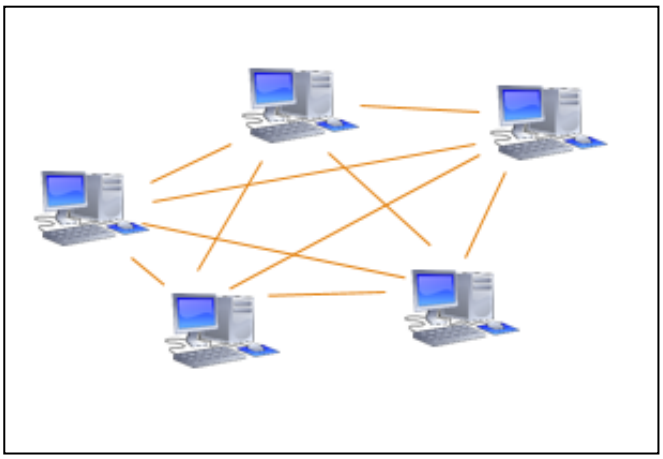
The network can be managed centrally and it is easy to add more computers.

If one computer breaks the network still runs.

Disadvantages

If the server breaks no computers will work.

Needs specialist equipment (switch)



MESH NETWORK

In a mesh network all computers are connected to every other computer in the network. This means all computers are the same importance.

Advantages

Very robust and reliable way to cable a network.

Not reliant on a server. If one computer breaks the rest are fine.

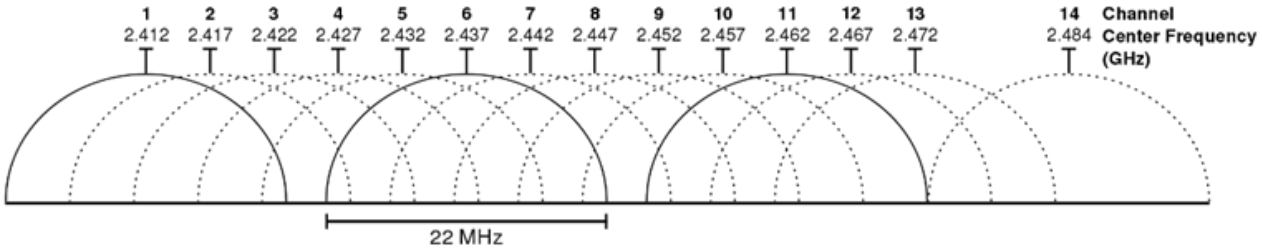
Disadvantages

Requires a lot of cable to set up – this is expensive.

WI-FI—FREQUENCY AND CHANNELS

A standard for connecting computers together into a wireless network by **sending data across radio waves**. The acronym doesn't stand for anything—it is just a brand name.

Frequency—the number of **oscillations per second** the radio wave uses. Wi-Fi signals operate at a range of frequencies that are split up into channels.



A channel is a **frequency range** that Wi-Fi will transmit across. The available frequencies can be split in channels of different widths depending on the technology being used.

Sometimes, you might want to change to a different channel if lots of devices in the area are using one or overlapping channels. This will **prevent interference** and improve performance.

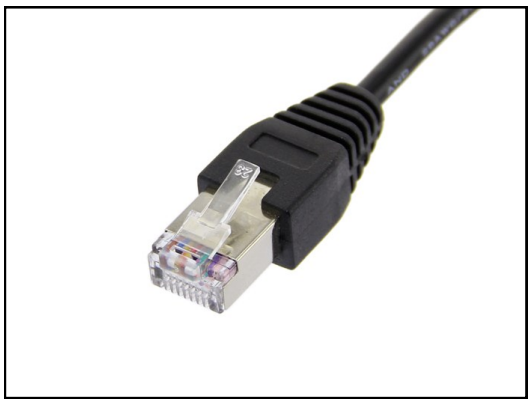
WI-FI ENCRYPTION

Normally, you wouldn't want somebody to access the data being sent across Wi-Fi otherwise they could steal important data or use your internet connection for free. A signal can be encrypted to prevent this. There are 4 types of Wi-Fi encryption:

