

OCR GCSE Computer Science (J277)

Revision Guide



Covering the 9 – 1 specification

Use this revision guide to help you revise the theory you learn in lessons, and practice the exam questions at the end of each topic

Paper 1

Contents:

	<u>Pages</u>
1.1 Systems Architecture	3 – 17
1.2 Memory and Storage	18 – 86
1.3 Computer Networks, Connections and Protocols	87 – 129
1.4 Network Security	130 – 144
1.5 Systems Software	145 – 162
1.6 Ethical, Legal, Cultural, Environmental ...	163 – 183
Additional Resources	184 – 188



“I’m your guide to revision! I’ll be pointing out key things to remember across different parts of each topic. Look out for me!”



All technical terms and definitions can be found at the start of each topic. All technical terms within each topic are in **red**



It’s your turn!

Look out for opportunities to answer exam style questions on specific aspects of each topic

1.1 Systems Architecture

In this section you will revise the following:

1.1.1 Architecture of the CPU

- The purpose of the CPU:
 - The fetch-execute cycle
- Common CPU components and their function:
 - ALU (Arithmetic Logic Unit)
 - CU (Control Unit)
 - Cache
 - Registers
- The Von Neumann Architecture:
 - MAR (Memory Address Register)
 - MDR (Memory Data Register)
 - Program Counter
 - Accumulator

1.1.2 CPU Performance

- How common characteristics of CPUs can affect their performance:
 - Clock Speed
 - Cache Size
 - Number of Cores

1.1.3 Embedded Systems

- The purpose and characteristics of embedded systems
- Examples of embedded systems



Technical Terms

Technical Term	Definition
Computer Architecture	This is the internal, logical structure and organization of the computer hardware. It is how all the different pieces of the computer fit together and work together efficiently
Von Neumann Architecture	<p>The Von Neumann Architecture explains how all devices follow a general rule when processing information. All data and programs are stored in the computer's memory and are stored as binary digits (0s and 1s).</p> <p>Input – Data is inputted into the device via an input device (e.g. keyboard, mouse, microphone etc.)</p> <p>CPU – Data is processed by the CPU, via the Control Unit and ALU</p> <p>Memory Unit – Data is transferred between the CPU and the computer's memory</p> <p>Output – Finally, once processed, the data is outputted to the user via an output device (e.g. monitor, speakers, printer etc.)</p> <div style="text-align: center;"> <pre> graph LR ID[Input Device] --> CPU subgraph CPU [Central Processing Unit] CU[Control Unit] ALU[Arithmetic/Logic Unit] end MU[Memory Unit] CPU <--> MU CPU --> OD[Output Device] </pre> </div>
Input Device	A device we use to send information into the computer e.g. mouse, keyboard, microphone etc.
Output Device	A device we use to send information out of the computer e.g. monitor, speakers, printer etc.
CPU (Central Processing Unit)	This is the brain of the computer. It processes all instructions given to it by the user, using the fetch, decode, execute cycle
Hz (Hertz)	This is what we measure the speed of a CPU in. 1Hz = 1 instruction that can be executed per second. Common speeds of CPU's are now measured in Megahertz (MHz) or Gigahertz (Ghz)

Instruction	This is something that has been requested by the user, that the CPU must carry out
Clock Speed	This is the speed of a CPU, which tells us how many instructions can be carried out each second. For example, a 2GHz CPU would be able to carry out 2,000,000,000 (2 billion) instructions per second
Core	This is the number of processors within a CPU, that can carry out instructions. Processors can be multi-core (e.g. Dual Core, Quad Core etc.) Each core executes instructions independent to the other cores
Cache	The is memory located on the processor chip. It acts as a very small amount of memory located in between the processor and Main Memory (RAM). We store frequently used instructions here to make accessing them quicker and easier
Efficiency	Completing a task as quickly as possible, without affecting the quality of the result
Fetch, Decode, Execute cycle	<p>This is the cycle the CPU goes through in order to process an instruction:</p> <p>Fetch – An instruction is fetched from memory (RAM) Decode – The instruction is broken down into small instructions, and converted into a language the CPU understands (binary) Execute – The instruction is executed, and the user receives what they requested e.g. a program opening up</p> <p>As this is a cycle, once the CPU executes an instruction, it goes back to the start and fetches a new instruction, and the process happens again</p>
ALU (Arithmetic Logic Unit)	This performs all arithmetic (addition and subtraction) and logical (greater than, less than, equal to) operations within the CPU
CU (Control Unit)	This works with the CPU to control the flow of data within the system and to decode instructions
Register	This is a small amount of memory within the CPU. There are a variety of registers, all of which do different jobs
MAR (Memory Address Register)	This stores the address of the data or instruction that is currently being accessed by the CPU
MDR (Memory Data Register)	This stores the data or instruction that is currently being accessed by the CPU

Program Counter	This stores the address of the next instruction to be processed, which then goes onto the MAR
Accumulator	This temporarily stores data whilst calculations are being processed by the ALU
Embedded System	<p>Performs a single task within a larger piece of equipment. It is a small processor that is inside a large piece of equipment, dedicated to a single task</p> <p>Examples of embedded systems – Washing Machine, Dishwasher, DVD Player, Microwave, Games Console, Mobile Phone etc.</p>

The CPU

The **CPU (Central Processing Unit)** is the most important element of any computer system, we often think of it as the brain of the computer.

The CPU is a small chip that is located on the motherboard of a computer system. A CPU is measured in Hertz (Hz). The higher the Hz, the faster the CPU will be, and the more instructions that can be executed every second. Typically, a CPU today is often measured in Gigahertz (GHz). This means, for example, a 2GHz CPU will be able to execute 2,000,000,000 (2 billion) instructions every second.



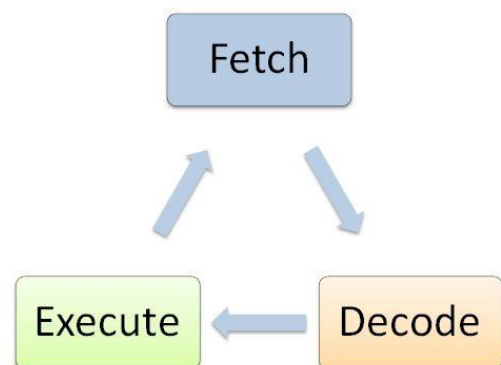
“Remember not to get caught out by numbers! Imagine you had two CPUs. The first CPU is 3GHz, the second CPU is 10MHz. Even though 10 is bigger than 3, we look at the measurement. 1MHz = 1,000,000 (1 million). 1GHz = 1,000,000,000 (1 billion). Therefore, the first CPU is faster as it can execute 3 billion instructions every second, compared to the second CPU which can only execute 10 million instructions every second”

The CPU is responsible for processing all instructions that are given to the computer by the user. It processes each of these instructions individually. In order to process these instructions, it follows a specific cycle. This is known as the **Fetch, Decode, Execute Cycle**:

Fetch — In this stage an instruction is fetched from **Main Memory (RAM)**. The oldest instruction is always fetched

Decode — In this stage the instruction is broken down and converted into a language that can be understood (binary)

Execute — In this stage the instruction is executed and carried out, and the user receives what they requested



As this is a cycle, once an instruction has been executed, the cycle begins again. A new instruction is fetched, and the process happens again.

For this cycle to work however, it requires different parts of the CPU to all work together. These are the **CU (Control Unit)**, **ALU (Arithmetic Logic Unit)**, **PC (Program Counter)**, **MDR (Memory Data Register)**, **MAR (Memory Address Register)**, and **Accumulator**.

If we now break the Fetch, Decode, Execute cycle down again, we can see where these different parts of the CPU undertake their role:

Fetch:

In order to fetch the correct instruction, the processor looks to **the PC (Program Counter)**. This register records the address of the next instruction to fetch. Once fetched, the data is stored in the **MDR (Memory Data Register)**, which holds the data of the current instruction being fetched. As well as this, the address of the data being fetched is also stored, in the **MAR (Memory Address Register)**.

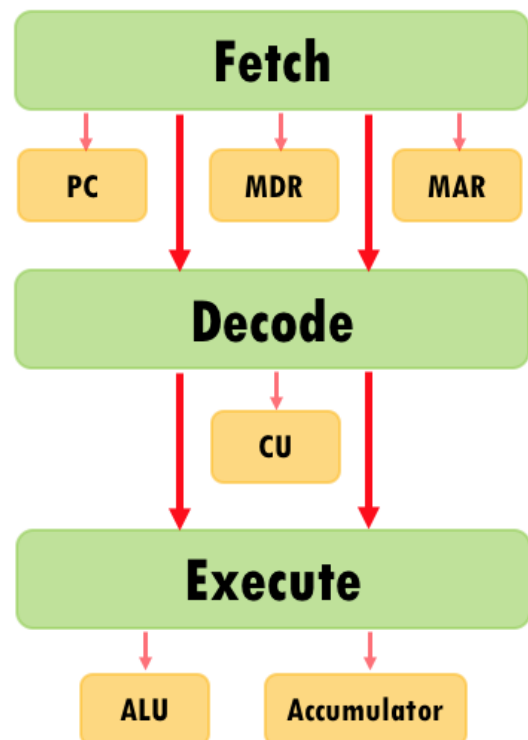
Once this above process is complete, the **Program Counter** will update so it now stores the address of the next instruction to fetch, once the current instruction has been executed.

Decode:

In order to execute an instruction, the **CU (Control Unit)** now has to determine what instruction it is. For example, is it data from an input device? Is it data from an output device?

Does the processor need to perform a mathematical or logical operation on the data? In order to understand this, it breaks the instruction down and converts it into machine language, or binary.

If further instructions are required from memory in order to execute the instruction, the **Control Unit** will control the flow of data here in and out the CPU, so the instruction can be executed.



Execute:

Once the instruction has been decoded, the instruction is ready to be executed. The **ALU (Arithmetic Logic Unit)** may now be required, to perform any arithmetic (addition, subtraction etc.) or logical (greater than, less than, equal to etc.) operations on the data. Whilst the **Arithmetic Logic Unit** performs these operations, the **Accumulator** will store any data necessary whilst these operations are completed.

As then mentioned before, the cycle then repeats itself.



“Remember, a register is a small amount of memory within the CPU. There are many registers that all do different jobs!”

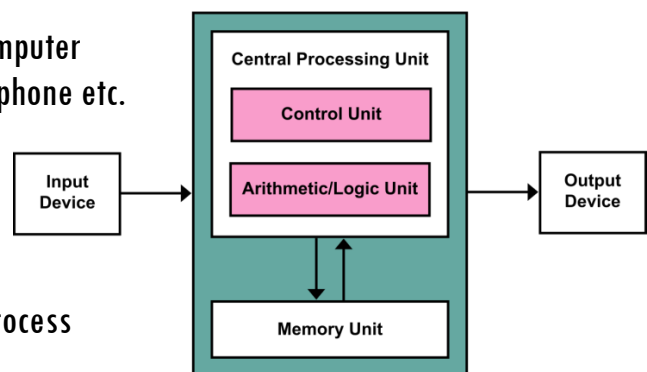
This process above, involving the Control Unit, Arithmetic Logic Unit, and different registers, is known as **The Von Neumann Architecture**.

A **Computer Architecture** is the internal, logical structure and organization of the computer hardware. It is how all the different pieces of the computer fit together and work together efficiently

John Von Neumann explained his architecture as how all devices follow a general rule when processing information. All data and programs are stored in the computer’s memory and are stored as binary digits (0s and 1s).

Input Device — Here data is inputted into the computer via an input device e.g. Keyboard, Mouse, Microphone etc.

CPU — Instructions are processed by the CPU. The CPU contains the Arithmetic Logic Unit and Control Unit, both of which undertake separate roles in the process



Memory Unit — Data is transferred between the CPU and the computer’s memory

Output Device — Here data is outputted by the computer via an output device e.g. Screen, Speakers, Printer etc.

Describe four stages in the Fetch-Decode-Execute Cycle

[4]

It's your turn!

1. _____

2. _____

3. _____

4. _____

Describe the role of the Control Unit in processing instructions

[2]

Factors that affect the performance of the CPU

There are certain factors that can affect how efficiently the CPU can perform. These factors can all affect how fast the CPU can process all the instructions given to it by the user. There are three factors we need to be aware of. These are **Clock Speed**, **Number of Cores**, and **Cache Memory**.

Clock Speed:

The Clock Speed is the number of Fetch, Decode, Execute cycles that can be completed every second, and is measured in Hertz (Hz). For example, a CPU with a 2GHz Clock Speed will be able to perform 2,000,000,000 (2 billion) Fetch, Decode, Execute cycles every second.

The higher the Clock Speed is, the more instructions the CPU can process every second, and the less likely we are to experience the computer slowing down.

Number of Cores:

A core is a processor within the CPU. The more processors we have in the CPU, the more instructions that can be carried out at once. Imagine we had 20 maths problems to solve. On the first team there were five students. On the second team there was only one student. Who would complete the maths problems first?

The first team would of course. This is because they could split up the tasks and complete multiple problems at the same time, compared to the second team who would only complete one problem at a time.

This is the same for the CPU. The more cores we have, the more instructions that can be carried out at once. CPUs could be single core (1 processor), dual core (2 processors), or quad core (4 processors). The more cores we have, the better our CPU can perform.

Cache Memory:

Cache Memory is a small amount of memory located on the CPU, that acts as memory between the CPU and RAM (Random Access Memory). Frequently used instructions are stored here. It is quicker to access the instructions stored in Cache Memory as it is closer to the CPU than RAM. However, it is only small. The bigger our Cache Memory is, the more instructions can be stored in here, improving the performance of the CPU.



Look at the table below:

Computer A	Computer B
Quad Core Processor	Dual Core Processor
2.4 GHz Processor	2.2 GHz Processor
256 KB Cache Memory	256 KB Cache Memory

Explain two reasons why Computer A would perform better than Computer B

[4]

Embedded Systems

An **Embedded System** is a computer system with a dedicated function within a larger computer system. An Embedded System is dedicated to a single task

There are many different examples of embedded systems. These include:

- Washing Machines
- Dishwashers
- DVD Players
- MP3 Players
- Mobile Phones
- Games Consoles
- Microwaves



“Often, in the exam, they will ask you to give a brief description of what an embedded system is, and then ask you to provide examples of embedded systems. Make sure you remember some of the above as examples!”

Past Exam Questions

Answer the questions below, to help you revise what has been covered in 1.1 Systems Architecture.

1. John is buying a new computer. He has been told the CPU is an integral part of a computer system.

a. What does CPU stand for? [1]

b. Describe three factors specific to the CPU John should consider when buying a new computer [6]

- c. When John is looking at computers, he notices that Computer A is dual core, and Computer B is quad core.

i. Describe what is meant by a core [1]

ii. Explain which computer would be better for John to buy based on the number of cores [2]

2. Look at the table below. Tick **one** box in each row to show whether each statement is True or False [5]

Statement	True	False
CPU stands for Central Processing Unit		
The CPU fetches and decodes instructions		
The speed of a CPU is usually measured in GigaHertz (GHz)		
If a CPU has many cores, this slows the computer down		
The hard disk drive is part of the CPU		

3. Describe four stages that occur in the Fetch, Decode, Execute Cycle [4]

- 1. _____

- 2. _____

- 3. _____

- 4. _____

4. Describe the role of the Memory Address Register and Memory Data Register when processing instructions [2]

- _____
- _____
- _____
- _____

5. Identify two components, other than the CPU, that can be upgraded in order to improve the performance of a computer [2]

- 1. _____
- 2. _____

6. John buys a new washing machine. He is told it is an embedded system.

i. Describe what is meant by an 'embedded system' [1]

ii. Other than the example given above, identify two examples of embedded systems [2]

1. _____

2. _____

1.2 Memory and Storage

In this section you will revise the following:

1.2.1 Primary Storage (Memory)

- The need for primary storage
- The difference between RAM and ROM
- The purpose of ROM in a computer system
- The purpose of RAM in a computer system
- Virtual Memory

1.2.2 Secondary Storage

- The need for secondary storage
- Common types of storage:
 - Optical
 - Magnetic
 - Solid State
- Suitable storage devices and storage media for a given application
- The advantages and disadvantages of different storage devices and storage media relating to these characteristics:
 - Capacity
 - Speed
 - Portability
 - Durability
 - Reliability
 - Cost

1.2.3 Units

- The units of data storage:
 - Bit
 - Nibble (4 bits)
 - Byte (8 bits)
 - Kilobyte (1,000 bytes or 1Kb)
 - Megabyte (1,000 Kb)
 - Gigabyte (1,000 Mb)
 - Terabyte (1,000 Gb)
 - Petabyte (1,000 Tb)
- How data needs to be converted into a binary format to be processed by a computer
- Data capacity and calculation of data capacity requirements

1.2.4 Data Storage

- Numbers:
 - How to convert positive denary whole numbers to binary numbers (up to and including 8 bits) and vice versa
 - How to add two binary integers together (up to and including 8 bits) and explain overflow errors which may occur
 - How to convert positive denary whole numbers into 2-digit hexadecimal numbers and vice versa
 - How to convert binary integers to their hexadecimal equivalents and vice versa
 - Binary shifts
- Characters
 - The use of binary codes to represent characters
 - The term 'character set'

- The relationship between the number of bits per character in a character set, and the number of characters which can be represented, e.g.:
 - ASCII
 - UNICODE
- Images:
 - How an image is represented as a series of pixels, represented in binary
 - Metadata
 - The effects of colour depth and resolution on:
 - The quality of the image
 - The size of an image file
- Sound:
 - How sound can be sampled and stored in digital form
 - The effect of sample rate, duration, and bit depth on:
 - The playback quality
 - The size of a sound file

1.2.5 Compression

- The need for compression
- Types of compression:
 - Lossy
 - Lossless



Technical Terms

Technical Term	Definition
Main Memory	This is the main storage within a computer, which the CPU has direct access to. This is RAM (Random Access Memory)
RAM (Random Access Memory)	This is also known as the Main Memory within a computer system. RAM stores all the open programs and files. When a program/file is loaded, it is opened from Secondary Storage, and stored in the RAM. This is so the CPU can access the program/file and its data quickly
ROM (Read Only Memory)	This is the memory within a computer system that stores the program for booting up the computer system.
BIOS (Basic Input/Output System)	This is the program that stores all the instructions for booting up the computer system, such as instructions for the input devices to work. It also loads the Operating System, which allows the user to actually interact with the device.
Volatile	This means when the device is turned off (there is a loss of power), the contents of the memory are all deleted/lost. RAM is volatile, ROM is not volatile.
Rewritable	This means the contents of the memory can be changed. RAM is rewritable, ROM is read only (not rewritable)
GB/MB/KB	GB – Gigabyte MB - Megabyte KB – Kilobyte These are all the different memory sizes. ROM is usually measured in KB/MB. RAM is usually measured in GB
Virtual Memory	Virtual Memory refers to how the computer continues to operate once the RAM becomes full. Rather than stopping working when the RAM becomes full, the computer partitions (splits off) a section of the internal hard drive. This section then acts as additional RAM, allowing the computer to continue functioning. However, this greatly affects the performance of the computer, slowing it down. This is because data must be swapped between the virtual memory and RAM when being actively used.

SSD (Solid State Drive)	This is an example of Flash Memory. It acts as a permanent storage in a computer system. It behaves in the exact same way to a Hard Disk, however, is much lighter and can work much quicker, due to having no moving parts. However, it is more expensive than a Hard Disk, and therefore is still emerging.
Secondary Storage	This is where we store for longer than just whilst the computer is turned on. It is not volatile, and therefore data remains even after the power has been turned off.
Optical Storage	<p>This is a type of Secondary Storage.</p> <p>Optical Storage is used within an Optical Drive, where a laser is shone at the surface of the disc, and then processing the reflection from the disc. Optical Storages are discs, and examples are CDs, DVDs, and Blu-Rays.</p> <p>CD-R, DVD-R – Read Only, so the contents cannot be changed</p> <p>CD-RW, DVD-RW – Rewritable, so the contents can be changed</p>
Magnetic Storage	<p>This is a type of Secondary Storage.</p> <p>Data is stored on Magnetic Storage via magnetised dots. Magnetic Storage often has moving parts. An example of Magnetic Storage is an Internal Hard Disc Drive.</p>
Solid State Storage	<p>This is a type of Secondary Storage.</p> <p>Data is stored on Solid State Storage via electricity. It is becoming increasingly popular as its capacity increases, and its cost decreases. Examples of Solid-State Storages are Memory Sticks, SSDs, and SD Cards.</p>
Capacity	This refers to the amount of data that can be stored on the media. The higher the capacity, the more data it can store without becoming full.
Speed	This refers to the speed in which the data can be read and transferred. The higher the speed, the faster data can be read and transferred to and from the media.
Portability	This refers to how easy the media is to transport and move around from one place to another. The better

	the portability, the easier it is to move the device from one place to another.
Durability	This refers to how robust the media is, how likely it is to break when shaken or dropped. The better the durability, the less likely the device is to break or lose data if dropped or shaken.
Reliability	This refers to how likely it is to be able to be used repeatedly, without failing. The better the reliability, the less likely the media is to fail over time.
Cost	This refers to how expensive the media is to buy. The better the cost, the cheaper the media is to buy.
Unit	Used as a measurement of storage. The order is as follows: Bit – Nibble – Byte – Kilobyte – Megabyte – Gigabyte – Terabyte – Petabyte
Binary	This is the language of the computer. Binary is used to represent all data within a computer system. It refers to transistors opening and closing allowing electricity to pass through or not, which is then represented using 1's (ON) and 0's (OFF)
Denary	Our number system which utilises 10 numbers (0-9).
8 bit Binary	Used when there are 8 bits used to represent a number. The maximum number that can be represented using 8 bits is 255 (11111111).
Overflow Error	Occurs when two binary numbers are added together, and the resulting number has 9 bits rather than 8. The 9 th bit cannot be stored and is therefore lost.
Binary Shift	The process of moving bits within a binary number either to the left (binary shift left) or to the right (binary right shift). A right shift effectively halves the original number, and a left shift effectively doubles the original number.
Hexadecimal	Used by computer scientists to represent binary numbers. Is called a base 16 system as it uses 16 characters (0-9, A-F). The maximum number that can be represented using 2 hexadecimal characters is 255 (FF).
Character Set	The characters that are defined and recognised by the computer hardware and software. The size of the

	character set is dependent on the number of bits being used per character.
ASCII	Has a character set of 128 characters, as it only uses 7 bits per character.
Extended ASCII	Has a character set of 256 characters, as it uses 8 bits per character.
UNICODE	Uses multiple bytes to represent each character (depending on the UTF), and therefore has a character set of over 1 million.
Pixel	An individual 'square' on an image. Images are made up of millions of pixels. The more pixels the greater the quality of the image. Each pixel is a colour which is represented in binary
Metadata	Additional data stored about the image which allows the computer system to build the image on the screen. Some data stored here is the height of the image (in pixels), the length of the image (in pixels), the bits per pixel, GPS location etc.
Colour Depth	This refers to the number of bits per pixel, and therefore the number of colours that can be represented in an image. The greater the colour depth the more colours that can be in an image, however the larger the file size will be.
Resolution	This refers to the number of pixels within an image. The greater the resolution the better the quality of an image will be, however the larger the file size will be.
Sound Sampling	This refers to the process of converting an analogue wave into a digital wave. The computer takes measurements of the wave at different time intervals known as a sampling interval. Each sampling interval is stored as a binary number. These samples are then pieced together to create a digital wave.
Sample Size	Total number of bits in a sound. Can be calculated by multiplying the bit depth by the number of samples per second, multiplied by the number of seconds.
Bit Rate	This refers to the number of bits (or amount of data) stored per sample. The higher the bit rate, the better the quality of the sound. The bit rate for audio is often referred to as kbps (kilobytes per second).
Sampling Frequency	This refers to the number of samples stored per second. The greater the number of samples the better the digital wave will represent the original analogue wave.