WEP	The first type of wireless encryption invented. It uses an encryption key which has been found to be too short and is vulnerable to a brute force attack. A hacker could guess a WEP password within a few minutes using widely available software.
WPA	Was introduced to improve on the vulnerabilities of WEP. This method involves changing the encryption key for every data packet making it much harder to breach.
WPA2	An even stronger version of WPA. This uses 128 bit encryption and in now mandatory in all devices showing the Wi-Fi brand symbol.
WPA3	Released in January 2018 this method uses 192 bit encryption and has extra security for users who choose to use weak passwords.

ETHERNET

Ethernet is a **protocol** that governs the transmission of data between devices. It uses **cables to transmit the data in a LAN**.



Ethernet is useful for connecting devices in close proximity. After 100m the **signal degrades** and becomes unusable. This can be extended with range boosters.

Ethernet uses **broadcast addressing**.

This means if a device sends some data it broadcasts it out and all the devices on the network receive it. They then need to decide if the broadcast is for them or not and either read the message or ignore it.

Devices can only send data when there is no other devices transmitting to avoid data becoming jumbled up. An Ethernet system uses **collision detection** to stop these kinds of data collisions.

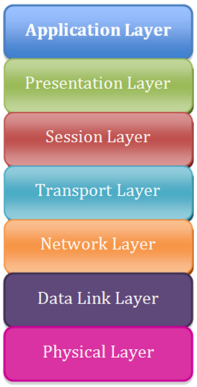
IP vs MAC ADDRESS

An IP address is given to everything that is **connected to the internet**.

It is a **unique number** that identifies your computer / device and can be used as a way to know where to send data to and where it is sent from.

A MAC address is a unique number that is **hard wired into every piece of networking equipment**. It does not change.

Protocol	What it stands for	What it does
TCP/IP	Transmission Control Protocol / Internet Protocol	For sending any data across the internet
HTTP	Hyper Text Transfer Protocol	For sending and receiving data about web pages
HTTP/S	Hyper Text Transfer Protocol Secure	For sending and receiving **encrypted** data about web pages
FTP	File Transfer Protocol	For sending files
POP	Post Office Protocol	For **receiving** emails
IMAP	Instant Message Access Protocol	For **receiving** emails and syncing emails to the server
SMTP	Simple Mail Transfer Protocol	For **sending** emails



PROTOCOL LAYERS

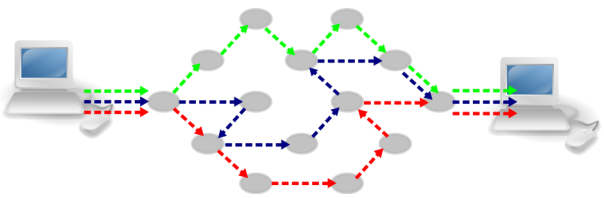
Protocols aren't just one process.

They are broken down into layers – each layer does a different job. All the jobs combined complete the task of sending the data.

Each protocol is different but an overarching model has been made called the OSI model that tries to show you all the possible layers.

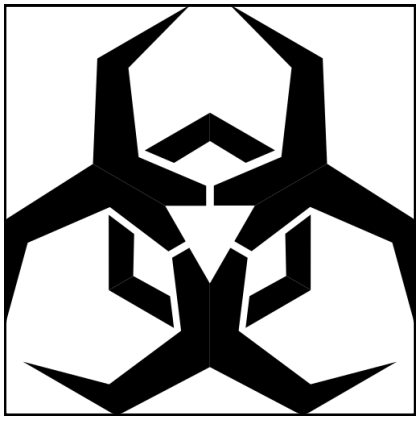
PACKET SWITCHING

1. Data is split into chunks called packets
2. Each packet is marked with: the sending and receiving IP address; the sending and receiving MAC address; how many packets there are in total and which packet this one is.
3. The packets can then take **any route** across the internet.
4. The are **reassembled** at the other end into the original full message.
5. If a packet becomes lost in transmission then it can be requested again.