Compression	The process of reducing the size of a file by changing its attributes. There are two types of compression, lossy and lossless.
Lossy Compression	A type of compression. This reduces the size of the file by removing data. Lossy compression can be used on files such as images with little to no difference from the original (depending on the level of compression).
Lossless Compression	A type of compression. This reduces the size of the file by rewriting the data in a more efficient way. No data is lost or deleted when lossless compression is used. Lossless compression can be used on files such as spreadsheets or text documents where data cannot be erased/removed.

RAM and ROM

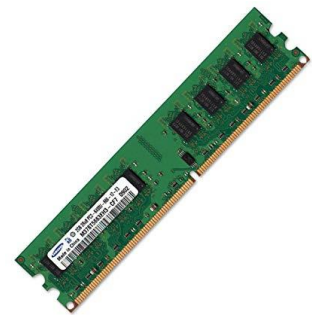
Just like we discussed in the previous topic about the CPU, both **RAM (Random Access Memory)** and **ROM (Read Only Memory)** play important roles in a computer system.

However, they both do different jobs. There are also some differences between RAM and ROM, other than their job roles, that we need to know.

RAM:

RAM stands for **Random Access Memory**. It is also referred to as the computers **Main Memory**. This is because it is the memory that the CPU has direct access to.

The job role of RAM is to store all the computers open programs and files. When a program/file is loaded up, it is opened from Secondary Storage (we will cover this in a later topic) and stored in the RAM. This is so the CPU can access the program/file and its data quicker.



“You can see on your computer which programs and files are stored in your RAM. It is all the programs and files that are open at the bottom of your screen. As soon as you open a program or file it goes straight into your RAM. As soon as you close it, it is removed from the RAM and stored back in Secondary Storage, freeing up space for a new program or file!”

The process for loading up a program or file is:

1. The user clicks on a program or file to open it up
2. The program or file is loaded from the hard drive (Secondary Storage)
3. It is stored in the RAM so the CPU can access it quickly
4. The user uses the program or file
5. Once finished, the user closes down the program or file. It is then removed from the RAM, and stored back in the hard drive

ROM:

ROM stands for **Read Only Memory**. It is called Read Only because it is not **rewritable**, therefore it can only be read (it cannot be changed).

The job role of ROM is to store the program required for booting up (loading up) the computer system. This program is called the **BIOS (Basic Input/Output System)**.



The BIOS stores all the instructions for the computer system to boot up and work. For example, the BIOS would contain the instructions necessary for any input or output devices to work. The most important part of this program is the **Operating System**. This allows the user to interact and use the device. An example of an Operating System is Windows.

The process for ROM working is:

1. The user turns on the device
2. ROM runs the boot up program (BIOS) which loads everything the device requires to work
3. The Operating System is then loaded, which allows the user to interact with the device
4. Once the device is loaded up, ROM has no more work to do

It's your turn!

Describe the roles of RAM and ROM in a computer system

[4]

Hint: The question is worth 4 marks. You need to state what both RAM and ROM stand for, and then describe both their job roles to get full marks

RAM and ROM: The Differences

There are some key differences between RAM and ROM that must be remembered for the exam.

RAM	ROM
<p>RAM is volatile. This means when the device is turned off (there is a loss of power) all the contents of RAM get deleted.</p> <p>This means next time you turn on the device, RAM is empty. This is why when you turn off your computer and then load it back up, there are no programs already open.</p>	<p>ROM is not volatile. This means when the device is turned off (there is a loss of power) all the contents of ROM remain.</p> <p>This is important because it means every time we turn off the device, the instructions to boot it up are not lost. If ROM was volatile, we would never be able to boot our device back up again.</p>
<p>RAM is rewritable. This means the contents of RAM can be changed.</p> <p>This means we can open and close different programs and files. If RAM was not rewritable, we would never be able to open or close different programs or files.</p>	<p>ROM is read only. This means the contents of ROM cannot be changed, and only read from.</p> <p>This is important because it prevents a user accidentally changing or deleting the BIOS which would then lead to the computer not being able to boot up correctly, or at all.</p>
<p>RAM is usually measured in Gigabytes (GB).</p> <p>This is so that the device has a large amount of storage in RAM, therefore more programs and files can be open at once without the RAM quickly filling up.</p>	<p>ROM is usually measured in Megabytes (MB) or Kilobytes (KB).</p> <p>This is because ROM only contains the BIOS and therefore does not need to be any bigger.</p>

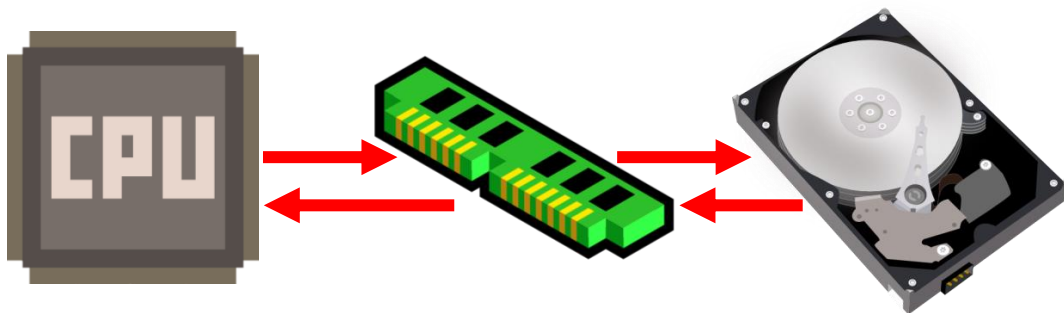


“Remembering these differences is important for the exam. There is usually a question on this. Just remember that RAM is bigger than ROM, is volatile, and can be changed, and ROM is the opposite to all of those!”

Virtual Memory

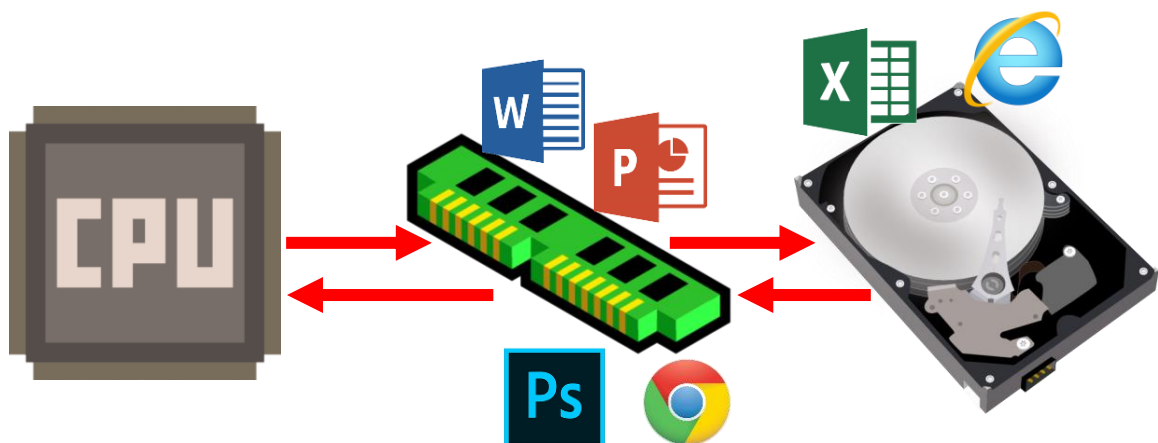
Sometimes, when a user has a large number of programs or files open at once, the RAM can become full. Rather than the computer simply stopping anymore programs or files being opened, the computer makes use of **virtual memory**.

Virtual memory is used when the RAM becomes full. When this happens, part of the internal Hard Drive is partitioned (sectioned off) and acts as additional RAM. This allows further programs and files to be opened and allows the computer to continue to function.



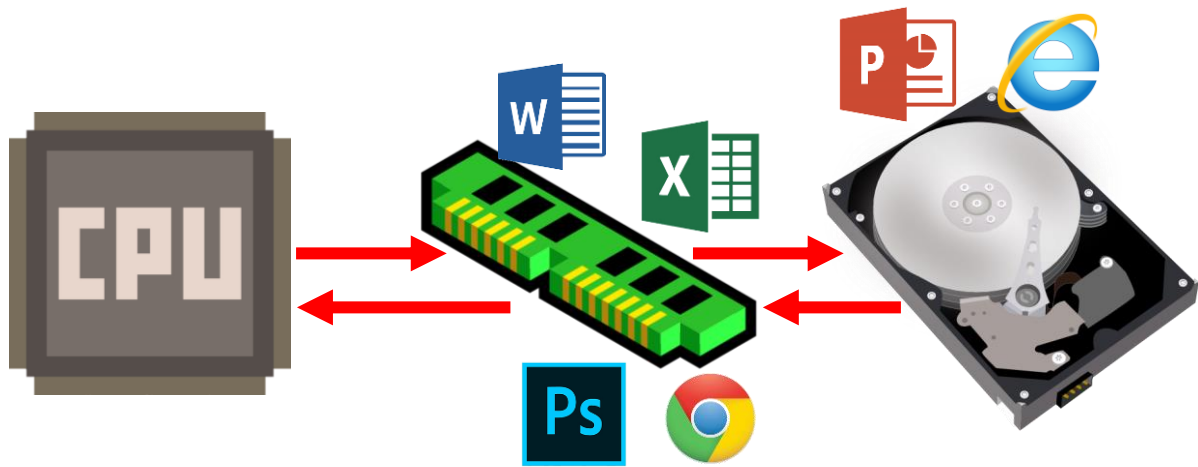
However, this impacts upon the performance of the computer. The CPU does not have direct access to the virtual memory. Therefore, any programs or files that are stored in the virtual memory must be swapped into RAM (and something else swapped out of RAM and into the virtual memory) for them to be actively used. This process slows the performance of the device down.

Let us look at an example of this to better understand how virtual memory works:



In the example above our user has a number of programs open. As Microsoft Excel and Internet Explorer are not actively being used by the user, they are currently stored in the virtual memory. However, the user now wants to use Microsoft Excel again! Therefore, it needs to be moved into the RAM. That means something else needs to be moved out.

In this case Microsoft PowerPoint is not actively being used, so it can be swapped out into the virtual memory, making room for Microsoft Excel to be stored and accessed in the RAM:



This is how virtual memory works! As you can see though, this process takes up precious time and therefore makes the performance of the device decrease.

We can avoid using virtual memory by upgrading our RAM so it is bigger. This would mean it would take longer for the RAM to become full, and therefore virtual memory is less likely to be used.

Secondary Storage

Secondary Storage is where we store for longer than just whilst the computer is turned on. It is not volatile, and therefore data remains even after the power has been turned off. This means we can save our programs and files on Secondary Storage, turn off our device, and the next time we turn our device back on, we won't have lost them.

This is why we need Secondary Storage. It allows us to store programs and files when they are not in use, as well as whilst the power has been turned off.



“Remember, because Secondary Storage is not volatile, its contents remain even after the power is turned off. If we saved our programs and files in the RAM (which is volatile), we would never be able to access them again once the power was turned off. This is because they would get deleted due to RAM being volatile!”

It's your turn!

Describe why Secondary Storage is important in a computer system [2]

Secondary Storage: The different types

There are three main types (also called technologies) of Secondary Storage. These are **Optical**, **Magnetic**, and **Solid State**. Each one has its advantages and disadvantages, and it is important to be able to compare each of them against each other.

Optical:

Optical Storage is used within an Optical Drive, where a laser is shone at the surface of the disc, and then processing the reflection from the disc. Optical Storages are discs, and examples are CDs, DVDs, and Blu-Rays.



For some extra information:



CD-R, DVD-R — Read Only, so the contents cannot be changed

CD-RW, DVD-RW — Rewritable, so the contents can be changed”

Magnetic:

Data is stored on Magnetic Storage via magnetised dots. Magnetic Storage often has moving parts. An example of Magnetic Storage is a Hard Disc Drive (HDD). Another example is a Floppy Disk; however, these are no longer used due to their poor durability and reliability.



Solid State:

Data is stored on Solid State Storage via electricity. It is becoming increasingly popular as its capacity increases, and its cost decreases. Examples of Solid-State Storages are Memory Sticks, SSDs, and SD Cards.



“A common mistake is students writing ‘an example of a Solid-State storage is a USB’. A USB is not correct! Make sure you call it a Memory Stick, or a USB Memory Stick”

Characteristics of Secondary Storage

Now we know the three main types of Secondary Storage, we need to be able to compare them against each other. Once we know what the advantages and disadvantages are for each storage type, we can then start to apply them to given scenarios.

Below is a table which outlines all the different characteristics. For each Secondary Storage type, there is a description as to how it performs in that characteristic. Each Secondary Storage type has then been graded based on how it performs against the other types:

Bronze — This means the Secondary Storage type performs worst on this characteristic out of the three

Silver — This means the Secondary Storage type is in the middle on this characteristic out of the three

Gold — This means the Secondary Storage type performs the best on this characteristic out of the three

	Optical	Magnetic	Solid State
Capacity	Has a relatively small capacity ranging from 500MB to 5GB	Has a large capacity. The largest of the three types. Can range anywhere from 256GB to 1.5TB (Terabytes)	Has a medium to large capacity. Can range anywhere from 2GB to 256GB
Speed	Slow to read and write data to. Data is burnt onto disks, and takes and lengthy period of time	Provides fast access to data. Data can be written and read from media quickly	Has the fastest read and write time, providing very fast access to data
Portability	Is light and relatively easy to carry around. May not fit inside a pocket but will fit inside a bag	Is bulky and heavy, not at all easy to carry around, and is usually left inside a computer rather than removed and transported	Is light and very portable. Can easily fit inside a pocket and be transported from one place to another
Durability	Can be easily scratched. Once the disk becomes scratched it may not function. Can withstand shaking	Easily damaged, and data can become easily corrupted. If placed near magnets, shaken, or dropped, data is likely to be lost	Very durable. Can withstand being shaken and dropped, and is strong and unlikely to break easily

Reliability	Quite reliable. Unlikely to stop working if looked after. However, unsuitable for rugged applications	Can falter over time and require replacing	Quite reliable. Unlikely to stop working if looked after. Suitable for rugged applications due to its reliability
Cost	Cheap to buy in bulk. Can buy 100 CD-Rs for approximately £10	Can be expensive to replace, ranging anywhere from £50 to £150. However, their price per unit of storage is relatively cheap, averaging £0.03 per Gb	Prices vary depending on the type. External Hard Drives can cost approximately £60, where a USB Memory Stick can cost £10. Depends on the media you choose. Price per unit of storage is higher however than magnetic storage, averaging £0.15 per Gb

We can then summarise this table:

Optical — Advantages: **Cheap, portable, average durability and reliability**
 Disadvantages: **Small capacity, slow data transfer speed**

Magnetic — Advantages: **Large capacity, fast data transfer speed, relatively cheap per unit of storage**
 Disadvantages: **Not durable, not portable**

Solid State — Advantages: **Durable, reliable, easily portable, fast transfer speed**
 Disadvantages: **Price can vary depending on the media you choose**



Describe one advantage and one disadvantage to using Solid State storage [4]

Now we know the advantages and disadvantages to each, we can start to apply them to given scenarios. Let's look at the scenarios below, and identify which type of Secondary Storage would be best to use:

Scenario 1:

A software development company wants to release its newest software for sale to customers in shops.

Q. Which Secondary Storage type should they use?

A. **Optical**. This is because they are cheap to buy in bulk, so the company will save money on costs and increase their profits. Optical storage should also have enough capacity to hold the software, and they can purchase read only media (such as CD-Rs) which means the media cannot be overwritten or used again.



Scenario 2:

A BMX stunt rider wants to attach a camera to his helmet and record the stunts he performs.

Q. Which Secondary Storage type should they use?

A. **Solid State**. This is because it is durable, and therefore the rider is less likely to lose any of his data whilst they are performing their tricks. It is also portable and light, so won't add any additional weight to the camera or the helmet. It also has a medium to large capacity, so will be able to handle both SD (Standard Definition) and HD (High Definition) video.



“You might have been tempted to say Optical storage for the scenario above with the BMX rider. However, you have to think about it logically. Would you realistically put a disk (such as a DVD) in a camera to record something? No! It would mean the camera would need to be large, and therefore would not fit on the rider's helmet. Hence, Solid State is better for this scenario”



Scenario 3:

A new company wants to upgrade their Secondary Storage. They have a large amount of data and need it all storing on the same media.

Q. Which Secondary Storage should they use?

A. **Magnetic.** It is likely that the storage media will remain inside the devices and will not need transporting around. Also, due to the fact the company has a large amount of data, we will need something that offers us a large capacity, and magnetic storage will offer us this.



Now we have gone through some scenarios, an important point to remember is that sometimes more than one type of Secondary Storage may be suitable. However, **always read the scenario carefully**, and weigh up which one you think would be best. Also, always look to see if a specific device is mentioned (e.g. a tablet) and take that into consideration too.

For example, if the scenario mentioned a tablet computer and large amount of data, despite magnetic seeming the best option, you wouldn't put an internal hard drive into a tablet computer. It would make it bulky, heavy, and no longer portable.

Always read the question and scenario carefully!

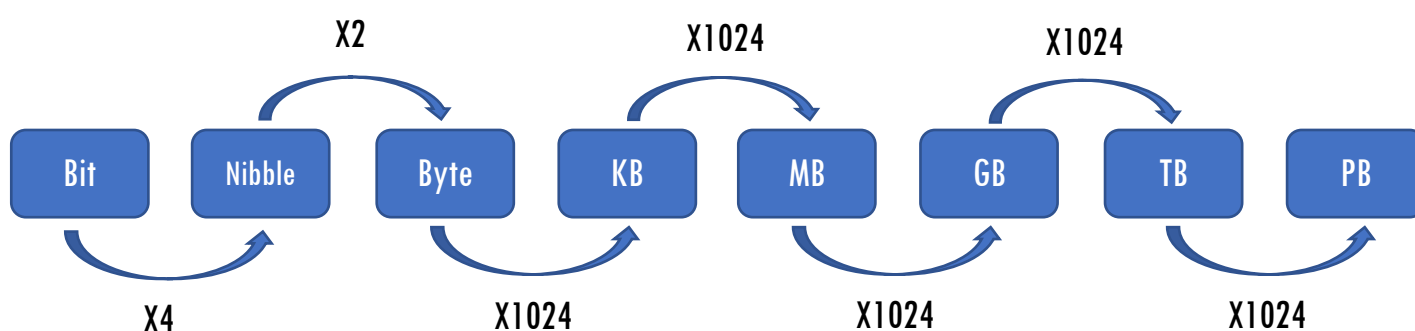
Units of measurement

Data is stored in the computer as binary digits (1s and 0s). Each digit is a bit of data.

There are 4 bits in a nibble, and 8 bits in 1 byte. Now, you may have heard the word byte in terms such as megabyte, gigabyte etc.

What you need to know for your exam is how to order different units from smallest to largest.

Below are the different units of measurement from smallest to largest:



KB = Kilobyte
 MB = Megabyte
 GB = Gigabyte
 TB = Terabyte
 PB = Petabyte

As you can see from the diagram above:

- There are 4 bits in a nibble, and 8 bits in a byte
- There are 2 nibbles in a byte
- There are 1024 bytes in a kilobyte
- There are 1024 kilobytes in a megabyte
- There are 1024 megabytes in a gigabyte
- There are 1024 gigabytes in a terabyte
- There are 1024 terabytes in a petabyte

We can also work out from the above how many megabytes for example are in a terabyte (we did this in paper 1). We firstly calculate how many steps it is between megabyte and terabyte,

which is 2. We then do 1024^n where n is the number of steps. In this case it is 1024^2 which is 1,048,576. Therefore, there are 1,048,576 megabytes in a terabyte.

Now, in the exam you are not allowed to use a calculator, which means you don't have to be so specific and use 1024 bytes. You can use 1000. This approximation is fine for GCSE.

So, doing the same calculation as above for how many megabytes in a terabyte, we could do 1000^2 which is 1,000,000. Therefore, there are approximately 1,000,000 megabytes in a terabyte. This is fine for your exam.

Why data must be in binary

For computer systems to be able to process and execute our instructions they must be in a format the computer understands. Computers do not understand sound, or pixels, or letters. All these must be converted into binary so that the instructions can be understood and executed.

In the coming sections we are going to look at how numbers, letters, images, and sounds are all converted to binary so that the computer can understand them.

Data Capacity and Requirements

In order to select the best Secondary Storage type, it is good to be able to calculate the required capacity in a situation.

For example, how many word documents could fit on a 2GB USB Memory Stick, compared to a 256GB Internal Hard Disk?

In order to be able to calculate capacities and requirements, we are going to use the below examples of each Secondary Storage type, and the below files. Please note – these are only examples. Both the Secondary Storage types and the files can vary in sizes. It is highly unlikely you will get these exact sizes in the exam, but the process on how we calculate the capacities remains the same.



Optical – 640MB



Magnetic – 2TB



Solid State – 8GB



Word Document (.docx) – 246KB



Image File (.JPG) – 4342KB



Music File (.mp3) – 8485KB



Video File (.mov) – 62,896KB

Let's look at a question:

Q. How many documents can you fit on a 2TB Hard Disk?

Step 1:

First thing we need to do is ensure both units are the same. We will convert both to MB (Megabytes)

2TB = 2,000,000MB (roughly)

246KB = 0.2MB (roughly)

Note how we are converting these roughly. They do not need to be exactly accurate but need to be close enough.

To do this, there are roughly 1000KB in a MB, 1000MB in a GB, and 1,000,000MB in a TB.

Step 2:

Now we divide the two

$$\frac{2,000,000\text{MB}}{0.2\text{MB}} = 10,000,000$$

This means we can store 10,000,000 246KB documents on our 2TB Hard Disk.



“You are allowed a calculator in the exam, so don't panic about doing these in your head! Just remember those two simple steps. Convert both to the same unit, then divide the media by the file”

Another example:

Q. How many documents can you fit on an 8GB USB Memory Stick?

Again, let's go through our steps:

Step 1:

First thing we need to do is ensure both units are the same. We will convert both to MB (Megabytes)

8GB = 8000MB (roughly)
246KB = 0.2MB (roughly)

Step 2:

Now we divide the two

$$\frac{8000\text{MB}}{0.2\text{MB}} = 40,000$$

This means we can store 40,000 246KB documents on our 8GB USB Memory Stick.

Let's do another example, but with a different file type now:

Q. How many video files can you fit on a 2TB Hard Disk?

Again, let's go through our steps:

Step 1:

First thing we need to do is ensure both units are the same. We will convert both to MB (Megabytes)

2TB = 2,000,000MB (roughly)

62,896KB = 62.9MB (roughly)

Step 2:

Now we divide the two

$$\frac{2,000,000\text{MB}}{62.9\text{MB}} = 31,796$$

This means we can store 31,796 62,896KB video files on our 2TB Hard Disk.

It's your
turn!

How many 8485KB music files could you fit on a 2TB Hard Disk? [1]

How many 4342KB image files could you fit on an 8GB USB Memory Stick? [1]

Representing numbers in binary

As we already know, binary only uses two numbers (1 and 0). It is therefore called a base 2 system.

We often refer to binary numbers as being **8-bit**. All these means is there are 8 individual 1s and 0s which form a binary number. Please keep this in mind as the exam will often ask you to convert to or from an 8-bit binary number!

How to convert positive denary whole numbers (0-255) into 8-bit binary numbers and vice versa

When we refer to a **denary** number, we are referring to our number system we use as humans. It is called denary because there are 10 numbers used in total to form any number (0,1,2,3,4,5,6,7,8,9).

It is straightforward to convert between denary and binary. Let's convert denary numbers to binary first.

Q: Convert the denary number 56 to an 8-bit binary number. You must show your working.

Firstly, we are going to draw the below table:

128	64	32	16	8	4	2	1

The reason we have used the numbers we have is because we only use two numbers in binary (0 and 1). You will notice we start at 1 and multiply by 2 each time, up to 128 which gives us 8 empty boxes for numbers in total (8 bits).

Now, to convert 56 into binary, all we do is look at the numbers along the top of the table and think about which ones we can use to make 56. In this case we can add together 32, 16, and 8. Because we have used these numbers, we put a 1 underneath them.

128	64	32	16	8	4	2	1
		1	1	1			

Now, under the rest of the numbers, we put a 0. There must be a number in each column so we must fill the rest in with 0's!

128	64	32	16	8	4	2	1
0	0	1	1	1	0	0	0

That's it! The denary number 56 converted into an 8-bit binary number is 00111000.

Let's do another.

Q: Convert the denary number 151 to an 8-bit binary number. You must show your working.

Again, we are going to draw the below table:

128	64	32	16	8	4	2	1

Now, to convert 151 into binary, all we do is look at the numbers along the top of the table and think about which ones we can use to make 151. In this case we can add together 128, 16, 4, 2, and 1. Because we have used these numbers, we put a 1 underneath them.

128	64	32	16	8	4	2	1
1			1		1	1	1

Now, under the rest of the numbers, we put a 0. There must be a number in each column so we must fill the rest in with 0's!

128	64	32	16	8	4	2	1
1	0	0	1	0	1	1	1

That's it! The denary number 151 converted into an 8-bit binary number is 10010111.



“It is very important to note here, as with the rest of the conversion and addition topics in this section, **you must show your working!** It is just like when we learnt about the searching and sorting algorithms, you must show the examiner how you are calculating the answer!

Now, let's have a go at converting from binary to denary.

Q: Convert the 8-bit binary number 00110010 to denary. You must show your working.

Once again, we're going to draw our table.

128	64	32	16	8	4	2	1

Now, we write out binary number into the table. If you are ever given a binary number that is not 8-bits, you always add an extra 0 **to the left of the number!**

128	64	32	16	8	4	2	1
0	0	1	1	0	0	1	0

We now need to calculate what this binary number is in denary. Wherever there is a 0, you can ignore, we are not interested in it. Wherever there is a 1, we look at the main number at the top of the table and add these together.

Therefore, in this case, we are adding together 32, 16, and 2. This gives us 50.

That's it! The 8-bit binary number 00110010 in denary is 50.

Let's do another.

Q: Convert the 8-bit binary number 01101011 to denary. You must show your working.

Once again, we're going to draw our table.

128	64	32	16	8	4	2	1

Now, we write out binary number into the table.

128	64	32	16	8	4	2	1
0	1	1	0	1	0	1	1

We now need to calculate what this binary number is in denary. Wherever there is a 0, you can ignore, we are not interested in it. Wherever there is a 1, we look at the main number at the top of the table and add these together.

Therefore, in this case, we are adding together 64, 32, 8, 2, and 1. That gives us 107.

That's it! The 8-bit binary number 01101011 in denary is 107.

Binary Addition and Overflow Errors

Another skill we need to know is how to take two binary numbers and add them together, understanding what happens if the final answer exceeds 8-bits.

When adding two binary numbers together, it is important to note you **cannot** convert the two numbers back to denary, add them together, then convert the answer back to binary. This is not answering the question and will achieve you no marks in the exam. You must add the two binary numbers together, understanding how to add 1s and 0s together.

Here are the rules we are going to follow:

- ❖ If you add together a 0 and a 0, the answer is a 0
- ❖ If you add together a 0 and a 1, the answer is a 1
- ❖ If you add together a 1 and a 0, the answer is a 1
- ❖ If you add together a 1 and a 1, the answer is a 0, and you carry the 1

It's important to remember as well that the most significant bit is the bit that holds the greatest numerical value (in other words the bit furthest left) and the least significant bit is the bit that holds the smallest numerical value (in other words the bit furthest right).

Let's have a look at some examples to help us understand how to apply these rules.

Q: Add the binary numbers 10010001 and 00101100. You must show your working.

Firstly, we are going to write out our numbers in the form of a column addition.

$$\begin{array}{r}
 1\ 0\ 0\ 1\ 0\ 0\ 0\ 1 \\
 0\ 0\ 1\ 0\ 1\ 1\ 0\ 0 \\
 \hline
 \end{array}$$

Now, when adding binary numbers, we always start from the right-hand side, just like you would do in maths when using column addition. This means we're looking at the 1 and 0 first. Adding a 1 and a 0 together gives us a 1 (using our rules to help us), so we write that underneath.

$$\begin{array}{r}
 1\ 0\ 0\ 1\ 0\ 0\ 0\ 1 \\
 0\ 0\ 1\ 0\ 1\ 1\ 0\ 0 \\
 \hline
 1
 \end{array}$$

Now we move onto the next two numbers, which are 0 and 0. Again, using our rules, this gives us a 0, so let's write that in.

$$\begin{array}{r}
 1\ 0\ 0\ 1\ 0\ 0\ 0\ 1 \\
 0\ 0\ 1\ 0\ 1\ 1\ 0\ 0 \\
 \hline
 0\ 1
 \end{array}$$

Now, we simply continue down the line moving from right to left filling in the answers to the addition. In this case we have no carries so it's nice and simple!

$$\begin{array}{r}
 1\ 0\ 0\ 1\ 0\ 0\ 0\ 1 \\
 0\ 0\ 1\ 0\ 1\ 1\ 0\ 0 \\
 \hline
 1\ 0\ 1\ 1\ 1\ 1\ 0\ 1
 \end{array}$$

That's it! The answer to adding together the binary numbers 10010001 and 00101100 is 10111101.

Let's do another, but this time include a situation where we need to carry.

Q: Add the binary numbers 00100010 and 00011010. You must show your working.

Firstly, we are going to write out our numbers in the form of a column addition.

$$\begin{array}{r} 00100010 \\ 00011010 \\ \hline \end{array}$$

Now, using our knowledge, we can add together the first two numbers (0 and 0) which gives us 0.

$$\begin{array}{r} 00100010 \\ 00011010 \\ \hline 0 \end{array}$$

Now, the next numbers are a 1 and a 1. We know from our rules that adding a 1 and a 1 gives us a 0, and we need to carry the 1. This is the same as in maths when you add together two numbers (say 7 and 5) and the answer goes above the units in that part of the addition. In the 7 and 5 case you would write 3 and carry the 1. In our binary case we are going to write 0, and carry our 1.

$$\begin{array}{r} 1 \\ 00100010 \\ 00011010 \\ \hline 00 \end{array}$$

Now, to make our life easier, we are only going to add up two numbers at any one time. Therefore, we are going to draw in a little addition line to show we are only adding up two numbers (this doesn't get us any extra marks or lose us marks, it is simply for our benefit).

$$\begin{array}{r}
 00100\overset{1}{\underline{0}}10 \\
 00011010 \\
 \hline
 00
 \end{array}$$

Now, let's do the first addition, which is the carried 1 and 0. This would give us 1. Therefore, we can now change that 0 to a 1, so we don't forget what it is now, ready for the second addition.

$$\begin{array}{r}
 00100\color{red}{1}10 \\
 00011010 \\
 \hline
 00
 \end{array}$$

Now, we do the second part of the addition just like we normally would, adding together a 1 and a 0 which gives us a 1.

$$\begin{array}{r}
 00100110 \\
 00011010 \\
 \hline
 \color{red}{1}00
 \end{array}$$

Now, we can complete the rest of the addition as we know there are no more carries. We can also change that 1 we just changed in the question back to a 0 now (in the exam you might have crossed out the 0 and put a 1, you wouldn't lose marks if you left it like this as you've shown the examiner you had to carry a 1. We're going to change it back now just so we don't get confused what the original question was asking us to answer).

$$\begin{array}{r}
 0\ 0\ 1\ 0\ 0\ 0\ 1\ 0 \\
 0\ 0\ 0\ 1\ 1\ 0\ 1\ 0 \\
 \hline
 0\ 0\ 1\ 1\ 1\ 1\ 0\ 1
 \end{array}$$

That's it, the answer to 00100010 and 00011010 being added together is 00111101.

Let's do one more, but this time include more than one carry.

Q: Add the binary numbers 00100110 and 01000111. You must show your working.

Once again, let's put together our column addition.

$$\begin{array}{r}
 0\ 0\ 1\ 0\ 0\ 1\ 1\ 0 \\
 0\ 1\ 0\ 0\ 0\ 1\ 1\ 1 \\
 \hline
 \end{array}$$

Let's complete the first addition. A 0 and a 1 gives us a 1.

$$\begin{array}{r}
 00100110 \\
 01000111 \\
 \hline
 1
 \end{array}$$

Now, let's do the next addition. As we know, a 1 and a 1 added together gives us a 0, and we carry the 1.

$$\begin{array}{r}
 1 \\
 00100110 \\
 01000111 \\
 \hline
 01
 \end{array}$$

Once again, to make life easier for us, let's draw our line in so we are only dealing with two numbers at once.

$$\begin{array}{r}
 1 \\
 00100\underline{1}10 \\
 01000111 \\
 \hline
 01
 \end{array}$$

Adding together the carried 1 and the first 0 gives us a 1, so we can change the 0 to a 1 now.

$$\begin{array}{r}
 0\ 0\ 1\ 0\ \mathbf{1}\ 0\ 1\ 0 \\
 0\ 1\ 0\ 0\ 0\ 1\ 1\ 1 \\
 \hline
 1\ 0\ 1
 \end{array}$$

Now we have a 1 and a 0, which gives us a 1.

$$\begin{array}{r}
 0\ 0\ 1\ 0\ 1\ 0\ 1\ 0 \\
 0\ 1\ 0\ 0\ 0\ 1\ 1\ 1 \\
 \hline
 \mathbf{1}\ 1\ 0\ 1
 \end{array}$$

Finally, let's complete all the other additions using our rules, and change back those numbers in the question we have changed due to carries (again, just so we don't get confused on what we were adding. If you didn't do this in the exam you wouldn't lose any marks as you will have shown it was due to carries and you will have crossed numbers out etc.)

$$\begin{array}{r}
 0\ 0\ 1\ 0\ 0\ 1\ 1\ 0 \\
 0\ 1\ 0\ 0\ 0\ 1\ 1\ 1 \\
 \hline
 \mathbf{0\ 1\ 1\ 0\ 1\ 1\ 0\ 1}
 \end{array}$$

That's it. Adding together 00100110 and 01000111 gives us the answer 01101101!

But what happens when you end up with an addition that leaves you with 9-bits rather than 8? Let's have a look.

Q: Add the binary numbers 10010011 and 11101100. You must show your working.

Once again, let's put together our column addition.

$$\begin{array}{r} 1\ 0\ 0\ 1\ 0\ 0\ 1\ 1 \\ 1\ 1\ 1\ 0\ 1\ 1\ 0\ 0 \\ \hline \end{array}$$

Firstly, let's do all our addition up until the final number, using our rules that we know.

$$\begin{array}{r} 1\ 0\ 0\ 1\ 0\ 0\ 1\ 1 \\ 1\ 1\ 1\ 0\ 1\ 1\ 0\ 0 \\ \hline 1\ 1\ 1\ 1\ 1\ 1\ 1\ 1 \end{array}$$

Now, in our final addition we are left with a 1 and a 1. We know this means the answer is 0, and we carry the 1. But where will we carry the 1, we're at the end of our addition. Simple, we carry it just like we normally would, over into an imaginary 9th column!

$$\begin{array}{r} 1 \\ 1\ 0\ 0\ 1\ 0\ 0\ 1\ 1 \\ 1\ 1\ 1\ 0\ 1\ 1\ 0\ 0 \\ \hline 0\ 1\ 1\ 1\ 1\ 1\ 1\ 1 \end{array}$$

Now, we can't leave that 1 floating around, it needs to go somewhere! Therefore, we fill the remaining space underneath it with 0's.

$$\begin{array}{r}
 1 \\
 0\ 1\ 0\ 0\ 1\ 0\ 0\ 1\ 1 \\
 0\ 1\ 1\ 1\ 0\ 1\ 1\ 0\ 0 \\
 \hline
 0\ 1\ 1\ 1\ 1\ 1\ 1\ 1
 \end{array}$$

Now, we complete our addition just like we normally would (the carried 1 and the first 0 gives us 1. Then this 1 and the second 0 gives us 1).

$$\begin{array}{r}
 0\ 1\ 0\ 0\ 1\ 0\ 0\ 1\ 1 \\
 0\ 1\ 1\ 1\ 0\ 1\ 1\ 0\ 0 \\
 \hline
 1\ 0\ 1\ 1\ 1\ 1\ 1\ 1\ 1
 \end{array}$$

However, we have a problem! You will notice now we have been left with 9 bits at the bottom rather than 8. In this case (and for GCSE) we are only allowed 8 bits, anymore and we have an error!

We call this error an **overflow error**.

An overflow error occurs when we add together two 8-bit binary numbers, and the result leaves us with a 9th bit. This bit cannot be stored and therefore is deleted. This means the result is of course incorrect. In the case above we were adding together 147 and 236, which is 383. However, the largest number we can represent in 8-bit binary is 255. Due to this 9th bit being lost, the answer we get out of this addition is actually 127, which we know is incorrect.

Hexadecimal Conversion

This section is going to cover two elements of this unit. This is because in converting between hexadecimal and denary we are going to use binary, so we can cover both of these points together to save us some revision time!

Hexadecimal is a base 16 system. This is because it uses 16 digits and characters in total. These are 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F.

You will notice after 9 we suddenly stop using numbers and change to letters. Each of the letters below represents the following number:

A = 10

B = 11

C = 12

D = 13

E = 14

F = 15

It is important to remember this!

The maximum number we can make with 2 hexadecimal digits is 255, the same as using an 8 bit binary number. However, computer scientists prefer to represent data in hexadecimal form rather than binary as it is quicker to write down 2 digits rather than 8 binary digits. You are also less likely to make a mistake when writing down the hexadecimal form with it being 2 digits, compared to 8 binary digits.

For the exam you need to be able to convert between binary, denary, and hexadecimal. First we will look at how you convert a denary and binary number to hexadecimal.

Q: Convert the denary number 65 to hexadecimal. You must show your working.

To answer this question, we are going to follow these three simple steps:

Step 1 – Convert the denary number to binary (if in the exam you were given a binary number then this step won't be necessary).

Step 2 – Split the 8-bit binary number into 2 separate nibbles.

Step 3 – Calculate the worth of each table and convert any numbers between 10 and 15 to their equivalent letter.

Let's do step 1 first of all. Below is 65 converted to binary.

128	64	32	16	8	4	2	1
0	1	0	0	0	0	0	1

Now we split this table into two separate nibbles, and simply move each bit down into the new tables. As you can see the red numbers have dropped into the first table, and the blue numbers have dropped into the second table.

8	4	2	1
0	1	0	0

8	4	2	1
0	0	0	1

You will also notice we have not used 128, 64, 32, and 16 as the numbers at the top of each column in the first table. This is because the largest single digit we can have in hexadecimal is 15 (or F). If we used these numbers it would put us way over 15. However, using 8, 4, 2, and 1 means the largest we can have is 15 ($8 + 4 + 2 + 1 = 15$).

Finally, we calculate how much each table is worth. To do this we ignore all the 0's, and add up the numbers at the top of the table wherever there is a 1.

8	4	2	1
0	1	0	0

The red table is worth 4.

8	4	2	1
0	0	0	1

The blue table is worth 1.

That's it! All we do now is simply put those two answers together. Therefore, 65 in hexadecimal is 41. We say it as four one, not forty one.

Let's have another example.

Q: Convert the denary number 29 to hexadecimal. You must show your working.

Again, let's do the first step which is to convert 29 to binary.

128	64	32	16	8	4	2	1
0	0	0	1	1	1	0	1

Now we split this table into two separate nibbles, and simply move each bit down into the new tables. As you can see the red numbers have dropped into the first table, and the blue numbers have dropped into the second table.

8	4	2	1
0	0	0	1

8	4	2	1
1	1	0	1

Finally, we calculate how much each table is worth. To do this we ignore all the 0's, and add up the numbers at the top of the table wherever there is a 1.

8	4	2	1
0	0	0	1

The red table is worth 1.

8	4	2	1
1	1	0	1

The blue table is worth 13.

Now, remember we can't have any numbers bigger than 9, and if we do, we have to swap them to their correct letter? We have 13 from the blue table! Therefore, we swap 13 to its letter which is D.

That's it! Once again, we put our two answers together and get the answer 1D. Therefore, the denary number 29 in hexadecimal is 1D.

Now let's have a look at going the other way.

Q: Convert the hexadecimal number 74 to denary. You must show your working.

For this question we need to change the hexadecimal number 74 back to denary. To do this we will follow these three simple steps:

Step 1 – Convert any letters back to numbers.

Step 2 – Multiply the first number by 16, and the second number by 1.

Step 3 – Add your two answers together.

For this question, we can skip step 1 as we have no letters, as we've been asked to convert 74 back to denary, so we don't need this step.

For step 2, we need to do some multiplication. Let's put a little table in to help us.

16	1
7	4

The reason we have used the numbers 16 and 1 is because in hexadecimal there are 16 digits and characters in total. Remember when we did binary, we started at 1 and multiplied by 2 each time? This is the same in hexadecimal, except we start at 1 and multiply by 16 each time. We don't need a third column as this would take us over the maximum 255, we can make with 2 hexadecimal digits.

Now, we are going to do the multiplication.

$$16 \times 7 = 112$$

$$1 \times 4 = 4$$

Finally, we add the two answers together.

$$112 + 4 = 116.$$

That's it! The hexadecimal number 74 converted to denary is 116.

Let's do another example.

Q: Convert the hexadecimal number D3 to binary. You must show your working

In this question we now have two differences. First is we have a letter we're going to need to convert back to a number, and the question wants our final answer in binary. No problem!

Firstly, let's convert that D back to a number. D is 13. Keep that in your head!

Now let's do our multiplication. Let's get our table back in.

16	1
13	3

$$16 \times 13 = 208$$

$$1 \times 3 = 3$$

Finally, we add the two together.

$$208 + 3 = 211$$

So, we know the hexadecimal number D3 in denary is 211! However, the question wants the answer in binary. Simple! All we will do now is convert 211 into binary!

128	64	32	16	8	4	2	1
1	1	0	1	0	0	1	1

And we have our answer! The hexadecimal number D3 in binary is 11010011.

It's your turn!

Convert the denary number 98 to hexadecimal. You must show your working.

[3]

Convert the hexadecimal number FA to binary. You must show your working.

[3]

Binary Shifts

A **binary shift** is the process of shifting (moving) each bit a certain number of places to the left or right.

A binary shift to the right effectively halves the number. A binary shift to the left effectively doubles the number.

Let's have a look at a question.