System Security

MALWARE



Stands for malicious software – it includes any software that has been designed to cause harm to a user or the computer.

Examples are:

- **Virus**: software that copies itself from machine to machine causing harm as it goes.
- **Trojan horse**: malware that is disguised as something beneficial e.g. a game or utility and only once downloaded does it cause damage.
- **Spyware**: malware that watches the keys you press trying to record your passwords and personal information
- **Ransomware**: locks your computer and all the files so you can't access it unless you pay the evil owner a huge sum of cash!

SQL INJECTION

Malicious code is entered into a form on a website that attempts to change the SQL statement that goes to the server.

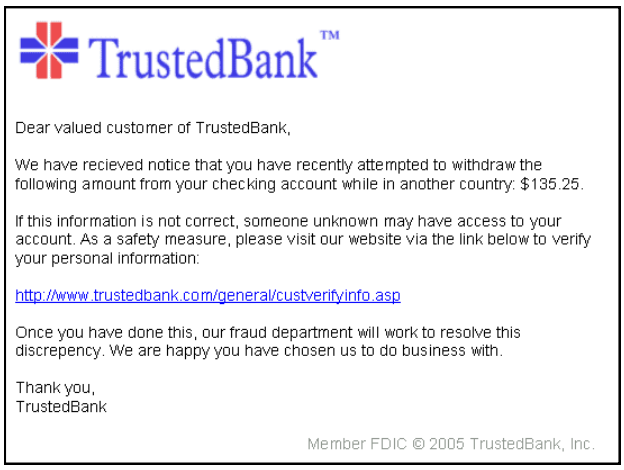
This could mean that the criminal gets unauthorised access to data from the database or could delete / modify the data.

e.g.

Adding ;DROP TABLE Customer to the end of a query string might delete a website's customer data if it wasn't securely protected.

PHISHING

An email is made to look like it comes from a legitimate source such as a bank. The email will try to trick the user into clicking on a link and entering their personal information. This was the hacker can gain access to your secure accounts!



TrustedBank™

Dear valued customer of TrustedBank,

We have recieved notice that you have recently attempted to withdraw the following amount from your checking account while in another country: $135.25.

If this information is not correct, someone unknown may have access to your account. As a safety measure, please visit our website via the link below to verify your personal information:

http://www.trustedbank.com/general/custverifyinfo.asp

Once you have done this, our fraud department will work to resolve this discrepency. We are happy you have chosen us to do business with.

Thank you,
TrustedBank

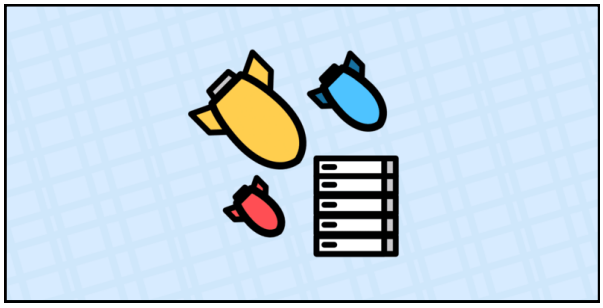
Member FDIC © 2005 TrustedBank, Inc.

BRUTE FORCE ATTACK

One way to try to guess somebody's password is to simply try every single possible combination of passwords available until the correct one is found. This is called a brute force attack.