Q: Perform a one place binary shift to the left on the 8-bit binary number 01101101. You must show your working.

As normal, let's draw our binary table and fill in the table with our binary number.

128	64	32	16	8	4	2	1
0	1	1	0	1	1	0	1

In this question we need to perform a left shift, meaning we are going to move each bit to the left. It says it needs to be a one place binary shift also, meaning each bit is going to move only once. Once again, we are going to start at the far right, and work our way across to the left. Let's shift the first bit one place to the left.

128	64	32	16	8	4	2	1
0	1	1	0	1	1	0	1
						1	

All we have done is simply shift the bit one place to the left. Now let's do the next bit.

128	64	32	16	8	4	2	1
0	1	1	0	1	1	0	1
					0	1	

Now let's do the next five bits in one go. Same process!

128	64	32	16	8	4	2	1
0	1	1	0	1	1	0	1
1	1	0	1	1	0	1	

Now, we get to the final bit in the 128 column. As with our column addition, we can't be left with more than 8-bits, therefore this bit simply 'falls' out of our table and is lost!

Finally, we have an empty space at the start of our shifted number. We can't have any empty spaces, so we simply fill this space with a 0.

128	64	32	16	8	4	2	1
0	1	1	0	1	1	0	1
1	1	0	1	1	0	1	0

That's it! We've performed a one place binary shift to the left on the 8-bit binary number 01101101 and have been left with 11011010.

Let's do another example.

Q: Perform a two-place binary shift to the right on the 8-bit binary number 11010010. You must show your working.

As normal, let's draw our binary table and fill in the table with our binary number.

128	64	32	16	8	4	2	1
1	1	0	1	0	0	1	0

Firstly, let's perform our first shift on all the bits. Simply move all the bits one place to the right. As with the last question, the bit in the 128 column (which is a 1) will 'fall' out of the table.

128	64	32	16	8	4	2	1
1	1	0	1	0	0	1	0
	1	1	0	1	0	0	1

Now let's fill in our empty space in the 128 column with a 0, as we can't have any empty spaces!

128	64	32	16	8	4	2	1
1	1	0	1	0	0	1	0
0	1	1	0	1	0	0	1

Now let's perform our second shift. Once again the bit inside the 1 column (this time it's a 1) 'falls' out of the table.

128	64	32	16	8	4	2	1
1	1	0	1	0	0	1	0
0	1	1	0	1	0	0	1
	0	1	1	0	1	0	0

Finally, we need to fill in our empty space with a 0.

128	64	32	16	8	4	2	1
1	1	0	1	0	0	1	0
0	1	1	0	1	0	0	1
0	0	1	1	0	1	0	0

That's it! We've performed a two-place binary shift to the right on the 8-bit binary number 11010010 and have been left with 00110100.



"As mentioned before, you must show your working with these questions! You will notice as well with the above example, we effectively halved the original number each time we performed a right shift. We started with 210 (11010010) and ended up with 52 (00110100).

It's your turn!

Perform a three-place binary shift to the left on the 8-bit binary number 00010110. [3]

State what happens when a binary shift to the left takes place. [1]

Characters

When we talk about how letters, numbers, and symbols are represented in computer systems, we talk about **characters** and **character sets**.

A character set refers to all the characters that are defined and recognised by the computer hardware and software. The size of the character set is dependent on the number of bits being used per character. The more bits per character used, the more characters that can be represented.

For example, **ASCII** is a character encoding standard for computer systems. Here characters are given a code within the system. In the original version of ASCII, a total of 127 characters were covered. This was because the system used a 7-bit encoding system, meaning the maximum number of characters represented was 127. In **extended ASCII**, this rose to 255 as the system used an 8-bit encoding system, increasing the maximum number of characters.

Below you can see the characters covered in the original version of ASCII:

ASCII Table

Dec	Hex	Oct	Char	Dec	Hex	Oct	Char	Dec	Hex	Oct	Char	Dec	Hex	Oct	Char
0	0	0		32	20	40	[space]	64	40	100	@	96	60	140	`
1	1	1		33	21	41	!	65	41	101	A	97	61	141	a
2	2	2		34	22	42	"	66	42	102	B	98	62	142	b
3	3	3		35	23	43	#	67	43	103	C	99	63	143	c
4	4	4		36	24	44	\$	68	44	104	D	100	64	144	d
5	5	5		37	25	45	%	69	45	105	E	101	65	145	e
6	6	6		38	26	46	&	70	46	106	F	102	66	146	f
7	7	7		39	27	47	'	71	47	107	G	103	67	147	g
8	8	10		40	28	50	(72	48	110	H	104	68	150	h
9	9	11		41	29	51)	73	49	111	I	105	69	151	i
10	A	12		42	2A	52	*	74	4A	112	J	106	6A	152	j
11	B	13		43	2B	53	+	75	4B	113	K	107	6B	153	k
12	C	14		44	2C	54	,	76	4C	114	L	108	6C	154	l
13	D	15		45	2D	55	-	77	4D	115	M	109	6D	155	m
14	E	16		46	2E	56	.	78	4E	116	N	110	6E	156	n
15	F	17		47	2F	57	/	79	4F	117	O	111	6F	157	o
16	10	20		48	30	60	0	80	50	120	P	112	70	160	p
17	11	21		49	31	61	1	81	51	121	Q	113	71	161	q
18	12	22		50	32	62	2	82	52	122	R	114	72	162	r
19	13	23		51	33	63	3	83	53	123	S	115	73	163	s
20	14	24		52	34	64	4	84	54	124	T	116	74	164	t
21	15	25		53	35	65	5	85	55	125	U	117	75	165	u
22	16	26		54	36	66	6	86	56	126	V	118	76	166	v
23	17	27		55	37	67	7	87	57	127	W	119	77	167	w
24	18	30		56	38	70	8	88	58	130	X	120	78	170	x
25	19	31		57	39	71	9	89	59	131	Y	121	79	171	y
26	1A	32		58	3A	72	:	90	5A	132	Z	122	7A	172	z
27	1B	33		59	3B	73	;	91	5B	133	[123	7B	173	{
28	1C	34		60	3C	74	<	92	5C	134	\	124	7C	174	
29	1D	35		61	3D	75	=	93	5D	135]	125	7D	175	}
30	1E	36		62	3E	76	>	94	5E	136	^	126	7E	176	~
31	1F	37		63	3F	77	?	95	5F	137	_	127	7F	177	

© w3resource.com

As you can see, each character is given a code to represent it. For example, 70 represents the capital letter F. Capital and lowercase letters need separate codes as they are different characters!

Now, as we know the computer uses binary to process data. Therefore, these codes must be converted to binary for the computer to be able to process the data and display and store these characters.

So, referring back to our example above of 70 for the capital letter F, the computer would store this as 01000110.

As we said above, the more bits per character we have, the more characters we can have within our character set. ASCII used 7-bits, meaning a maximum of 127 characters, extended ASCII used 8-bits, meaning a maximum of 255 characters. **UNICODE** however uses up to 32 bits per character, meaning there are over 1.1 million characters that are in UNICODEs character set.

Of course, using this many bits per character means more characters which means more languages etc. can be covered, but storing these characters means more storage space is taken up on your device.

We calculate the size of a text file by the following:

size = bits per character x number of characters

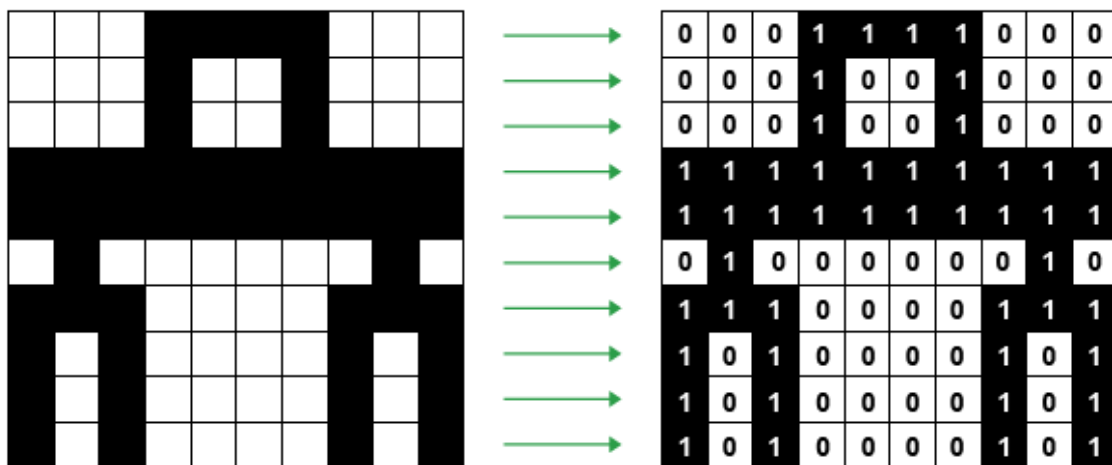
Images

An image is made up of millions of **pixels**. A pixel is an individual 'square' on an image, that when combined produce an image.

We often talk about the **resolution** of an image when thinking about quality. Resolution refers to the number of pixels an image has. The more pixels an image has, the better the quality. However, this of course means a bigger file size which takes up more storage space when saved.

We also refer to the **colour depth** of an image. The colour depth of an image is effectively the number of different colours that can be represented in an image. This is calculated by the number of **bits per pixel**. The higher the number of bits per pixel, the more colours that can be represented in the image. However, once again, the higher the bits per pixel the greater the file size.

Let's look at an example.



As you can see in the above example, the image is a simple black and white image. However, when displayed in binary to show how the computer would store each pixel, we can see each white square is represented as a 0, and each black square is represented as a 1.

In this image the resolution would be low as we only have a small number of pixels in the image (100 pixels). The colour depth is also small too. We are using 1 bit per pixel (each pixel is being represented using just a single bit (a single number), either 1 or 0. This means the maximum number of colours we could have using this number of bits per pixel is 2.

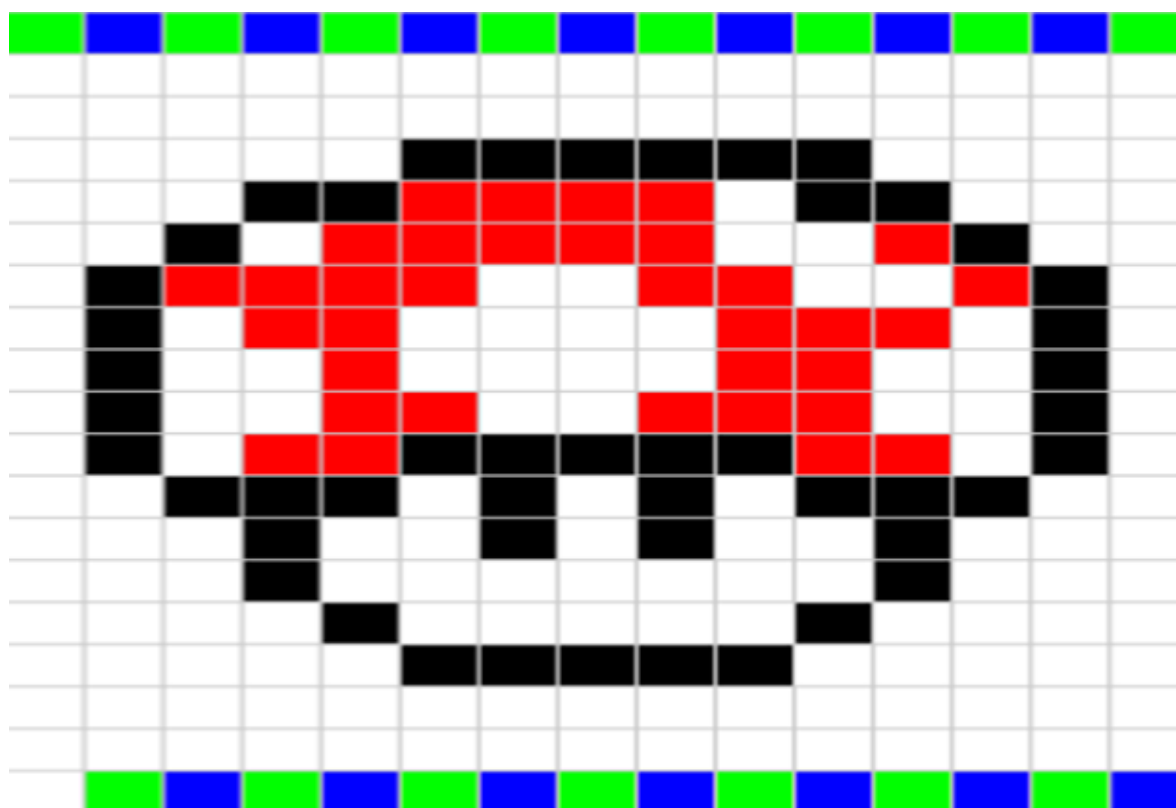
We calculated this by doing the following:

2^{\wedge} number of bits per pixel.

In this case this was:

$2^{\wedge} 1 = 2$ possible colours.

Now let's have a look at an image that has a greater colour depth:



In this image each colour again would be represented in binary. For example, the red pixels might be represented as 110. The blue pixels might be represented as 010.

This means we would be using 3 bits per pixel. As you can see, the greater the number of bits per pixel the greater the colour depth, however it does mean the greater the file size. In this case, if we were using 3 bits per pixel, the maximum number of colours we could have would be 8:

$2^{\text{number of bits per pixel}}$

$2^3 = 8$ possible colours

As well as storing the data for the image itself, there is also some additional data stored with the image that allows the device to rebuild the image, as well as provides some useful information to the user. We call this **metadata**.

Some data stored in the metadata of an image is the height of the image (in pixels), the length of the image (in pixels), the bits per pixel, GPS location etc.

We can calculate the file size of an image by multiplying its height in pixels by its width in pixels, and then multiplying this by the bits per pixel used in the image.

So, for example, for the Mario image above it would be:

$19 \times 15 \times 3 = 855$ bits

We would then also add an additional 10% on to account for the metadata being stored with the image.

$855 + 10\% = 941$ bits.

We calculate the size of an image file by the following:

size = colour depth x image height (pixels) x image width (pixels)

Sound

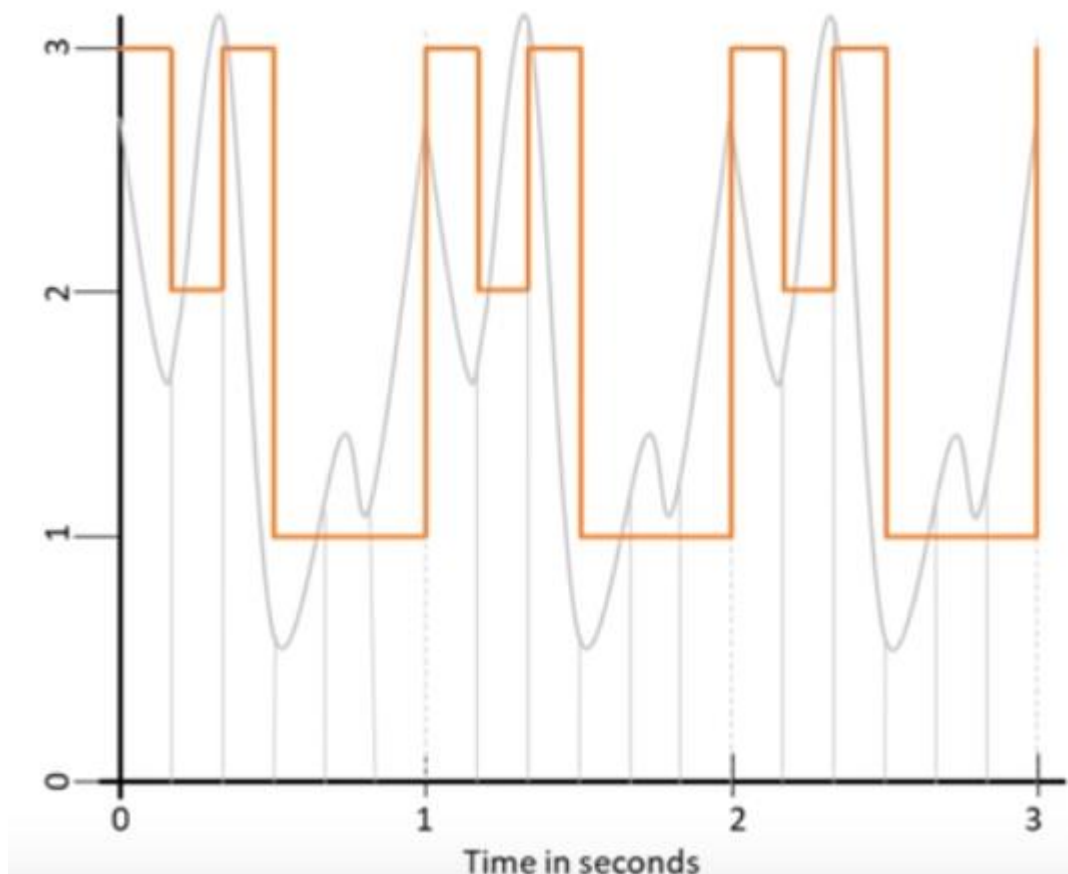
As with images (and everything else) sound must also be converted to and stored in binary.

A sound is transmitted through the air as an **analogue wave**. This analogue wave must be converted to a **digital wave** so it can be stored within the computer as binary.

We call this process **analogue to digital conversion** (ADC).

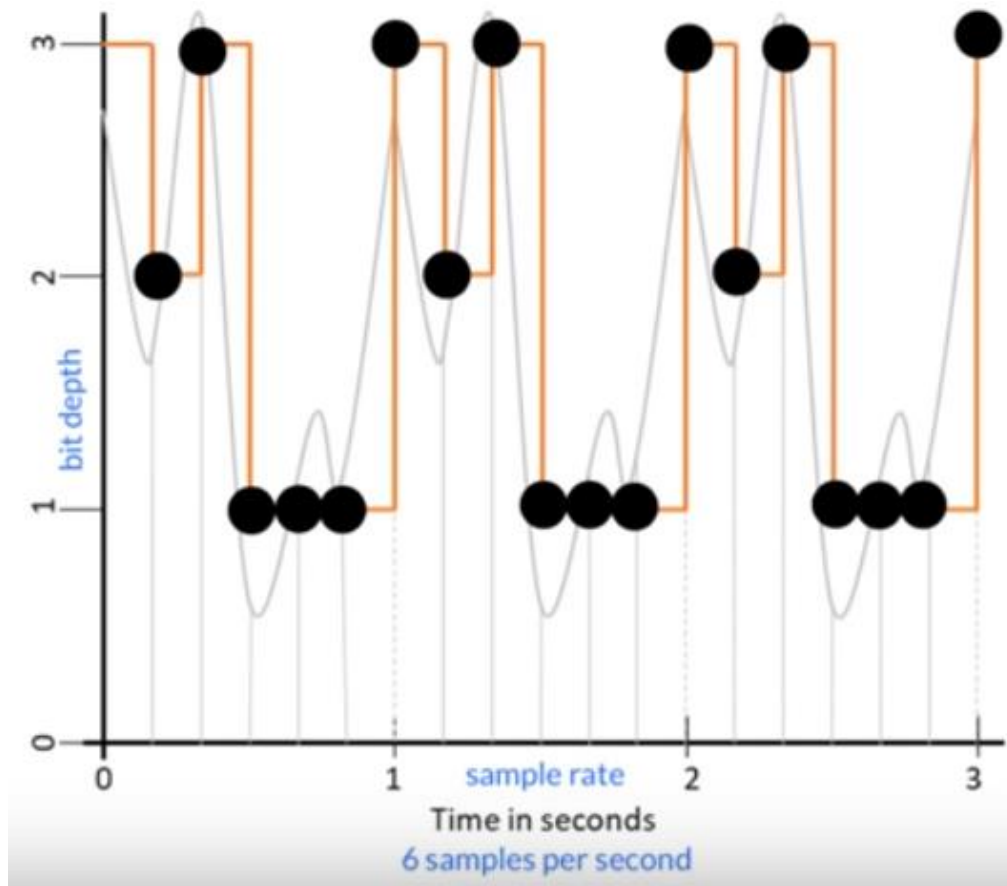
In this process we take measurements of the frequency of the wave at regular intervals.

In the image below we have our analogue wave in the background. What our device does is, at intervals, takes a measurement of the frequency of the wave. These measurements are then joined together to create a digital wave:



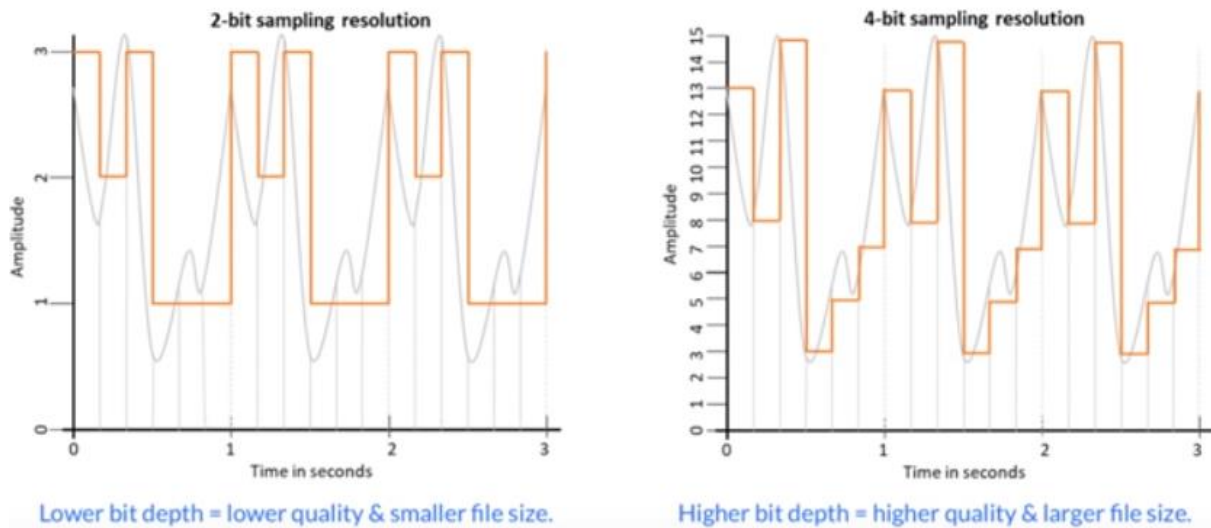
In the above example, the intervals where the sound is **sampled** is represented using the grey lines. This means this sound is sampled 6 times a second. The average sound for a CD is sampled over 44,000 times a second. The more samples we do a second the better the quality of the sound, but the more information we are storing per second and therefore the file size increases.

Below we can now see the points of each sample, represented with the black dots:



You can also see the **bit depth** going up the side. This is the number of bits stored for each sample. The greater the bit depth, the more accurate the sound will be represented in the digital wave, and therefore the better the quality of the sound. However, just like the sample rate, the higher the bit depth the greater the file size.

In this example our bit depth is 2. The numbers up the side of the graph are in denary for convenience, however we know these would be binary for the computer system. That means the numbers would be 00 (for 0), 01 (for 1), 10 (for 2), and 11 (for 3) giving us a bit depth of 2.



In the above image you can see the effect of increasing our bit depth from 2 to 4 (e.g. 15 being represented in binary as 1111). As you can see the digital wave is a much closer representation of the original analogue wave and allows for a greater quality of sound.

When converting a sound to binary we want to use a high sample rate and a high bit depth, therefore giving us a better quality of sound as we are taking more samples per second and storing more data per sample. However, the higher these two things are, the larger the file size will be.

We calculate the size of a sound file by the following:

$$\text{size} = \text{sample rate} \times \text{duration} \times \text{bit depth}$$

Compression

Compression is when the size of a file is reduced by changing some of the file's attributes e.g. its file type, dimensions etc. For example, we may compress a WAV sound file (which has a high audio quality but a large file size) down to an MP3 sound file (which has a lower sound quality but a much lower file size). This would then allow us to store more sound files on a device such as an iPod, due to the file sizes being smaller.



We may also need to compress a file to allow us to have additional room on a storage device, or to make a file small enough to send in an email.

There are two types of compression, these are:

- **Lossy Compression** — This is when the size of the file is reduced, however the quality of the file also reduces (meaning the quality gets worse)
- **Lossless Compression** — This is when the size of the file is reduced, however the quality of the file remains the same

Looking at the above you might now be thinking “why don’t we just always use lossless compression then? It reduces the file size, but we don’t lose quality, surely that’s best!”. Well, unfortunately lossless compression won’t always reduce the size of the file enough, and therefore isn’t always suitable. Therefore, sometimes we will have to use lossy compression to ensure the file is compressed enough to meet our needs.



“Although compression creates space on a hard drive, we wouldn’t want to compress absolutely everything in order to optimise space. You always have to find the balance between the quality of a file and the space it takes up”

Past Exam Questions

Answer the questions below, to help you revise what has been covered in 1.2 Memory and Storage.

1. State what is meant by 'RAM' and 'ROM' [2]

2. Describe what the purposes are of both RAM and ROM in a computer system [2]

3. Look at the table below. Tick **one** box in each row to show whether each statement is about RAM, or ROM [5]

Statement	RAM	ROM
Programs and data which are currently in use are loaded here		
All the contents are lost when the power is turned off		
It is used to boot up the computer when it is switched on		
It is usually measured in Gigabytes (GB)		
It is rewritable		

4. Mina's computer has 4GB of RAM.

i. Describe how the size of the RAM affects the performance of a computer [2]

ii. Mina decides to upgrade her RAM to 6GB.

Describe how this will now affect the performance of her computer [2]

5. Mina's computer also uses Virtual Memory (VM).

i. Describe what is meant by Virtual Memory [2]

ii. State why Virtual Memory is needed [1]

6. Most computer systems use at least one storage device.

i. Explain one reason why a secondary storage device is needed in a computer system [2]

ii. Describe why RAM cannot be used as permanent, long term storage [2]

7. State the three most common Secondary Storage technologies [3]

1. _____

2. _____

3. _____

8. Apu is looking to buy a new e-book reader. He is told it contains Secondary Storage, to store his downloaded books on.

i. State which type of storage is most suitable for storing the electronic books inside the e-book reader [1]

ii. Explain **one** reason why this type of storage is most suitable [2]

iii. Describe why magnetic storage would not be a suitable storage for the electronic books stored on the e-book reader [4]

9. Sally receives a free trial for a piece of software through the post on a CD-ROM.

i. State whether a CD-ROM is magnetic, optical, or solid-state storage [1]

ii. Give two reasons why a CD-ROM is suitable in this case [2]

1. _____

2. _____

10. A water sports club want to invest in cameras their customers can wear whilst taking part in their activities. The cameras are in waterproof cases, and not exposed to water.

Describe whether magnetic, optical, or solid-state storage would be the most appropriate for the water sports club to use, and why [2]

11. A secondary school is upgrading their computer equipment.

i. Complete the table below to show whether magnetic, optical, or solid-state storage is most appropriate for each of the following uses. Give a reason for each case.

The first one has been done for you.

Use	Magnetic, Optical, Solid State	Reason why this is most appropriate
Storing pictures in a digital camera	Solid State	It is not affected by the camera being shaken and moved around
Handheld devices used by students for field work		
Storage devices on the school's main file server		
Videos of the recent school drama production to be given to parents		
Storage devices for Year 11 students to store coursework on for multiple subjects		

13. Different secondary storage devices have different capacities and can hold different amounts of data.

Troy has downloaded a music file, which has a file size of 8485KB.

i. How many music files could Troy fit on a 4GB USB Memory Stick? [1]

ii. How many music files could Troy fit on a 3TB Hard Disk? [1]

iii. How many music files could Troy fit on a 640MB CD-ROM? [1]

14. Different secondary storage devices have different characteristics.

i. Why is capacity important when purchasing a new secondary storage device? [1]

ii. State three other characteristics of secondary storage devices [3]

1. _____

2. _____

3. _____

15. Convert the denary number 173 to binary. You must show your working. [2]

16. Convert the binary number 00111110 to denary. You must show your working. [2]

17. Convert the denary number 201 to hexadecimal. You must show your working. [3]

18. Convert the hexadecimal number BE to binary. You must show your working. [3]

19. Perform a one place left shift on the binary number 11110011. You must show your working. [1]

20. Perform a two-place right shift on the binary number 11110011. You must show your working. [2]

21. State what is meant by a character set. [1]

22. Describe the effect using a larger number of bits per character has on a character set. Refer to ASCII and Extended ASCII in your answer. [4]

23. In an image the colour red is represented using the binary code 1111.

a. Identify the number of bits per pixel used in this image. [1]

b. Identify the total number of possible colours this image could have. [1]

c. Describe how the number of bits per pixel effects the colour depth and file size of an image. [2]

24. Describe what is meant by the resolution of an image. [2]

25. Explain how the sample rate and bit depth effects the quality of a sound when it is converted to a digital wave. [4]

26. James is told the higher the sample rate the lower the file size of the sound.
Identify if James has been told the correct information or not and why. [3]

1.3 Computer Networks, Connections and Protocols

In this section you will revise the following:

1.3.1 Networks and Topologies

- Types of networks:
 - LAN (Local Area Network)
 - WAN (Wide Area Network)
- Factors that affect the performance of networks
- The different roles of computers in a client-server and peer-to-peer network
- The hardware needed to connect stand-alone computers into a Local Area Network:
 - Wireless Access Points
 - Routers
 - Switches
 - NIC (Network Interface Controller/Card)
 - Transmission Media
- The Internet as a worldwide collection of computer networks:
 - DNS (Domain Name Server)
 - Hosting
 - The Cloud
 - Web servers and clients
- Star and Mesh technologies

1.3.2 Wired and Wireless Networks, Protocols, and Layers

- Modes of connection:
 - Wired
 - Ethernet
 - Wireless
 - Wi-Fi
 - Bluetooth

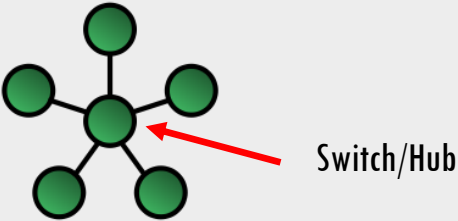
- Encryption
- IP addressing and MAC addressing
- Standards
- Common protocols including:
 - TCP/IP (Transmission Control Protocol/Internet Protocol)
 - HTTP (Hypertext Transfer Protocol)
 - HTTPS (Hypertext Transfer Protocol Secure)
 - FTP (File Transfer Protocol)
 - POP (Post Office Protocol)
 - IMAP (Internet Message Access Protocol)
 - SMTP (Simple Mail Transfer Protocol)
- The concept of layers

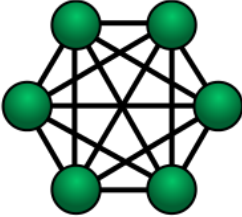


Technical Terms

Technical Term	Definition
Network	<p>This is where two or more devices are connected together to communicate.</p> <p>You must have at least two devices connected to create a network.</p>
Stand Alone	<p>This is a device that is not connected to any other devices and is therefore on its own.</p>
LAN (Local Area Network)	<p>This is a type of network.</p> <p>A LAN covers a small geographical area such as one building, or two buildings close together. Examples of LANs would be a school, a house, and a police station.</p>
WAN (Wide Area Network)	<p>This is a type of network.</p> <p>A WAN covers a large geographical area such as a city, country, or the world. Examples of WANs would be the internet, an international bank, or ATMs (Automated Teller Machine) that dispense money.</p>
Interference	<p>This refers to when signals are slowed down due to other factors. For example, it may refer to a brick wall slowing a signal down. It may also refer to other signals which then interfere with each other, slowing signals down. Devices such as microwaves emit signals which can interfere with signals sent out by mobile phones, routers etc.</p>
Bandwidth	<p>This refers to how much data can be sent and received over a network successfully in a given time. For example, a 32Mbps bandwidth means 32 Megabytes of data can be transferred over the network per second. This would therefore be slower than a 60Mbps bandwidth, as 60 Megabytes of data can be sent over this network per second.</p>
Client-Server Network	<p>This is a type of network where all the devices are connected to a central server. The server is responsible for distributing data to and from the clients (the users). The central server is also responsible for managing the network.</p>

Peer-to-Peer Network	This is a type of network where all the devices are responsible for being servers on the network. This means whenever data is requested from a server, all devices are responsible for searching for and sending the requested data, and devices manage the network.
Wireless Access Points	This is used to allow devices to connect to a network wirelessly, without the need of any cables.
Router	This is used to send data between multiple networks. You cannot connect to a WAN such as the internet without a router. A router often has a modem built into it now, which enables you to connect to the internet. A router uses an IP Address to direct traffic between networks.
Switch	This is used in a network to send data around a network. A switch however sends data only to the correct device on the network, rather than all the devices on the network. This is because they can read the data packets being sent and therefore work out where the receiver is.
Hub	This is used in a network to send data around a network. A hub however sends data to all devices on a network, rather than just the correct device.
NIC (Network Interface Controller/Card)	This is used to connect a device to a wired or wireless network and is built into the device. It uses protocols to ensure the communication between the device and network is consistent.
Cables	<p>These are used to create a wired connection in a network.</p> <p>Copper Cables (Unshielded Twisted Pair) – These cables are used to create a wired network. Copper cables are twisted around each other, where one cable is responsible for sending data, and one is responsible for receiving data.</p> <p>Fibre Optic Cables – Use light to transmit data. They can cover a much larger range compared to Copper Cables and have a much higher bandwidth due to less interference.</p>
Internet	This is a collection of LANs all connected together. It allows data to be transferred from one LAN to another.
WWW (World Wide Web)	This is a service used on the internet, to allow users to interact with the internet. It allows users to share data and files across the internet in a user-friendly way.

DNS (Domain Name Server)	A Domain Name Server contains the IP Addresses for the various web pages associated with a website. DNS are used as it makes using the internet more user friendly. Users find it easier to remember URLs rather than IP Addresses.
IP Address	An IP Address is unique to each device connected to the internet. IP Addresses are used to allow data to be directed around the internet from senders to the correct receivers.
MAC Address	These are addresses that a specific to a piece of hardware on a network. They are built into the hardware (NIC) and therefore cannot be changed.
Hosting	This is when websites are stored on servers dedicated to acting as DNS (Domain Name Servers). Hosts often provide 24/7 access to the website, access for multiple users, and greater security, compared to hosting your own website.
The Cloud	This is when your applications and data are stored and accessed via the internet, rather than locally (on your device).
Virtual Networks	This is when the logical structure is applied to a network independent of the physical structure. For example, you may have what appears to be one LAN, however that LAN is actually two separate LANs that both are independent of each other.
Star Topology	<p>This is a type of LAN.</p> <p>In a star topology all devices are connected to a central switch of hub, via their own cable. Each device on the star network is called a node. Data travels through the central switch of hub, therefore reducing data collisions and speeding up data transfer.</p> <p>We draw the star topology like this:</p> <div style="text-align: center;">  </div>

<p>Mesh Topology</p>	<p>This is a type of LAN.</p> <p>In a mesh topology all the devices on the network connect to as many other devices on the network as they can. Each device on the mesh network is called a node. Data travels in multiple directions and via multiple routes in a mesh network.</p> <p>We draw the mesh topology like this:</p> 
<p>Wi-Fi</p>	<p>Wi-Fi is a common standard for wireless networks and is the term we often use when referring to a wireless network.</p>
<p>Frequency</p>	<p>Due to data being transferred via signals, it has to be transferred via frequencies. Each frequency is then given its own channel.</p>
<p>Channel</p>	<p>This is attached to a frequency to allow us to identify different frequencies. As long as our devices (specifically our NIC) and the channels match up, our devices can communicate with each other.</p>
<p>Encryption</p>	<p>This is a security measure when sending data. Data is scrambled into a secret code, which can only be decrypted using a master 'key'. Only the sender and receiver have this key, which therefore prevents the data being hacked/intercepted, and understood.</p> <p>Prior to encrypted data being sent, both devices check with each other to ensure they have the correct master key.</p>
<p>Ethernet</p>	<p>This is a standard for communication on a wired LAN.</p> <p>Often now twisted pair cables are used as it allows data to be both sent and received at the same time.</p>
<p>IP Address</p>	<p>An IP Address is unique to each device connected to the internet. IP Addresses are used to allow data to</p>

	be directed around the internet from senders to the correct receivers.
MAC Address	These are addresses that are specific to a piece of hardware on a network. They are built into the hardware (NIC) and therefore cannot be changed.
Protocol	This is a rule or standard that devices must follow when communicating with each other over a network. This allows devices to be able to communicate effectively.
TCP/IP (Transmission Control Protocol/Internet Protocol)	This protocol sets out the rules devices must follow when communicating with each other. It also plays an important role in packet switching.
HTTP (Hyper Text Transfer Protocol)	This protocol is used to transfer web pages from web servers to clients.
HTTPS (Hyper Text Transfer Protocol Secure)	This protocol is a more secure version of HTTP. Data sent using this protocol is encrypted and therefore is more secure. This protocol will be used when transferring secure web pages such as when users log into their online banking accounts.
FTP (File Transfer Protocol)	This protocol is used to transfer large files over a network and organise files for websites on a web server.
POP (Post Office Protocol)	This protocol is used to access emails from an email server for the client to read. The email is downloaded and therefore removed from the web server when accessed.
IMAP (Internet Message Access Protocol)	This protocol is also used to access emails from an email server for a client to read. However, this protocol allows the user to access the email directly from the email server, therefore removing the need to download or remove it. It is more advanced than POP.
SMTP (Simple Mail Transfer Protocol)	This protocol is used to send emails to an email server.
Network Layers	Networking is complex, so it is broken down into layers to make the problem more manageable. Each layer addresses its own problem, but all layers work together overall.
Physical Layer	This is the physical part of the network we can see and touch, such as the router, cabling, switch etc.
Data Link Layer	This layer is responsible for connecting and linking devices together on a network. It decides whose turn it is to communicate on the network and converts data into data signals ready for sending.

Network Layer	<p>This layer transmits data across a network. It identifies the destination IP Address and the quickest route.</p>
Transport Layer	<p>This layer establishes a connection with the network. It then agrees protocols, size of packets, speed of transfer etc. between the sending device and the receiving device.</p>
Data Packets	<p>Data is too large to be sent over a network in one big go. Therefore, data is broken down into lots and lots of data packets.</p> <p>Each data packet is given a header which contains important information such as:</p> <ul style="list-style-type: none"> ▪ Senders IP Address – Where the packet has come from ▪ Receivers IP Address – Where the packet is being sent to ▪ Error Check – Determines whether the packet arrives correctly ▪ Packet Sequence – The order in which the data packets are put back together ▪ Data – The data from the original request itself
Packet Switching	<p>This is the process of sending data packets over a network. There are multiple steps involved in packet switching:</p> <ol style="list-style-type: none"> 1. A request is received from a client. TCP breaks down the data being requested into lots of data packets 2. Each packet is stamped with important information such as senders address, error check etc. 3. The packets are sent to the receiver via the quickest route by IP. Packets will often split up here. It doesn't matter how they get to the receiver, just that they get there, and get there as quickly as possible 4. Once the packets are received an error check takes place 5. TCP checks to see if the transmission between to the sender and receiver was successful. 6. If any packets are missing or are damaged, the clients TCP will request for them to be resent

7. A timer is set. Should the requested packet not arrive within a specific amount of time, an error message is sent back to the sender
 8. TCP then puts the packets back together again using the packet sequence
- Finally, the user sees the information they requested

Networks

A **network** is two or more devices that are connected so that they can communicate with each other.

To have a network, you must have at least two devices connected to each other. A device that is not connected to any other devices is called a **Stand-Alone device**. This is because it stands on its own and has no other devices to communicate with.

There are many advantages and disadvantages to creating a network.

Advantages:

- ✓ Users can share files with each other, and therefore work collaboratively
- ✓ Users can share peripherals on the network, such as printers
- ✓ Users can share an internet connection, saving the need to create and pay for multiple connections
- ✓ Users can access files and data from any device on the network
- ✓ Users can communicate with each other over the network e.g. emails
- ✓ Software updates can be rolled out all in one go across all the devices on the network, saving time



Disadvantages:

- ❖ There is an increased security risk to data. Devices are easier to hack when connected on a network
- ❖ Malware and viruses can spread easily and quickly between devices on the network if appropriate security measures are not put in place
- ❖ If the server for the network fails, the whole network may go down
- ❖ If there is a large amount of data travelling over the network, the devices on the network may slow down
- ❖ Networks can be expensive to install and maintain e.g. the buying and installation of the hardware, and hiring someone to monitor the network can be expensive



Networks: The Types

There are multiple different types of networks: LAN, MAN, WAN, PAN, VPN, VLAN.

The two we are focusing on in this section are LAN (Local Area Network) and WAN (Wide Area Network).

LAN (Local Area Network):

A LAN is a network that covers a small geographical area, such as one building or two buildings close together. Some examples of LANs are:

- A school
- A house
- A corner shop

WAN (Wide Area Network):

A WAN is a network that covers a large geographical area, such as a city, country, or the world. They are a series of LANs all connected. Some examples of WANs are:

- The internet
- An international bank
- ATMs (Automated Teller Machines) that dispense money



“If asked to give examples of either a LAN or WAN, be specific. For example, if you are saying a police station is an example of a LAN, make sure you say, ‘one individual police station’. Likewise, if you are saying a police station is an example of a WAN, make sure you say, ‘multiple police stations spread across the country’. Simply saying ‘police station’ is confusing!”

Factors that affect the performance of a network

There are multiple factors that can affect the performance of a network. Don't forget, this could be positive or negative!

Bandwidth:

This is the amount of data that can be sent and received successfully in a given time. Bandwidth is measured in bits per second e.g. a 32Mbps bandwidth would mean 32 Megabytes of data can be transferred over a network every second.



“It is important to remember that bandwidth is **not** a measure of how fast the data travels, but how much data can be sent at once. Although we often think of bandwidth as the speed of the network, it isn't directly the speed. However, it does impact upon it”

Number of Users:

The number of users on the network will impact upon the performance of the network. Too many users on the network will mean more of the bandwidth is being spread out to try and meet all the users' needs. When there is not enough bandwidth to manage all the users on the network, the network will slow down.

Transmission Media:

The media you choose to use in your network will impact upon how well it can perform. A wired network for example has a higher bandwidth compared to a wireless network, due to less interference. Using fibre optic cabling rather than copper cabling will have a higher bandwidth, due to less interference again.

Error Rate:

This refers to the number of errors that occur when data is transferred. The higher the error rate, the more frequently data has to be resent before arriving safely and correctly.

For example, the error rate on a wireless network is likely to be higher than the error rate on a wired network, due to the data having to be transmitted via waves and likely to be interfered with. The error rate is also likely to increase the further away a user is from the wireless access point.

Latency:

This is the delay from transmitting data to receiving it. This can be increased by not having the correct network hardware to direct traffic around the network appropriately, causing 'traffic jams' and therefore slowing data down.



The number of users on a network is one factor that can affect the performance of a network.

Describe two factors, other than the number of users, that can affect the performance of a network [4]

Hint: The question is worth four marks. You will get one mark for naming a factor, and one mark for describing it. You need to name and describe two different factors. You cannot use 'Number of Users' though!

Client-Server vs Peer-to-Peer

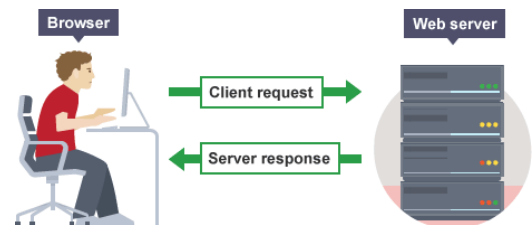
When creating a computer network, there are different types of network we can create.

Two of these are a **Client-Server** network, and a **Peer-to-Peer** network.

When discussing these two networks, we are going to refer to clients and servers. A client is a device that is requesting information. A server is a device that is sending information.

Client-Server:

In this model the relationship between client and server is that the client makes a service request to the server. The server then sends the requested information to the client. For example, a user sends a request to the server for a website using a web browser. The server processes the request and sends back all the appropriate information for that website.