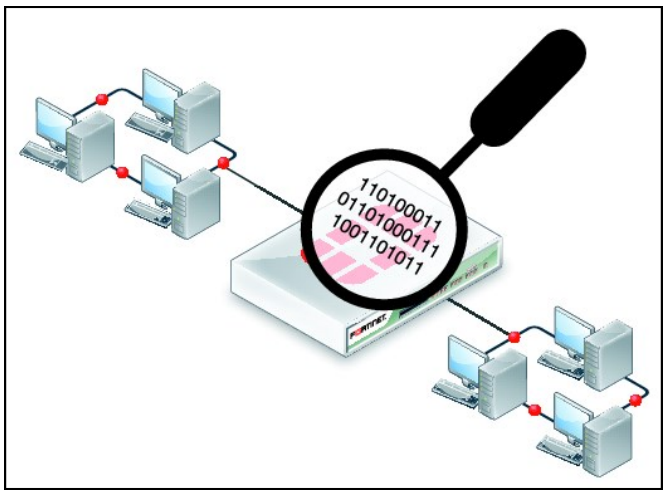
The longer the password and the wider range of characters (e.g. numbers, letters, special characters) the harder it is to do this sort of attack.

DENIAL OF SERVICE ATTACK



A web server is flooded with requests so that it cannot cope with the demand and either shuts down or stops being able to answer the real requests.

DDoS (distributed denial of service attack) is a variant of this and involves the hacker taking over a whole host of computers and using them to perform the attack in unison. This makes it much harder to stop as the attacks are coming from different locations all around the world.



DATA INTERCEPTION AND THEFT

Each time any communication is sent across a network, whether it is a Local Area Network or a Wide Area Network, it is split up into packets and sent by various routes. As they travel from one part of the network to another, they are at risk of being intercepted, read, altered or deleted.

One way data can be intercepted is if someone uses some hijacking software and pretends to be the destination for communications across a network. Another way is for a user to use 'packet sniffing' software and hardware to monitor network traffic and intercept those packets it is interested in. People using packet sniffers are especially looking for plain text files, passwords and set-up information being set across the network, which they can steal, analyse and extract information from.

SOCIAL ENGINEERING

This includes any number of techniques designed to trick people into giving away crucial data or passwords. Effectively this is the same as an old fashioned “con”. Some of the scams available include:

- Pretexting—impersonating a trusted source like a police officer or bank clerk
- Phishing—see above
- Tailgating—looking over someone’s shoulder to see their PIN
- Quid quo pro—phoning up pretending to be from technical support

POOR NETWORK POLICY

Every good network should have policies in place to prevent users doing harmful things. If these policies are not there then the network is at risk. Network policies might state:

- Users should not access any account they are not authorised to
- Users should refrain from viewing illegal, defamatory or pornographic content
- Users should refrain from downloading files without knowing their source
- Users should not click on links in emails without knowing their source.

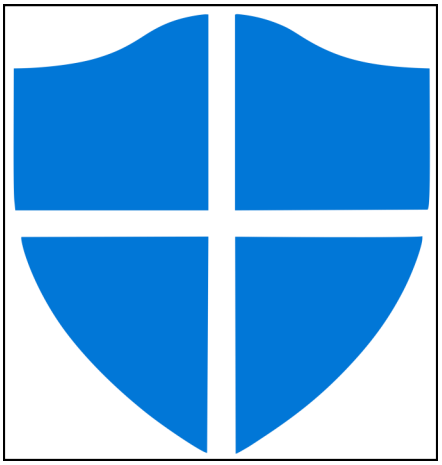
Ways to Protect

PENETRATION TESTING

Sometimes called pen testing. This is when a company hires somebody with hacking skills to try to break into their system. If they are successful they can tell the company the weaknesses so that they can fix them and protect themselves from real attacks.

NETWORK FORENSICS

The process of monitoring and analysing traffic on a network. It will allow you to see which users are performing suspicious actions and can be used to find the source of attacks.



NETWORK POLICIES

Rules for using a network that users have to agree to before they can touch a computer. Often this will include items such as agreeing not to install software, not to look at inappropriate content and not to create malware .

ANTI-MALWARE SOFTWARE

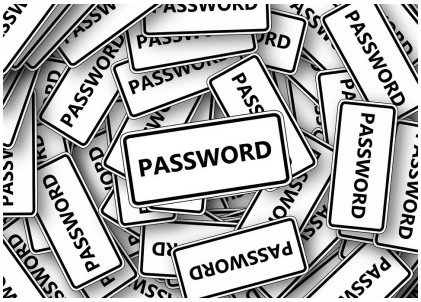
Protection software that stays in the computer's memory. It is constantly scanning the drives and memory for any malicious software. It compares suspicious items with a known database of threats and reports it to you when there is a match. You can then choose to quarantine the file or delete it.