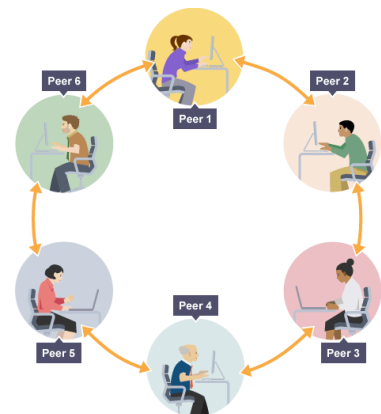


There is a central dedicated server (or group of central dedicated servers in larger businesses), and all clients request information from them.

Peer-to-Peer:

In this model there is no central dedicated server. Instead, all the devices on the network take on the responsibility of being a server, storing files and handling service requests. Each device has an equal responsibility for providing data when requested.

For example, if a client requests the same website using the same web browser as above, rather than that service request going to a dedicated server, it will now be sent round each device on the network. Each device will search through its files and storage to see if it has the requested information. If it does it will send it back to the client. If it doesn't it will pass the request on to the next device, and so on.



Both networks have their advantages and disadvantages. We can see these in the table below:

	Client-Server	Peer-to-Peer
Security	The server controls security of the network, and this is managed centrally. Security can be rolled out across all devices and be consistent across each device	All devices are responsible for security of the network and their own security. Security features may not be consistent with each other
Management	The dedicated server manages the network. However, it needs a team of specialised network engineers to manage and maintain the server	No central managing of the network, anyone can set it up and be responsible for it
Dependency	Clients are all dependent on the server. Should the server go down or experience high traffic and slow down, all clients will be affected	Clients are not dependent on one single server, therefore if one 'server' goes down, other clients can continue to act as servers and the network can continue to function
Performance	Server can be upgraded easily to improve and maintain performance of the network. However, upgrading a server can be expensive	If devices on the network are slow, they slow the whole network down. However, upgraded devices (depending on the number you have) can be cheaper than upgrading a server
Backups	Data is backed up on the server, meaning it is easy to access should there be a data breach (the data gets hacked and stolen), or loss of data	Each device on the network has to be backed up individually. This can lead to data being lost, not backed up, or media containing the backups being lost

Hardware required to create a LAN

There are many different pieces of hardware required to create a LAN, all of which do a specific job in order to allow devices on the LAN to communicate with each other.

These pieces of hardware are the **NIC (Network Interface Controller/Card)**, **Wireless Access Point**, **Switch**, **Router**, **Cabling**.

NIC (Network Interface Controller/Card):

The job of the NIC is to connect a device to a wired or wireless network and is built into the device. It uses protocols to ensure the communication between the device and network is consistent.



Wireless Access Point:

A Wireless Access Point is used to allow devices to connect to a network wirelessly, without the need of any cables. We will discuss the advantages and disadvantages to using a wired or wireless connection shortly.



Switch:

A Switch is used to send data around a network. A switch however sends data only to the correct device on the network, rather than all the devices on the network. This is because they can read the data packets being sent and therefore work out where the receiver is.



Hub:

A Hub is used to also send data around a network. A hub however sends data to all devices on a network, rather than just the correct device. This is therefore not good for security, as it allows any device on the network to intercept a data packet and potentially steal its contents.



Router:

A Router is used to send data between multiple networks. You cannot connect to a WAN such as the internet without a router. A router often has a modem built into it now, which enables you to connect to the internet. A router uses an IP Address to direct traffic between networks.

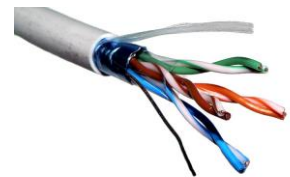


An **IP Address** is unique to each device connected to the internet. IP Addresses are used to allow data to be directed around the internet from senders to the correct receivers.

Cabling:

If you choose to have a wired connection, then you will require cabling. Cables are used to create a wired connection in a network. There are two main types of cabling used today:

Copper Cables (Unshielded Twisted Pair) – These cables are used to create a wired network. Copper cables are twisted around each other, where one cable is responsible for sending data, and one is responsible for receiving data. Copper Cables can also be known as Ethernet Cables.



Fibre Optic Cables – Use light to transmit data. They can cover a much large range compared to Copper Cables and have a much higher bandwidth due to less interference. Fibre Optical cabling still remains expensive and is therefore still emerging. However, it is now starting to be more widely used.



Therefore, if you are thinking of having a wired connection, it is better to go for Fibre Optic rather than Copper Wire, despite the cost!



“This topic is one of the more difficult ones in the course, so don’t be worried if you are struggling to remember all of these different pieces of network hardware and their roles! Try to remember the names of each device first, then their job role”

Wired or Wireless Network?

There are advantages and disadvantages to having both a wired or a wireless network.

Remember, a wired network requires the user to plug an ethernet cable into their device in order to access the network. A wireless network however allows the user to connect to a network without the need for cables.

Characteristic	Wired or Wireless?
Bandwidth	<p><u>Wired Networks:</u></p> <p>Due to there being less interference in a wired network compared to a wireless network, a wired network is more likely to have a higher bandwidth. This means a wired network will be able to cope with more traffic and more users compared to a wireless network.</p>
Range	<p><u>Wireless Networks:</u></p> <p>With a wired network you are restricted to the locations where you can access an ethernet cable. With a wireless network, you are able to connect to the network wherever you want, as long as you are in range of the Wireless Access Point.</p>
Security	<p><u>Wired Networks:</u></p> <p>If someone wants to hack into your network and you have a wired network, they have to physically plug an ethernet cable into their device. This means it is much more difficult to secretly hack a wired network. This is compared to a wireless network where, as long as the user is in range of the Wireless Access Point, they can attempt to hack the network.</p>
Cost	<p><u>Wireless Networks:</u></p> <p>It is cheaper to set up a wireless network, as you only need to purchase the Wireless Access Point and other necessary hardware. This is compared to a wired network where you would need to buy all the necessary hardware, as well as run cabling all through the building. This would cost for both the cabling and the installation damage, as well as the cost for the specialist team to come and fit the cabling</p>

The Internet and WWW

The **internet** is one of the most powerful creations to date. More than 3 billion people now use the internet, compared to 738 million in 2000, and this growth shows no signs of slowing down.

However, we often think of the internet and the **WWW (World Wide Web)** as the same thing, but they're not.

The internet is a collection of LANs all connected. It allows data to be transferred from one LAN to another. The internet is the physical part of the WAN, containing all the hardware required to share data across a large area.

The WWW (World Wide Web) is a service used on the internet, to allow users to interact with the internet. It allows users to share data and files across the internet in a user-friendly way.

In order to access the internet, a user must be connected to an ISP (Internet Service Provider). Examples of ISPs are Sky, Virgin, and BT.

DNS (Domain Name Servers):

DNS (Doman Name Servers) are special servers on the internet. Their job is to convert URLs the user types in into IP Addresses, so the locations of web pages associated with a website can be found.

For example, if we wanted to access the BBC website, we would type into our web browser `www.bbc.co.uk`. This is easy for us to remember. However, if we needed to remember the IP Address instead, we would need to remember `151.101.64.81`. Imagine having to remember that type of IP Address for all your favourite websites! It wouldn't be possible.

This is where the DNS comes in. When we search for a website using a URL, the DNS searches a database to find the IP Address for the website, which then directs us to the correct server containing all the information for that website. If the first DNS does not have the required information, it will pass us on to another DNS, which will check, and so on.

Hosting:

In order for a website to be available on the internet for users to access, it must be hosted. **Hosting** is when websites are stored on dedicated servers. Hosts often provide 24/7 access to the website, access for multiple users, and greater security, compared to hosting your own website. However, should the host server go down, your website will go down also. This could lose you money or customers, so there are both advantages and disadvantages to paying a company to host your website.

Web servers and Clients:

Data for websites is stored on a web server. These are special, dedicated servers responsible for managing requests from clients and sending data so websites can be viewed and accessed. A client is a device that is requesting this data. When loading up a website the client will send a request to the web server for the relevant websites data; the web server will process this request (here a process called packet switching takes place) and then send the requested data to the client.

The Cloud:

Cloud Computing is becoming more and more popular, as our lives become busier and busier. Cloud Computing is when your applications and data are stored and accessed via the internet, rather than locally (on your device).

There are both advantages and disadvantages to using the cloud:

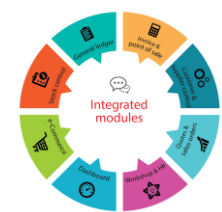
Advantages:

- ✓ Data is often backed up in a different location to where your network is, therefore protected should you ever need to restore it due to loss or theft
- ✓ There is often cross compatibility, meaning applications and files can be accessed on different devices (e.g. phones, tablets, laptops etc.)
- ✓ Updates for applications are done automatically, meaning you always have the most up to date version of the application
- ✓ Online applications are often free, saving the cost of buying licenses for the application
- ✓ People can work on the go, and on multiple devices, as long as they have an internet connection



Disadvantages:

- ❖ When something is uploaded to the cloud, you can sometimes lose ownership to it, which can lead to Copyright issues
- ❖ You are usually limited to a small amount of storage space for free, before having to pay for further storage
- ❖ The applications provided may not always offer you all the features you want or need, compared to the bought versions
- ❖ Data is easier to hack when stored online. Despite companies who offer cloud services providing security measures, it is not possible to guarantee data security
- ❖ Users must always have an internet connection in order to access applications and files. Therefore, if your internet connection drops, you would not be able to access your files or applications





Julie owns her own business and spends on average three hours a day travelling to and from work.

Describe why Cloud Computing would be advantageous for Julie [4]

Hint: The question is worth four marks. You will get one mark for naming a relevant advantage, and one mark for describing it. You need to name and describe two different advantages. Note – It must be a relevant benefit for Julie! Think about her travelling time, loss of working hours, how she would only have access to her handheld devices etc.

Network Topologies

A **topology** is a type or shape of a LAN. Each topology has its advantages and disadvantages. We are going to look at the bus, ring, star, and mesh topologies. For each topology, you need to be able to draw it, describe it, and provide advantages and disadvantages.

It is important to note that when drawing a topology, we show wired and wireless connections in different way:

- A solid line is used to show a wired connection between two devices
- - - A dashed line is used to show a wireless connection between two devices

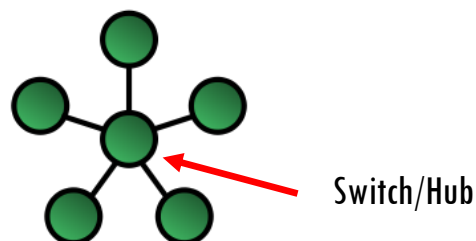
Star Topology:

In a **star topology**, all devices are connected together via a central switch/hub. Each device is connected via its own cable to the switch/hub, and therefore is independent to other devices on the network.



“Remember, a switch sends data to only the correct device because it can read the data packet, compared to a hub which sends it to all devices. We would therefore be better using a switch in a star network”

Data in a star topology is sent via the central switch/hub. The data is sent from the sender, the switch/hub then distributes the data. Again, each device in a star network is called a node. We draw a star topology like this:



The advantages to the star topology are:

- ✓ Limited data collisions due to the switch/hub managing data flow, reducing the error rate of the network
- ✓ Easy to add additional devices to, and also to add additional switches/hubs to, which allows you to expand the network
- ✓ If one device on the network fails, the network can still continue to work

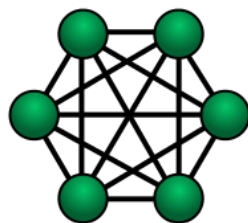
The disadvantages to the star topology are:

- ❖ Additional cost due to needing to purchase a switch/hub
- ❖ If the switch/hub fails, then the network will fail

Mesh Topology:

In a **mesh topology**, all devices are connected to as many other devices as possible. This creates multiple connections between devices.

In a mesh topology, data flows in multiple directions around the network. As there are multiple connections, data can flow via the quickest route if there is a build-up of traffic on the network. Again, each device on the network is called a node. We draw a mesh topology like this:



The advantages to the mesh topology are:

- ✓ If one connection fails, the network can still continue to work. Data will simply just be routed via a different connection in order to reach its destination
- ✓ Data transfer can be quick. This is due to having multiple connections. If data traffic builds up in one area of the network, then alternative routes can be used to ease congestion and reduce latency

The disadvantages to the mesh topology are:

- ❖ Increased cost due to the amount of cabling and switches required

Wi-fi: Frequencies, Channels, and Encryption

Wi-fi is a common standard used for wireless networks. It is often what we refer to when connecting to a wireless network.

In order for data to be sent via Wi-fi, **frequencies** and **channels** are used.

Frequencies are used to transmit signals. 2.417GHz is an example of a frequency. In order to make the frequency more convenient to remember and use, it is given a channel number. For example:

2.417GHz — Channel 1

2.427GHz — Channel 2

2.437GHz — Channel 3

In order for devices to connect via Wi-fi, the channels must be set to the same. For example, if your router is set to channel 2, but your computer is set to channel 3, the devices will not be able to connect to each other. The channel is set by the NIC (Network Interface Controller/Card) but this can be changed by the user. As long as two devices on the network are set to the same channel, they can communicate with each other.

This is where interference can also affect your network too. If other devices are set to the same channel, they can interfere with the signals being sent between your device and the router. This can then slow your connection down.

However, if data is being sent wirelessly, it is easier to intercept and steal. Data therefore must be **encrypted**, in order to protect it whilst being transmitted.

Encryption:

Encryption involves scrambling data before being transmitted, into a secret code. In order to decrypt the code, you must have a 'master' key. Only the device sending and the device receiving the data has this key. This is because prior to the data being sent, a 'handshake protocol' is used to ensure the same correct and valid key is being used by both the sender and receiver.

Ethernet

Ethernet is a standard for networking technologies, used for communication on a wired LAN (Local Area Network).

Twisted Pair Cables are commonly used now for creating ethernet connections. This is because it allows data to be both sent and received at the same time, due to different wires being used for both. Previously, a special protocol called CSMA/CD (Carrier Sense Multiple Access/Collision Detection) was used to detect when data was being transmitted over a wired network. It would detect communication on the network to avoid transmitting data at the same time, therefore avoiding data collisions. Due to Twisted Pair Cables having separate cables for sending and receiving, this is no longer necessary.

When data is transmitted via an ethernet connection, it is transmitted in frames. These include:

- Bits used to synchronise transmission and receiver clocks
- Start frame delimitator to signify the start of the data packet of the frame
- Sender and receiver MAC Addresses
- Actual data
- Cyclic redundancy check used for error checking on the frame

IP Addresses, MAC Addresses, and Protocols

In order for data to be transmitted over and between networks, **IP Addresses** and **MAC Addresses** are required.

An IP (Internet Protocol) Address is unique to each device connected to the internet. IP Addresses are used to allow data to be directed around the internet from senders to the correct receivers.

A MAC (Media Access Control) Address however is specific to a piece of hardware on a network. They are built into the hardware (NIC) and therefore cannot be changed.

Look at the table below, which identifies the differences between IP Addresses and MAC Addresses:

IP Address	MAC Address
IP Addresses can be both static and dynamic. This means they can remain the same and not change (e.g. the IP Address of a web server), but they can also be changed (e.g. the IP Address of a device on a network)	MAC Addresses are fixed into the NIC (Network Interface Controller/Card) of each device, and therefore cannot be changed
IP Addresses are configured (created and managed) by software	MAC Addresses are configured (created and managed) by hardware
An example of an IP Address could be 69.89.31.226	An example of a MAC Address could be 00:0a:95:9d:68:16

Network protocols are also required, in order for devices to be able to communicate over a network.

A network protocol is a rule (or set of rules) or standard devices must follow when communicating over a network. Without protocols, communication on a network would not be possible.

There are multiple protocols used in networking, all of which work in conjunction with each other to ensure communication over a network is smooth and effective. These are **TCP/IP (Transmission Control Protocol/Internet Protocol)**, **HTTP (Hyper Text Transfer Protocol)**, **HTTPS (Hyper Text Transfer Protocol Secure)**, **FTP (File Transfer Protocol)**, **POP (Post Office Protocol)**, **IMAP (Internet Message Access Protocol)**, and **SMTP (Simple Mail Transfer Protocol)**.

TCP/IP (Transmission Control Protocol/Internet Protocol):

This protocol sets out the rules devices must follow when communicating with each other over a network. It also plays an important role in packet switching (TCP), and routing of packets on a Wide Area Network (IP).

HTTP (Hyper Text Transfer Protocol):

This protocol is used to transfer web pages from web servers to clients.

HTTPS (Hyper Text Transfer Protocol Secure):

This protocol is a more secure version of HTTP. Data sent using this protocol is encrypted and therefore is more secure. This protocol would be used when transferring secure web pages such as when users log into their online banking accounts.

FTP (File Transfer Protocol):

This protocol is used to transfer large files over a network, and to organise files for websites on a web server.

POP (Post Office Protocol):

This protocol is used to access emails from an email server for the client to read. The email is downloaded onto the user current device and therefore removed from the web server when accessed.

IMAP (Internet Message Access Protocol):

This protocol is used to access emails from an email server for the client to read. However, this protocol allows the user to access the email directly from the email server, therefore removing the need to download or remove it. It is more advanced than POP.

SMTP (Simple Mail Transfer Protocol):

This protocol is used to send emails to an email server.



“These protocols are best remembered in groups. Both HTTP and HTTPS are responsible for web pages. SMTP, IMAP, and POP are all responsible for emails. Then TCP/IP and FTP are on their own”

It's your turn!

Describe the difference between HTTP and HTTPS

[4]

Network Layering

As you can see from all the content above, networking is a complex job! Network layers however allow us to make the problem more manageable. Networking is broken down into multiple layers. Each layer addresses its own problem, but all layers work together overall.

The four layers we need to make sure we understand are the Physical Layer, Data Link Layer, Network Layer, and Transport Layer. However, in order to best understand network layering, we will cover all the relevant layers.

Here is a diagram that shows each layer and its role:



Application Layer — This layer makes sure the data being produced and sent is in a format the application being used can understand

Presentation Layer — This layer deals with how the data should be presented e.g. does it need to be encrypted? Does it need to be compressed? Etc.

Transport Layer — This layer establishes a connection with the network, and agrees protocols, size of packets, speed of transfer etc. with the receiving device

Network Layer — This layer transmits data across the network. It identifies the destination IP address and the quickest route

Data Link Layer — This layer connects/links to devices on the network. It also decides whose turn it is to communicate, and converts all data into digital signals for sending

Physical Layer — This layer is the physical part of the network we can see and touch e.g. cabling, switches, routers etc.

Each layer links to the previous and next layer, allowing communication over a network to be made simpler. Each network works independently to the other layers so can be modified without disrupting the other layers

Past Exam Questions

Answer the questions below, to help you revise what has been covered in 1.3 Computer Networks, Connections and Protocols.

1. State what is meant by a ‘computer network’ [1]

2. Abid owns a business. He has been advised to install a LAN.

i. Describe what is meant by a LAN [2]

ii. Explain one advantage and one disadvantage to using a computer network [4]

iii. Identify three examples of a LAN [3]

- 1. _____
- 2. _____
- 3. _____

3. Ben explains to Abid that a school is an example of a WAN.

Explain why Ben is wrong [2]

4. In his home, Ben has a Peer-to-Peer network.

i. Explain what is meant by a Peer-to-Peer network [2]

ii. A friend of Bens has told him a Client-Server network exists also.

Describe what is meant by a Client-Server network [2]

iii. Explain two differences between a Peer-to-Peer network and a Client-Server network [4]

5. In order to set up a network in her home, Julie needs to purchase some network hardware.

i. Identify the job role of a router [1]

ii. Julie wants a wireless connection.

Describe what piece of hardware Julie will require in order to have a wireless connection [2]

ii. Julie is told that if she wants a wired connection, she should use fibre optic cabling.

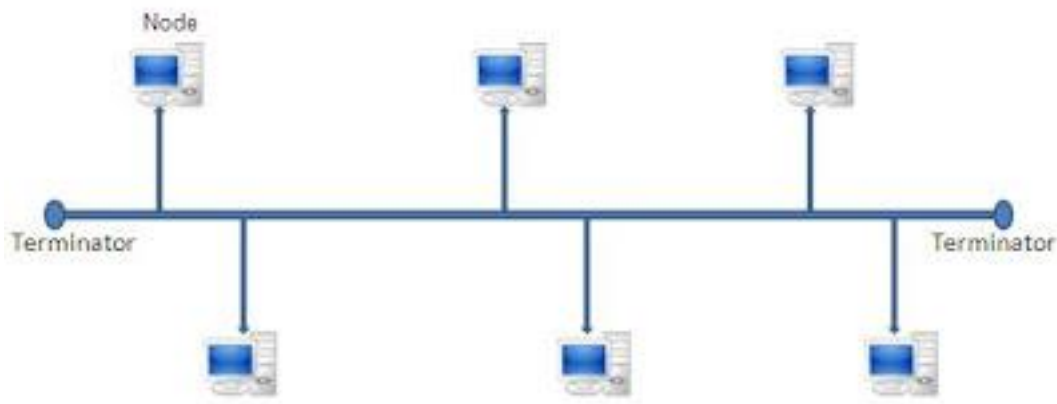
Describe why Julie should use fibre optical cabling instead of copper wire cabling [2]

7. Mr Singh searches for a website on his computer at home.

Describe the process of how the relevant information is retrieved for Mr Singh [4]

8. Describe one advantage and one disadvantage to using The Cloud [4]

9. The following diagram shows how the computers in a school are connected together to form a LAN:



i. State the correct name for this network topology [1]

ii. Describe the role of the terminator [2]

iii. Describe why a CSMA/CD protocol may be used in the above LAN [2]

10. The school has been advised that a star network may be better.

Explain what a star network is. You may draw a diagram to help explain your answer [4]

11. Explain the difference between a switch and a hub

[2]

13. Sally has noticed her laptop is not connecting to her router. Her ISP has told her it may be something to do with the channels her laptop and router are using.

Explain, with reference to channels, why Sally's laptop and router cannot connect [2]

14. Describe how data can be secured when being transmitted over a wireless network [3]

15. Devices connected to a network have an IP Address and a MAC Address.

i. Describe what is meant by an IP Address [2]

ii. Describe what is meant by a MAC Address [2]

iii. Describe two differences between IP Addresses and MAC Addresses [4]

16. Protocols are used in network communication.

i. Describe what is meant by a network protocol [1]

ii. Identify three network protocols [3]

1. _____

2. _____

3. _____

iii. Describe why HTTPS is likely to be used instead of HTTP when transmitting sensitive and confidential information over the internet [2]

17. Network layering is used when describing how networks work.

i. Describe what is meant by network layering [2]

ii. Identify two network layers [2]

1. _____

2. _____

18. When data is transmitted over the internet, packet switching is involved.

Explain how data is transmitted over the internet using packet switching [5]

1.4 Network Security

In this section you will revise the following:

1.4.1 Threats to Computer Systems and Networks

- Forms of attack:
 - Malware
 - Social Engineering e.g. phishing, people as the 'weak point'
 - Brute-force attacks
 - Data interception and theft
 - The concept of SQL injection

1.4.2 Identifying and Preventing Vulnerabilities

- Common prevention methods:
 - Penetration testing
 - Anti-malware software
 - Firewalls
 - User access levels
 - Passwords
 - Encryption
 - Physical security



Technical Terms

Technical Term	Definition
Threat	This is something that poses possible damage to either your network or your business e.g. loss of customers and revenue.
Malware	This is software that aims to damage and corrupt a computer system, by spreading around the system as quickly as possible. Examples include viruses, worms, and spyware.
Phishing	This is when an individual pretends to be someone you can trust, in order to gain confidential and important information from someone e.g. bank details.
Weak People	Weak people are people who work within the business but are careless and therefore open up opportunities for threats to access the network. Some of these opportunities could be not keeping protection software up to date, sharing usernames and passwords, not locking devices when they walk away etc.
Brute Force Attack	This is when an automated program continually tries to gain access to the network. This is to try and potentially steal data or access corporate systems.
DDOS (Denial of Service Attack)	This is when a network server is overloaded with requests which it cannot handle, causing the server to crash. This therefore brings down the network.
Data Interception and Theft	This is when data is intercepted (stolen) from the network, either directly from the network or during transmission. It may be usernames and passwords to access the network, or other crucial information such as customer information.
SQL Injection	This is when the contents of a database are outputted, revealing private and confidential information. It also opens up the possibilities for data to be amended, appended, or removed from the database.
Network Policy	This refers to the rules and regulations that must be followed when using the network. For example, one policy for the network may be to change passwords every three months.
Penetration Testing	This is when either an individual or group try to gain unauthorised access to the network. This then reveals areas of weakness in the network, which can then be fixed to prevent the danger of real threats.

Network Forensics	This is the monitoring and recording of activity on the network. This then allows network managers to locate potential misuses of the network, as well as trace back threats to find where they first entered the network.
Anti-Malware Software	This software is used to prevent and remove malware. It scans devices and alerts users to potential threats found on their device, so they can be removed.
Firewalls	This is used to control what goes in and what goes out of the network. It prevents unauthorised access by only allowing authorised access to the network.
User Access Levels	User Access Levels provide different levels of access to the network depending on who the user is. For example, a network manager would need to be able to access all the different elements of the network. An admin assistant however wouldn't need such high level of access, so won't be able to access as much.
Passwords	These allow users to access the network using a combination of letters, numbers, and characters only they know.
Encryption	<p>This is a security measure when sending data. Data is scrambled into a secret code, which can only be decrypted using a master 'key'. Only the sender and receiver have this key, which therefore prevents the data being hacked/intercepted, and understood.</p> <p>Prior to encrypted data being sent, both devices check with each other to ensure they have the correct master key.</p>
Physical Security	This refers to the process of securing the actual hardware of the network with physical measures such as locking doors to server rooms, placing servers in cabinets that lock etc.

Reasons for Attack

Before we go into detail on the various ways someone can attack or protect a network, it is important to understand some reasons why people may want to attack a network.

Most businesses and individuals heavily rely now on access to a network, in order to keep a constant flow of data. Therefore, if someone wants to damage a business or individual in a way, they may be able to get away with it, then bringing down a network is where they may look to.

There are multiple reasons why someone might want to bring down a network:

- To gain a competitive advantage over the business or individual (customers may lose trust in the company that has gone down, and look to its rivals for more security)
- To blackmail an individual in order to gain either money or something similar
- Outline political views the individual may have (they may not agree with the business or its values)
- To exploit weaknesses in the businesses network security
- Simply due to boredom

Despite some of the above seeming to be unjustified reasons to bring down a whole network, they still happen. Key examples are the recent shutdowns of PlayStation Network and the NHS, both of which were shut down for days for different reasons.

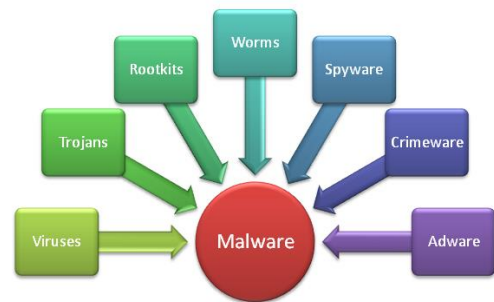
Threats to a network

There are various threats to a network, all of which could cause considerable damage to a network.

These are **Malware**, **Phishing**, **Weak People**, **Brute Force Attacks**, **DDOS Attacks (Distributed Denial of Service)**, **Data Interception and Theft**, **SQL Injection**, and **Weak Network Policies**.

Malware:

Malware (also known as bad software), is software that aims to damage and corrupt a computer system, by spreading around the system as quickly as possible. Malware can often be downloaded accidentally, as it is often attached to something else a user downloads that seems genuine and safe. Malware can often go undetected for long periods of time with the right protection methods in place, and easily spread from one device to another via emails, secondary storage, and shared files.



Examples include viruses, worms, and spyware.

Phishing:

Phishing Scams have been around for long periods of time. However, now we all do everything on the internet, they have become much more popular on there. The purpose of a Phishing Scam is to try and entice confidential and important information out of someone by pretending to be someone they can trust.



For example, a phisher pretending to be your bank may email you claiming you have won a prize for being a loyal customer. They make the email seem genuine, so it looks just like an email from your bank would. They ask you to click on a link they provide and log in to your account to claim your prize. Again, the website you are taken to looks genuine and real. However, once you attempt to log in, your log in fails, and your details are sent directly to the phisher.

Weak People:

One of the biggest threats to a network are the people that actually work using the network. Often users may lack the necessary security knowledge in order to keep the network safe from threats, and therefore put the network at risk.

Some of the dangers Weak People pose to a network are:

- Leaving computers logged on and unattended
- Writing passwords down on sticky notes and storing them on desks
- Sharing passwords with colleagues
- Not ensuring protection software is up to date
- Opening email attachments without ensuring they are safe first



Brute Force Attacks:

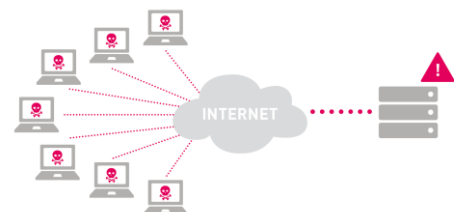
A Brute Force Attack is when an automated program continually tries to gain access to the network. This is usually done by trying to repeatedly guess a password until it gains entry. The program will try hundreds and thousands of combinations of letters, numbers, and characters in order to try and guess a password. It will also try commonly used passwords such as 'Password' or the users name.



This is to try and potentially steal data or access corporate systems.

DDoS Attack (Distributed Denial of Service):

A DDoS Attack occurs when a networks server is overloaded with requests which it cannot handle, causing the server to crash. This therefore brings down the network. It is possible then that whilst the network is down, further damage can be done to the network such as data theft, as it is likely the security systems for the network will be down also.



Data Interception and Theft:

Data Interception and Theft is when data is intercepted (stolen) from the network, either directly from the network or during transmission. It may be usernames and passwords to access the network, or other crucial information such as customer information.



SQL Injection:

SQL (Structured Query Language) is the language used for managing and maintaining databases. Databases are used in businesses to store vital and confidential information such as customer details and business accounts.

SQL Injection occurs when a user attempts to gain access to the database and the contents of a database are outputted, revealing private and confidential information. It also opens up the possibilities for data to be amended, appended, or removed from the database. SQL injection is often carried out by running a malicious SQL code in a form (such as those you may fill out when creating a new email account) that, when the form is submitted, interacts with the database directly.



Exposure of customer details can cause customers to lose faith in the businesses ability to keep their information private and safe. This could cause them to leave and cost the business in lost revenue.

Preventing Threats

Due to the fact there are multiple threats to a network, there has to be multiple ways we can prevent each threat. Some prevention methods specifically target an individual threat, whilst others can be used to prevent more than one threat.



The prevention methods we need to be aware of are **Penetration Testing**, **Anti-Malware Software**, **Firewalls**, **User Access Levels**, **Passwords**, and **Encryption**.

Penetration Testing:

Penetration Testing is when a legitimate individual or group try to gain unauthorised access to the network. This then reveals areas of weakness in the network, which can then be fixed to prevent the danger of real threats. We often call these people 'White Hat Hackers'. They will attempt to hack into a network, not to illicit money or information, but to allow those vulnerabilities to be fixed.



This then helps to prevent 'Black Hat Hackers' from gaining access to the network and causing damage.

Anti-Malware Software:

This may more commonly be called Anti-Virus Software. However, Anti-Malware Software prevents more than just viruses. Anti-Malware Software is used to prevent and remove malware. It scans devices and alerts users to potential threats found on their device, so they can be removed.



Malware can be thought of as viruses, spyware, worms etc. So, having a strong Anti-Malware Software is very important in protecting a network from these threats!

Anti-Malware Software can be both free as well as have a cost. It depends what features you are looking for and the size of your business network as to what Anti-Malware Software you install.

Firewalls:

A firewall is used to control what goes in and what goes out of the network. It prevents unauthorised access by only allowing authorised access to the network.

We can think of a firewall as a bit like a bouncer on the doors to a building. If you're not on the list, you're not authorised to go in the building, so you get sent away and refused entry. However, if someone inside the building has requested you and you are on the list, you're authorised, so you're allowed entry.



Sometimes threats can slip past firewalls through 'back doors' in a server, which then need to be protected as well.

User Access Levels:

User Access Levels are commonly used across organisations who have a network. They provide different levels of access to the network depending on who the user is. For example, a network manager would need to be able to access all the different elements of the network. An admin assistant however wouldn't need such high level of access, so won't be able to access as much.



Another example would be a school. A student doesn't need to access anything other than the basics on the network, so is given minimal access. A teacher then would need to access more areas of the network such as shared staff files, so would have more access than the student. Then the network manager would need to be able to access all areas of the network, so would have full access to the network. The network manager would also then be able to set permissions for other users and change whole network settings.

Passwords:

A password allows users to access the network using a combination of letters, numbers, and characters only they know. They are used with a username and should be kept private. Only you should know your password.

A strong password is something that:

- Contains at least 8 or more letters/numbers/characters
- Has a mixture of uppercase and lowercase letters
- Uses letters, numbers, and characters
- Is not something easy to guess or find out such as your date of birth, dogs name, or favourite football team
- Is changed regularly
- Is not shared across multiple different accounts you own. Each account should have a different password



Encryption:

Encryption involves scrambling data before being transmitted, into a secret code. In order to decrypt the code, you must have a 'master' key. Only the device sending and the device receiving the data has this key. This is because prior to the data being sent, a 'handshake protocol' is used to ensure the same correct and valid key is being used by both the sender and receiver.



Physical Security:

As well as protecting a network digitally, we must also protect it physically. This means preventing someone accessing or damaging the actual hardware used to operate the network.

There are multiple ways we could physically secure a network such as:

- Lock the door to the server room and only allow approved personnel in there
- Mount servers into cases that are lockable
- Monitor and track personnel who enter and leave the server room or access any of the network hardware

“Now we know different threats and prevention methods, it’s good to be able to match them up:

Malware — Protect against this using Anti-Malware Software, Firewalls, and training staff on the dangers of email attachments etc.

Phishing — Protect against this using strong network policies, and training staff on how to spot a phisher

Weak People — Protect against this by training staff on how to be safe when using the network, as well as using Network Forensics to identify staff who pose a danger to the network

Brute Force Attacks — Protect against this by ensuring passwords are strong and changed regularly, and a Firewall is installed

DDOS Attacks — Protect against this by ensuring a Firewall is installed

Data Interception and Theft — Protect against this by Encrypting any data that is sent around and out of the network, as well as ensuring all staff use strong passwords to prevent easy access to the network

SQL Injection — Protect against this by ensuring Access Levels are placed on databases only allowing authorised individuals in, and Penetration Testing takes place to identify weaknesses

As you can see, different threats can be protected against by using multiple prevention methods!”



Past Exam Questions

Answer the questions below, to help you revise what has been covered in 1.4 Network Security.

1. Ben has been alerted by his anti-malware software that he may have malware on his computer.

i. Describe what is meant by malware [2]

ii. Describe how anti-malware software will help prevent or remove malware [2]

iii. Identify three other security measures Ben could put in place to protect his home network: [3]

1. _____

2. _____

3. _____

2. A company has installed a firewall to help protect its network.

Describe the role of a firewall

[2]

3. Ben also has two stand-alone computers. He has found both of those have been infected with malware also.

Describe how Bens computers could have been infected with the malware also

[2]

4. Identify three ways people within a business could put the network at risk

[3]

1. _____

2. _____

3. _____

5. A company is worried about the potential threats to their network.

Explain two potential threats to the company's network [4]

6. Explain how SQL Injection could affect a large business holding data on thousands of customers [3]

7. Describe how penetration testing could protect a network [2]

8. A local doctors surgery wants to protect against its staff potentially causing accidental damage to their network.

With reference to the staff at the surgery, explain three different security measures that can be put in place to protect the network from the surgery staff causing damage [6]

1.5 Systems Software

In this section you will revise the following:

1.5.1 Operating Systems

- The purpose and functionality of Operating Systems:
 - User Interface
 - Memory Management/Multitasking
 - Peripheral Management and Drivers
 - User Management
 - File Management

1.5.2 Utility Software

- The purpose and functionality of Utility Software:
 - Encryption Software
 - Defragmentation
 - Data Compression



Technical Terms

Technical Term	Definition
Systems Software	This runs the computer's hardware and applications. It allows the user to interact with the hardware and application software. It consists of two parts, the Operating System, and Utility System Software.
OS (Operating System)	This is the core software required for the computer to work. It controls the computer, and manages the hardware, user interface, and other software running on the computer.
User Interface	This is when the OS provides a way for the user to interact with and control the computer. It can be graphical, or text based.
GUI (Graphical User Interface)	<p>This is a type of User Interface.</p> <p>With a GUI, the user has menus, icons, and lists to select from in order to navigate their way around the computers features and applications. Windows is an example of a GUI.</p>
Command Line	<p>This is a type of User Interface.</p> <p>With a Command Line, the user types in specific commands in order to control and use the computer. These commands will often look like code and have to be exactly correct in order for the computer to work.</p>
Voice Control	<p>This is a type of User Interface.</p> <p>With Voice Control, the user controls the computer using their voice. The user will provide commands for the computer by speaking to the computer and telling it what to do. The computer will then process the command and execute it. Siri is an example of Voice Control.</p>
Memory Management	This is when the OS manages the transfer of data between memory units (RAM, CPU, and storage (e.g. hard drive)).
Multitasking	This is when the OS allows for more than one program to be running at once.
Peripheral Management	This is when the OS manages the input and output devices connected to the computer e.g. keyboard, mouse etc.

Driver	This is a piece of software that is installed to allow a peripheral device to work correctly on a computer. It contains the instructions that allow the device to connect and then send data back and forth to the computer.
User Management	This provides the opportunity for different users to be able to log onto the same computer. The OS will retain individual settings for each account such as desktop backgrounds, permissions to access files and programs etc.
File Management	This provides the user with a logical structure for storage of data. It provides the user files to store data in, and the ability to create folder structures to organise files.
Utility System Software	Utilities help the user manage the computer. They help the user maintain, configure, and optimise the computer.
Encryption	<p>This is a security measure when sending data. Data is scrambled into a secret code, which can only be decrypted using a master 'key'. Only the sender and receiver have this key, which therefore prevents the data being hacked/intercepted, and understood.</p> <p>Prior to encrypted data being sent, both devices check with each other to ensure they have the correct master key.</p>
Fragmentation	This occurs when data from the same file is split up and spread across the hard drive. Data therefore takes longer to access due to not being saved together, causing the system to slow down.
Defragmentation	This is when the data stored on the hard drive is reorganised, so space is optimised and made best use of. Data that is linked to the same file will be reorganised, so it is located together, making access quicker and easier.
Compression	This is when the size of a file is reduced by changing some of the files attributes e.g. its file type, dimensions etc.
Lossy Compression	This is when the size of the file is reduced (compressed), however the quality of the file also changes (it is reduced).
Lossless Compression	This is when the size of the file is reduced (compressed), however the quality of the file does not change.

Systems Software: What is it?

As discussed in 1.1 Systems Architecture and 1.2 Memory, the internal and external hardware for a computer system is a necessity. Without the hardware, the computer simply cannot work!

However, the user cannot use the computer with just the hardware alone. Users cannot directly interact with the hardware. For example, a user cannot tell the computer to open up Google Chrome without something in the middle to pass the request on to the hardware.

This is where the role of **Systems Software** comes in. Systems Software runs the computer hardware and applications. It allows the user to interact with the hardware and applications and allows the user to actually use the computer.

There are two types of Systems Software. These are:

- Operating System
- Utility System Software (Utilities for short)

Operating System

An **OS (Operating System)** is the backbone and core software of any computer system. It controls the computer and manages the hardware, user interface, and other software running on the computer.

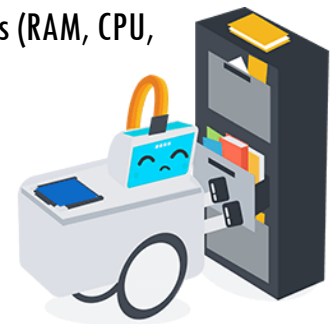
There are:

1. Memory Management
2. User Interface
3. Multitasking
4. Peripheral Management
5. User Management
6. File Management

Memory Management:

This is when the OS manages the transfer of data between memory units (RAM, CPU, and storage (e.g. hard drive)).

As programs are loaded up, they are taken from the hard drive and stored in the RAM (Random Access Memory), as we have already previously discussed. The Operating System will manage this process, as well as manage where in the RAM the programs are stored once loaded.

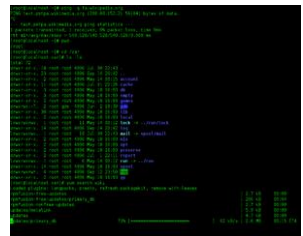
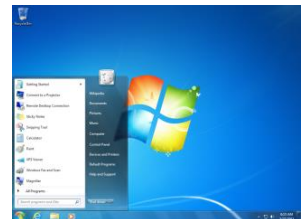


User Interface:

This is when the OS provides a way for the user to interact with and control the computer. It can be graphical, or text based. Without a User Interface, we wouldn't be able to control or use the computer!

There are three different types of User Interface. These are:

- **GUI (Graphical User Interface)** — This is when the user has menus, icons, and lists to select from in order to navigate their way around the computers features and applications. Windows is an example of a GUI.
- **Command Line** — This is when the user types in specific commands in order to control and use the computer. These commands will often look like code and have to be exactly correct in order for the computer to work.
- **Voice Control** — This is when the user controls the computer using their voice. The user will provide commands for the computer by speaking to the computer and telling it what to do. The computer will then process the command and execute it. Siri is an example of Voice Control.



Each User Interface has its advantages and disadvantages:

- **GUI (Graphical User Interface)** — Easy to use as the user can click on icons, menus, and buttons, and doesn't need to have any experience of the User Interface prior to using it; Takes up a large amount of storage space due to the large amount of icons, menus, and buttons that are all offered and used
- **Command Line** — Takes up the least amount of storage space due to how simple it is and the fact it uses no icons, menus, or buttons; By far the hardest User Interface to use, as specific commands have to be used. If a command is typed incorrectly, then it will not be executed. Needs training and practice in order to use
- **Voice Control** — Allows users to control the computer without the need of additional peripherals such as a mouse, keyboard etc. Also allows people with disabilities to control the computer; Takes up a large amount of storage due to the number of commands programmed into the Voice Control Interface to listen out for. Also, it is not always accurate when listening to the user and executing commands

Multitasking:

This is when the OS allows for more than one program to be running at once. This is done by allocating processing time to each open program.

Imagine only ever being able to open one program at once, work would take twice as long and would be twice as difficult! Thankfully, the OS allows us to have more than one program open at once by managing this process itself.

This means you can have your music program such as iTunes open, at the same time as having your web browser such as Google Chrome open, and your program used for work such as Microsoft Word.



Peripheral Management:

This is when the OS manages the input and output devices connected to the computer e.g. keyboard, mouse etc.

However, in order for the OS to be able to manage the peripherals, it must be able to understand the instructions being sent in by them.



A device driver is a piece of software that is installed to allow a peripheral device to work correctly on a computer. It contains the instructions that allow the device to connect and then send data back and forth to the computer. Each peripheral device needs a driver, without it the device cannot work. Many drivers these days are already built into the OS.

Furthermore, the OS also provides what are known as 'buffers'. These are small areas of temporary storage for holding data whilst it is processed by the device. For example, buffers are used in printing. Imagine you send 10 documents to print, they can't all be printed at the same time, so a queue is formed. The OS will create printing buffers enabling the print jobs to be stored and queued until the printer can complete the job.

User Management:

This is when the OS provides the opportunity for different users to be able to log onto the same computer. The OS will retain individual settings for each account such as desktop backgrounds, permissions to access files and programs etc.



User management also allows for new accounts to be created on the device, the setting of access rights and permissions, security settings etc.