FIREWALLS

Scans files as they come into your system from across a network or the internet. It will let you know if anything looks suspicious and you can set it to block certain types of files or files from certain sources.

USER ACCESS LEVELS

Means that you can allow only partial access to your system to different users. For example, a pupil in a school won't be able to access as many files as a teacher and the teacher won't be able to access as many files as the network administrator.



PASSWORDS

Strong passwords can help to protect against brute force attacks. The longer the password the better and it helps if it contains numbers, a mix of capital and lowercase letters and special characters. Favourite football teams or pet names should be avoided!

ENCRYPTION

Scrambles up data before it is sent across a network or the internet. Only the person who knows the secret encryption key can unscramble it so it doesn't matter if it is intercepted by criminals.

INPUT SANITISATION

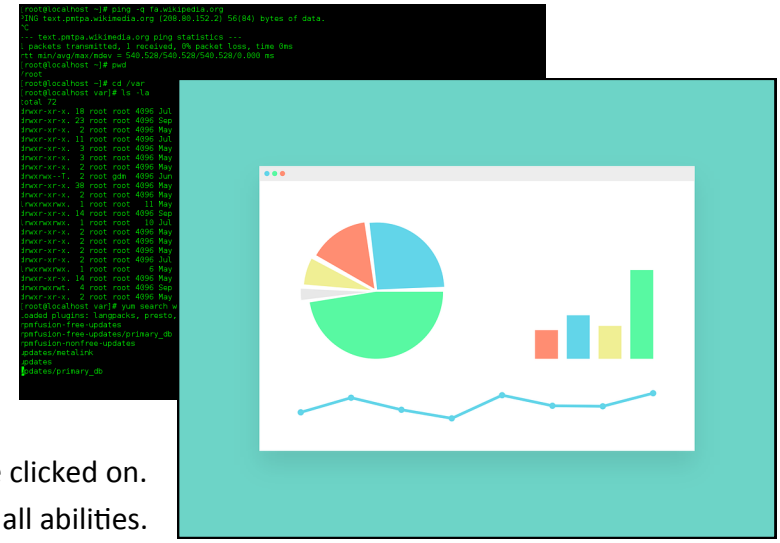
Takes data that has been entered into a form on a webpage and removes any malicious code from it. Techniques involve removing any special characters and using a feature called prepared statements that convert strings into correct SQL statements.

Systems Software

DEFINITION

Systems software provides an interface between the hardware and software and is used to control the hardware.

FUNCTIONS OF AN OPERATING SYSTEM

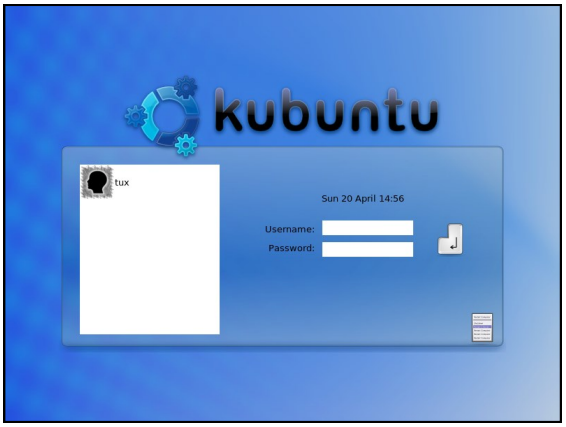


User Interface— This is the part of the OS that you can see. A user interface lets you enter commands and lets the OS display the results of those commands. Two types:

- CLI—Command Line Interface: commands are entered by typing them in. Very fast and powerful but only suitable for expert users.
- GUI– Graphical User Interface: commands are entered using a mouse / touchscreen and icons are clicked on. Slower and less powerful than a CLI but suitable to all abilities.

Memory Management—let's memory be shared so more than one process can be stored in RAM at once. This means that modern operating systems are usually **multi-tasking** i.e. they let you run lots of programs at the same time. Memory management also controls the use of **virtual memory** (see memory section).

Peripheral Management– a peripheral is a device you plug into your computer. It might be a mouse, keyboard, scanner, camera or any other. The operating system uses **device drivers** to act as a link between the hardware of the device and the software of the OS.



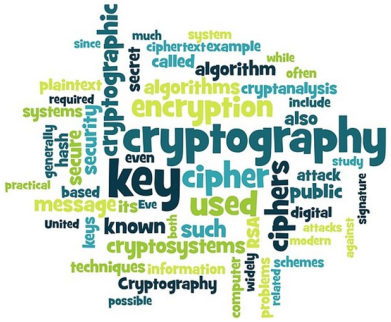
User Management– lets you have different log ins for different users. Each user might have different privileges (user access levels).

File Management– lets you organise your files into folders. Also lets you compress files to make them smaller and there might be some utilities for cleaning up old files.

Utility Software

DEFINITION

Software that fixes problems on your computer or maintains the good working order of your computer.



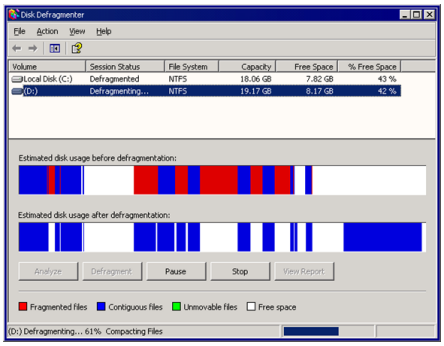
ENCRYPTION

Encryption takes data and scrambles it up so that it cannot be read.

Only if somebody has the correct password (called the key) can they unscramble the data and read what is inside.

This is particularly useful for sending data across the internet and is used in online shopping to protect credit card details.

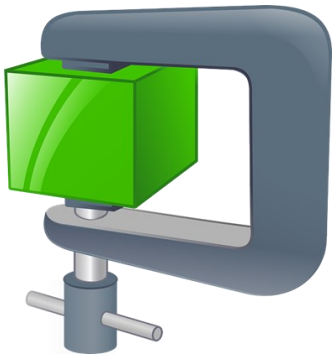
DEFRAGMENTATION



When a hard drive writes data it puts it onto the disk in no particularly order.

This can mean that files can get scattered across the disk – they become fragmented.

A defragmenter aims to put all the bits of related files together. This speeds up the hard disk as you don't need to keep going to all four corners to read files that are associated with each other. It can also free up space.



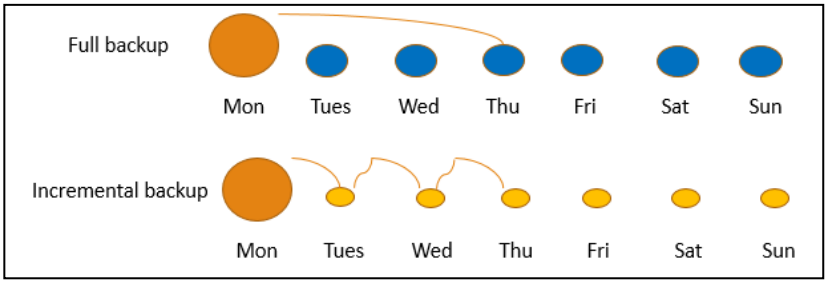
DATA COMPRESSION

Makes a file smaller so that it takes up less space and can be transferred faster.

It is possible to compress all the files on your disk. This gives you more space but is slower.

Two types = lossy and lossless.

BACKUP



A backup utility makes a copy of all your important files and documents and stores it somewhere else.

This is good as it means if your main drive fails you don't lose all your data.

A **full backup** will backup every necessary part of the system in one huge block. This is very systematic but takes a long time.

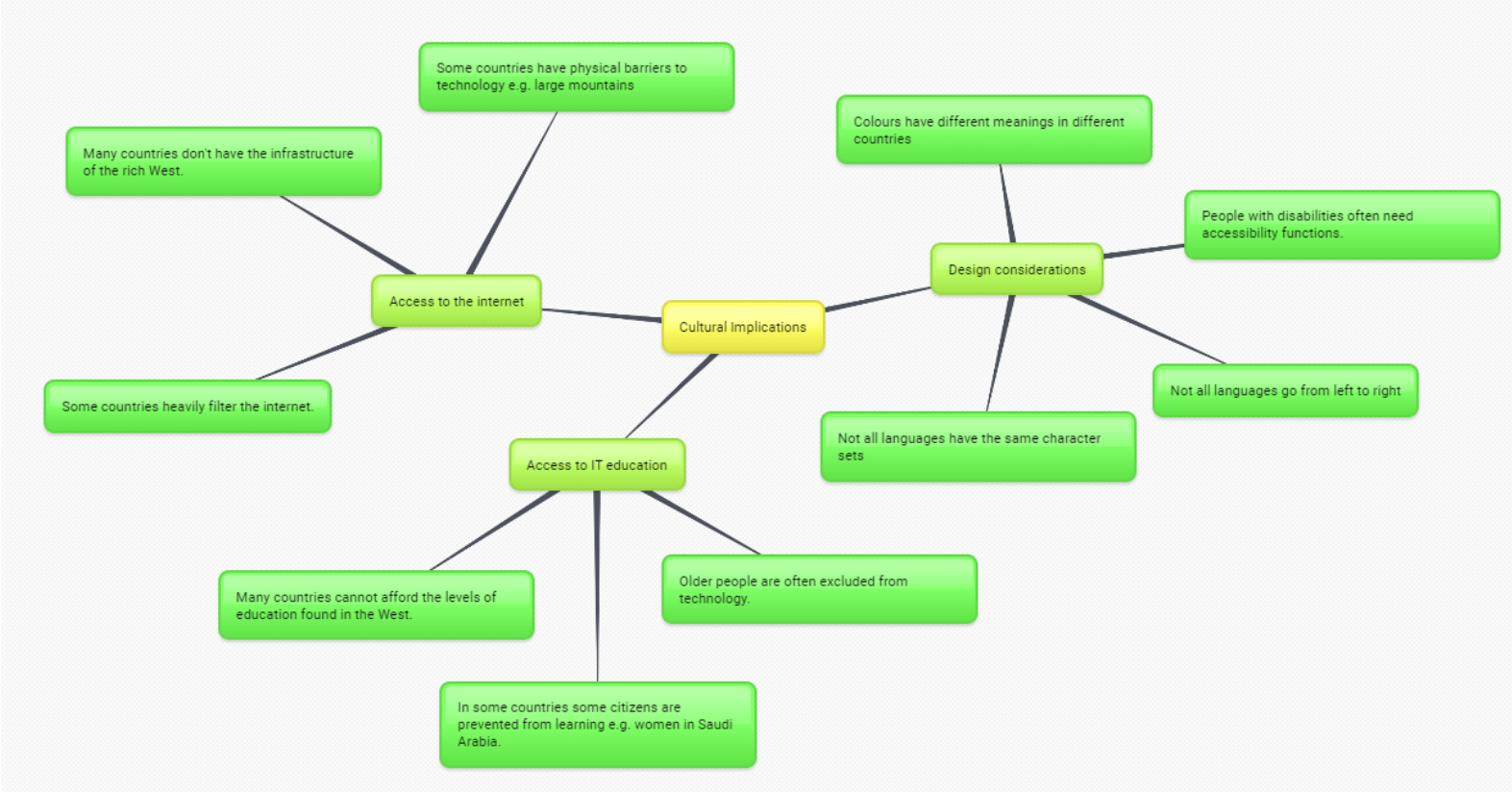
An **incremental backup** will only backup files that have changed since the last full backup. This is quicker to perform but it is harder to restore files from.

Ethical, Legal, Cultural and Environmental

ENVIRONMENTAL EFFECTS

GOOD	BAD
Using computers saves paper: • Emails reduce the amount of letters we send • Digital storage reduces the amount of paper files we keep	Computers use energy! Energy means fossil fuels are burned which increase climate change.
Using video conferencing services has reduced the need to travel for meetings	Computers are full of noxious chemicals that cannot easily be disposed of. Most of these chemicals end up in landfill sites damaging the environment for decades to come.
People can now work from home by dialling into their work's server. This reduces commuting and thus reduces traffic and pollution.	

CULTURAL IMPLICATIONS



LEGAL IMPLICATIONS

LAW	DESCRIPTION	DETAIL
The Data Protection Act 1998	The law that prevents the misuse of your personal information.	8 principles: 1. Data will be processed fairly and lawfully. 2. Data will only be used for the purpose it was gathered for. 3. Data will be adequate, relevant and not excessive. 4. Data will be accurate and up to date. 5. Data will not be held for longer than necessary. 6. Data will be processed with the rights of the data subjects. 7. Companies will protect against unauthorised access to data 8. Data will not be shared outside the European Economic Area.
Computer Misuse Act 1990	The law that stops people causing harm using computers.	Crimes are: Hacking (unauthorised access to a computer system). Creating malware.
Freedom of Information Act 2000	The law that lets the public have any information held by the government	Anybody can make a freedom of information request to the government for virtually any data they hold. There are some exceptions: • You can't ask for specific data about an individual e.g. somebody's medical history. • Data kept for national security e.g. military data
Copyright Design and Patents Act 1998	The law that protects published works and makes sure that only their creators get the rewards.	Any work that has been published e.g. book, film, music, software, TV show is covered by copyright law. The law states that the owner of the copyright has the right to be paid for the work they have done. Any copying or redistributing of the work is illegal.
Creative Commons Licensing	A type of license that means the author gives their work away	The creator of a work puts this license on whenever he wants people to be able to freely distribute it without fear of breach of copyright.

OPEN SOURCE VS CLOSED SOURCE

Type	Description	Advantages	Disadvantages
Open Source	Source code is published with the software. Often distributed free of charge.	You can edit the source code to customise it	Not as much support available or you may need to pay for it
		It's often free!	You need to be an expert to edit code
		A community of enthusiasts keep updating it	Not normally as many features as proprietary
Proprietary	You need to buy a license to use the software. Can be bought in shops or downloaded	High quality software with lots of features	You have to pay!
		Help and support provided	Not as customisable
		Updates provided by professionals	Can sometimes be too generic for specialist purposes

STAKEHOLDERS

A stakeholder is quite simply anybody who has an interest in a computer system or piece of software.

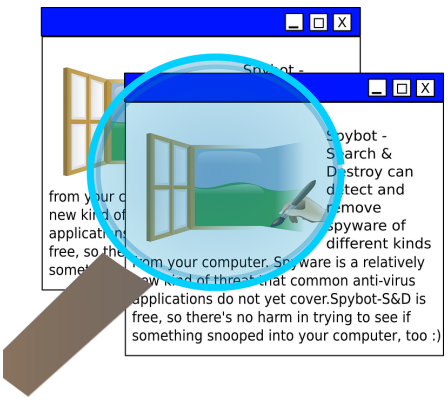
It could include:

- The customers.
- The developers.
- The staff in the PC shop who sell it.
- The support staff.
- The delivery men.

PRIVACY

Privacy is simply the right that all people have to not be watched. Many people feel this right is being eroded away in modern society:

- CCTV cameras are found in most town centres.
- Number plate recognition systems track your car wherever you go.
- Phone GPS systems can track your movements on foot.
- Your ISP can keep records of your internet habits.
- Your phone can be tapped by police under certain circumstances.



Many citizens have tried to combat this by using technologies that mask their IP addresses and encrypt their messages but the government is often pushing for even more control.