If connected to a network, a fixed profile may be imposed on a user, and manage log in requests, rather than the User Management. For example, when you log into a computer in school, you are automatically given a set background and list of desktop icons. These cannot be changed and are therefore fixed.

Utility System Software

Utility System Software, or Utilities for short, help the user manage the computer. They help the user maintain, configure, and optimise the computer. This means the user gets the most out of the hardware and applications.

Although a computer system doesn't necessarily need Utilities in order to function, it needs Utilities in order to function efficiently. Without Utilities, the computer will begin to slow down, which will cause stress and problems for the user.

There are different types of Utilities. These are:

- **Encryption Software**
- **Defragmentation Software**
- **Data Compression Software**

As well as those listed above, Utilities can also support in the following areas:

- **Software Updates** — The Utility Software will check regularly for updates for applications on the computer, and alert the user when an update is available
- **System Clean-up** — The Utility Software will perform a clean-up of the system, deleting old and unused files from the storage that may cause it to slow down. Examples of these files may be old installation files. Once a piece of software has been installed, we often forget to delete the files that installed the software that we no longer need. Utility Software will identify these and remove them, optimising our storage
- **Data Backup** — When we backup data, we take a copy of the data and store it in another location (e.g. on an external hard drive) so we can restore the original data should it be lost or damaged. It is always important to backup data onto a separate storage media, so that if the computer system or media it is originally stored on is damaged, the data can still be retrieved.

Encryption Software:

We've now covered encryption across three different topics, so hopefully you now remember what encryption is! As a reminder, encryption is when data is scrambled into a secret code, which can only be decrypted using a master 'key'. Only the sender and receiver have this key, which therefore prevents the data being hacked/intercepted, and understood.

Prior to encrypted data being sent, both devices check with each other to ensure they have the correct master key.

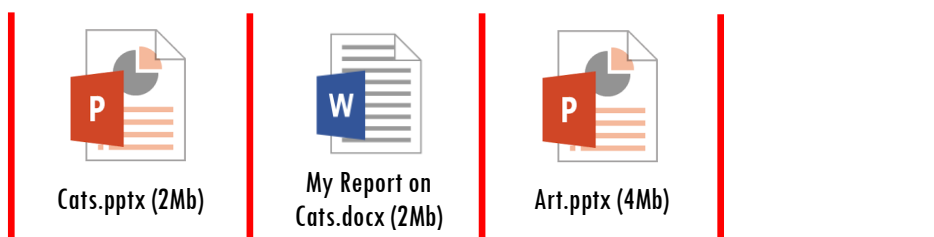
Encryption Software can be part of the Utility Software, as well as software that is run independently. This provides a level of security for the user.

Defragmentation Software:

In order to understand what **Defragmentation Software** does, we must first understand what fragmentation is.

Fragmentation occurs in computer systems regularly. It causes no harm to the computer system but will cause it to slow down and therefore not perform efficiently.

Imagine the below is a small portion of the hard drive in a computer system. As you can see, we have different files stored on the hard drive, all with their own place:

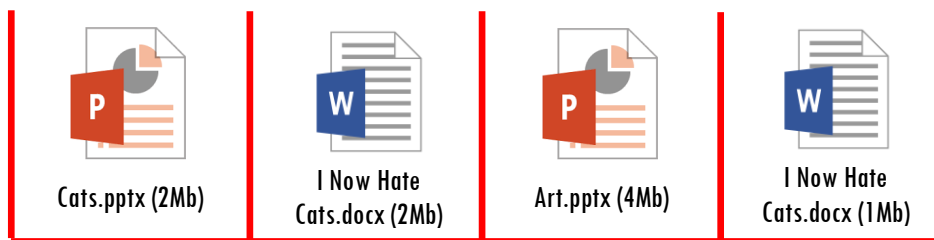


Each file has a different file size. We decide to delete some old files on our computer we no longer need. One of these is the file 'My Report on Cats.docx'. This now leaves a space on the hard drive. Remember, the 'My Report on Cats.docx' file was only 2Mb.



We then save a new file, now called 'I Now Hate Cats.docx' which has a file size of 3Mb. When we save the file, it will be stored on the hard drive in the first available places, even if that means it needs to be split up.

This now means, the first 2Mb of the file is stored in the gap left when we deleted the previous file, and the other 1Mb is stored in the next available place.



This is called **Fragmentation**. Fragmentation occurs when data from the same file is split up and spread across the hard drive. Data therefore takes longer to access due to not being saved together, causing the system to slow down. Luckily in our example above, the file was only split across two different locations, but it is easily possible for a file to be split across multiple locations. Obviously the more locations it is split across, the slower it is to access.

Defragmentation is when the data stored on the hard drive is reorganised, so space is optimised and made best use of. Data that is linked to the same file will be reorganised, so it is located together, making access quicker and easier. So, using the same example above for the 'I Now Hate Cats.docx' file which has been fragmented, defragmentation software would now reorganise the hard drive so both parts of the file are located together.



'It is important to defragment your computer regularly, otherwise you will find your computer slow down. It is also important to note defragmentation is a question they like to ask on the exam. However, it isn't always as straight forward as asking what it is. Look at the 'It's your turn!' question below''

Data Compression:

Compression is when the size of a file is reduced by changing some of the file's attributes e.g. its file type, dimensions etc. For example, we may compress a WAV sound file (which has a high audio quality but a large file size) down to an MP3 sound file (which has a lower sound quality but a much lower file size). This would then allow us to store more sound files on a device such as an iPod, due to the file sizes being smaller.



We may also need to compress a file to allow us to have additional room on a storage device, or to make a file small enough to send in an email.

There are two types of compression, these are:

- **Lossy Compression** – This is when the size of the file is reduced, however the quality of the file also reduces (meaning the quality gets worse)
- **Lossless Compression** – This is when the size of the file is reduced, however the quality of the file remains the same



“Although compression creates space on a hard drive, we wouldn’t want to compress absolutely everything in order to optimise space. You always have to find the balance between the quality of a file and the space it takes up”

Past Exam Questions

Answer the questions below, to help you revise what has been covered in 1.5 Systems Software.

1. Describe the role of systems software in a computer system [3]

2. Amy installs a new operating system on her computer.

i. Describe what the role of an operating system is [2]

ii. Amy is informed that one job role of the operating system is to multitask.

Describe what is meant by multitasking in relation to a computer system [2]

3. Multitasking is only one job role of the operating system.

Explain two **other** job roles of the operating system

[4]

4. Look at the table below. Tick **one** box in each row to show whether the job role is associated with the operating system or utility software

[5]

Job Role	Operating System	Utility Software
Defragmentation		
Peripheral Management		
Encryption Software		
File Management		
User Interface		

5. Describe what is meant by utility software

[2]

6. After three weeks of using her new computer system, Amy finds out her computers storage has become fragmented.

i. Describe what is meant by fragmentation [2]

ii. Identify the utility software that could overcome this problem [1]

iii. Describe how this utility software works [2]

7. Amy wants to send a picture of her new computer system to a friend. When she goes to send the picture, she is told the picture is too large to email. She is told by a friend to compress the file.

i. Describe what is meant by compression [2]

ii. Identify the two types of compression [2]

1. _____
2. _____

1.6 Ethical, Legal, Cultural and Environmental Impacts of Digital Technology

In this section you will revise the following:

1.6.1 Ethical, Legal, Cultural and Environmental Impact

- Impacts of digital technology on wider society including:
 - Ethical Issues
 - Legal Issues
 - Cultural Issues
 - Environmental Issues
 - Privacy Issues
- Legislation relevant to Computer Science:
 - The Data Protection Act 2018
 - Computer Misuse Act 1990
 - Copyright Designs and Patents Act 1988
 - Software licences (i.e. open source and proprietary)



“When talking about Ethical, Legal, Cultural and Environmental Concerns, the examiners like to put this as one of the extended writing questions. Therefore, when you come to the past exam questions at the end, you will see a lot of these!”



Technical Terms

Technical Term	Definition
Ethical Issue	An ethical issue relates to whether something could be deemed as morally right or wrong. This means it isn't necessarily illegal to do but could be deemed as being wrong to do.
Legal Issue	A legal issue relates to whether something is right or wrong to do by law. If something is done against the law, it can lead to consequences such as fines and imprisonment.
Cultural Issue	A cultural issue relates to whether something could have a positive or negative impact on a person, or group of peoples, culture. Again, a cultural issue is not necessarily illegal, but could be seen as being wrong to do.
Environmental Issue	An environmental issue relates to whether something is right or wrong to do in relation to the environment. This means how much of a positive or negative impact something could have on wildlife, plants, the air etc.
Privacy Issue	A privacy issue relates to whether someone personal and private life could be put in question. This could involve personal data about them, images of them etc.
Stakeholder	A stakeholder is someone who has an interest or part in a business or initiative. For example, if a school was to give all students iPads, stakeholders would be the teachers, students, parents, as well as the manufacturers of the iPads and those companies who sell them. All these groups of people would have an interest in this situation.
Open Source Software	This is when software is released and the programming code (source code) is accessible to all users to edit. It is often free, and users can modify and distribute the software legally.
Proprietary Software	This is when software is released and the programming code (source code) is not accessible to all users to edit. It often has a cost and users cannot modify and distribute the software legally. This type of software is often owned and sold by a company.
Legislation	Legislation refers to the laws that everyone must follow. These laws are passed by the government of a country.
Data Protection Act 2018	This is a piece of legislation that refers to how data should be gathered, stored, and destroyed correctly. It refers to eight key principles, and all must be met.

GDPR (General Data Protection Regulation)	Implemented in 2018, GDPR covers data protection and privacy in European Law, ensuring personal data is gathered and managed lawfully and securely.
Computer Misuse Act 1990	This is a piece of legislation that refers to how computers may be used to potentially cause damage or incite crime. It makes it illegal to make unauthorised access to data. There are three levels to the Computer Misuse Act, all of which have different consequences.
Copyright Designs and Patents Act 1988	This is a piece of legislation that is designed to protect an individual or companies' idea or creation. Individuals or companies apply to patent their idea or product, and once granted it prevents other people taking their idea or product and passing it off as their own.
Creative Commons Licensing	This is a standardised way to grant copyright permission to create work. It allows the author to retain copyright, whilst allowing others to copy, distribute, and make uses of their work.
Freedom of Information Act 2000	This is a piece of legislation that provides the public access to information held by public authorities such as schools, hospitals, and police stations. Public authorities have to then publish this data.

Legislation relevant to Computer Science

Legislation refers to the laws that everyone must follow. These laws are passed by the government of a country.

Due to the quick advancement of technology, legislation is now active that is specifically designed to monitor and prosecute against criminal activity when using Computer Science related concepts or devices.

There are three pieces of legislation you need to be familiar with for the exam. These are:

- **The Data Protection Act 2018**
- **Computer Misuse Act 1990**
- **Copyright Designs and Patents Act 1988**

Data Protection Act 2018:

The **Data Protection Act 2018** is a piece of legislation that refers to how data should be gathered, stored, and destroyed correctly. It refers to eight key principles, and all must be met. These eight key principles are:

- Data should be processed fairly and lawfully; not obtained by deception
- Data should only be used for the purpose specified
- Data should be relevant and not excessive
- Data should be accurate and up to date
- Data should only be kept for as long as is necessary
- Individuals have the right to see the data held about them, and to correct it
- Data must be kept secure
- Data cannot be transferred outside the EU unless the country has adequate data protection laws

All companies who hold data about anyone must follow all eight principles listed above, or can face prosecution (fines etc.)

The law was updated in 2018 to include GDPR (General Data Protection Regulation). In short, GDPR covers how data is gathered and managed on any citizen in the EU, regardless of where that data is stored. It effectively tightens up the security of data protection!

Computer Misuse Act 1990:

The **Computer Misuse Act 1990** is a piece of legislation that refers to how computers may be used to potentially cause damage or incite crime. It makes it illegal to make unauthorised access to data. There are three levels to the Computer Misuse Act:

Level 1 – Unauthorised access to computer material

Level 2 – Unauthorised access with intent to commit or facilitate commission of further offences

Level 3 – Unauthorised modification or computer material

This act makes hacking and the creation and spreading of viruses illegal. The consequences of breaking the Computer Misuse Act 1990 can range from a £1000 fine up to an unlimited fine and time in prison.

Copyright Designs and Patents Act 1988:

The **Copyright Designs and Patents Act 1988** is a piece of legislation that is designed to protect an individual or companies' idea or creation. Individuals or companies apply to patent their idea or product, and once granted it prevents other people taking their idea or product and passing it off as their own. For example, music artists will patent their songs before releasing them. This therefore means that you cannot download the song without their permission, and their permission to download it would mean you paying for it. This therefore means downloading the song without paying for it would be breaking the law.

Creative Commons Licensing falls into the bracket of the Copyright Designs and Patents Act 1988. This is a standardised way to grant copyright permission to create work. It allows the author to retain copyright, whilst allowing others to copy, distribute, and make uses of their work.



“There are some other ways work that has been copyrighted can be used without breaking the law, such as only using a small portion and changing it, using it for educational purposes, paying for it, giving credit to the original owner etc.”

It's your turn!

A farmer has a small farm selling fresh produce to local customers. He wants to create a website advertising his produce and allow customers to sign up for weekly delivery to their home.

Describe two legal issues that Fred must consider [4]

Hint: Think about the fact will be storing customer data, and how he must follow the Data Protection Acts eight principles

Environmental and Cultural Implications of Computer Science

Due to the rapid growth of Computer Science technologies across the world in the last 20 years, the impacts of this technology have also grown.

In this section, we will look at some Environmental Impacts and some Cultural Implications Computer Science is having.

Environmental Impacts:

An environmental issue relates to whether something is right or wrong to do in relation to the environment. This means how much of a positive or negative impact something could have on wildlife, plants, the air etc.

Computer Science has had both positive and negative impacts on the environment, despite us maybe only thinking immediately about the negative!

Some of the negative of impacts Computer Science has on the environment are:

- **Use of natural resources to create digital devices such as silicone are in limited supply. As demand for digital devices grows, so does the use of resources such as silicone. Once the resource is gone, it's gone!**
- **Production of digital devices as well as powering them uses large amounts of energy, which is often created through the burning of fossil fuels. This is harmful to the environment contributing to global warming and air pollution**
- **We often throw our old devices away. However, these devices contain harmful chemicals such as the mercury used in the batteries. When thrown away these devices break down and these chemicals are released into the environment. This could be the food or water supply for animals, which then contaminates the meat or kills the animals**

However, there are positive impacts:

- The development of Computer Science has led to a reduction in paper usage, meaning less trees are now being cut down
- The development of Computer Science technologies allows us to monitor the environment with greater accuracy, meaning we can now better predict environmental changes such as the weather, or the potential eruption of volcanoes



“As you can see above, there are some positive impacts Computer Science has had on the environment. However, it is likely the negatives outweigh the positives”

Cultural Implications:

A cultural issue relates to whether something could have a positive or negative impact on a person, or group of peoples, culture. Culture can be seen as the way in which we live our lives. Again, a cultural issue is not necessarily illegal, but could be seen as being wrong to do.

There are both positive and negative implications Computer Science has on culture.

Some of the negative of impacts Computer Science has on culture are:

- The development of Computer Science has widened the 'digital divide'. The digital divide refers to the gap between people who have access to technology and the internet, and those who do not. As technology has developed it has become more frequently available and affordable in some parts of the world, and less so in other parts. For example, in the UK we now have fibre optic broadband, allowing us to access internet speeds of above 100Mbps. However, poorer countries in the world such as Uganda won't even have access to the internet yet. This means people in poorer countries are being unfairly left behind
- The development of Computer Science has put extra strain on our lives. Cyberbullying has increased as technology has become easier to access, causing stress to people which can result in self harm or suicide. Also, being able to access work from home means more people are taking work home with them to continue with in the evening and at weekends, putting additional stress on them that they would not have had prior to technology becoming so developed
- Some countries are so concerned about their image and the potential for unrest that they limit the internet access to the public. This may be done to prevent criticism of a ruler or government, to prevent people breaking the law, or to prevent 'hate speech'. Countries such as North Korea are known to have heavily restricted internet access.

Some of the positive implications of Computer Science on culture are:

- The development of Computer Science has led to people being able to communicate, connect, and share with people all across the world. This means people can stay in touch with family who live long distances away, and share experiences with them
- Developments in areas such as gaming has allowed whole new opportunities for people to open up. With gaming, there is now the development of e-sports, meaning people can test themselves and excel in something completely different to the normal fields of sport or academia
- As Computer Science develops, people in the poorest and most remote parts of the world are being able to access some type of digital device. This means hospitals, schools etc. are able to access information that is shared across the world, widening their knowledge, and helping them learn more

Investigating and Discussing Computer Science Technologies

In the exam you are often given an extended writing question, where not only the quality of your answer but its structure and articulation is assessed. These questions will give you a scenario and ask you to discuss the impacts or implications it may have on four key areas. These four key areas could be:

- Stakeholders
- Ethical Issues
- Legal Issues
- Technology
- Privacy
- Cultural Issues/Implications

In this section we are going to look at some different examples of questions and break down possible groups of people for each section. However, before we do that, let's just make sure we know what is meant by the four areas above:

- **Stakeholders** — A stakeholder is someone who has an interest or part in a business or initiative
- **Ethical Issues** — This is an issue that may arise that could affect the way someone feels or thinks. As mentioned before, it is not illegal, but some people may think it is wrong to do
- **Legal Issues** — This is an issue that may arise involving the law. Always be thinking here about those different pieces of legislation we covered (Data Protection Act, Computer Misuse Act, Copyright Designs and Patents Act)
- **Technology** — This is a potential consequence (either positive or negative) for technology that may come about
- **Privacy** — This is an issue that may impact upon a person's right to keep something to themselves or not be disturbed by others
- **Cultural Issues/Implications** — This is an issue or implication upon the way someone lives their life, or their access to technology

Scenario 1:

A school is looking to upgrade its technology in school and is thinking about giving all new Year 7 students an iPad.

Discuss the impacts this would have.

You may want to consider the following areas in your answer:

[8]

- Stakeholders
- Ethical Issues
- Technology
- Legal Issues

The above question is an example of the type of question you could be asked in the exam. We would need to write four paragraphs in total, one paragraph for each of those areas. Even though it says, 'you may want to ...', you need to! In order to access all the marks, you have to cover each area.

Let's think about some different groups of people for each area.

Stakeholders:

Remember, a stakeholder is someone who has an interest or part in a business or initiative.

So, for this question, a stakeholder could be a teacher. It is likely the teacher will be involved in the Year 7's having iPads and using them in lessons, therefore they will have an interest in this.

We could also have parents. Parents will have an interest in whether their child is given an iPad or not, maybe to ensure internet access at home can be limited to ensure they only access websites they should do on the iPad, or to ensure they don't spend long amounts of time on it.

The companies who manufacture or sell the iPads will also have an interest in this decision, as they will be given an opportunity to sell a large amount iPads and potentially other supporting accessories such as cases in one go.

Ethical Issues:

Remember, an ethical issue is an issue that may arise that could affect the way someone feels or thinks. As mentioned before, it is not illegal, but some people may think it is wrong to do.

So, for this question, one ethical issue may be that giving students an iPad could lead to an increase in cyberbullying if the iPads are not used appropriately. This could lead to students feeling upset or depressed, and lead to more students feeling isolated.

Another ethical issue could be that the school are providing an access to a device some students would not be able to afford normally. The school is therefore closing their own digital divide in school and helping make all students feel and look equal. This is obviously a positive, you can cover positives too!

A third ethical issue could be that the students could develop health problems through using the devices too much, such as eyesight issues or headaches. This could cause lifelong issues.

Technology:

Remember, this is a potential consequence (either positive or negative) for technology that may come about. This one can be a bit trickier to cover sometimes and will require you to think a bit harder for examples.

One impact on technology this could have is that more devices could be paired with the iPad, creating a link between different devices. Devices could share information between each other. For example, students could complete work on a computer, share it with the iPad, and continue it outside of the lesson.

Another impact on technology could be that the increase of traffic on the network due to all the iPads connecting to it could cause the network to slow down. This could affect the performance of the network and therefore result in the network needing to be upgraded, which would be expensive to do.

Legal Issues:

Remember, a legal issue is an issue that may arise involving the law. Always be thinking here about those different pieces of legislation we covered (Data Protection Act, Computer Misuse Act, Copyright Designs and Patents Act).

So, in this question an example of a legal issue could be the threat of students misusing the iPads in order to potentially damage the school network or other networks or devices. This would therefore be breaking the Computer Misuse Act. Some students may use the iPads to create and spread viruses, which would therefore be breaking the law.

Another example of a legal issue could be that the students could use the iPads to download illegal content such as illegal music or movies. This would therefore be breaking the Copyright Designs and Patents Act.

As you can see above in the two examples, we have also named the legislation that would be broken. This is important to do! When you think of an issue, make sure you think about which piece of legislation would be broken by it, and name it in your answer.

Now you have thought about different examples for each of the four key areas, pick one from each that you feel most comfortable in being able to explain properly, and put your answer into four paragraphs:

One stakeholder in this situation would be ... They would have an interest in this because ...

One ethical issue in this situation would be ... This would be an issue because ...

One impact on technology would be ... This would impact upon technology because ...

One legal issue in this situation would be ... This would be an issue because ...

Scenario 2:

An outreach program has been set up to provide a small aboriginal tribe access to a digital device and the internet for the first ever time.

Discuss the impacts this would have.

You may want to consider the following areas in your answer:

[8]

- Stakeholders
- Ethical Issues
- Technology
- Legal Issues

Here is another example of a question you could get in the exam. Just like in scenario one, let's get some examples of groups of people for each area.

Stakeholders:

One stakeholder could be the people who are part of the tribe. They will be the ones given access to a digital device and the internet, and therefore will have a major interest in the situation above, especially considering they have never accessed this technology before.

Another stakeholder could be the company who are going to actually provide the technology. They will have an interest as they will need to be able to work out how to provide the opportunity for these people to access and use the device, as well as access the internet in what could be a very remote area.

Another stakeholder would be the outreach team who are offering this opportunity. They will have an interest as they will need to know how to monitor how the tribe use the devices and also what information they are trying to gather from this program. They will also need to monitor the success of the program and think about how they could potentially roll it out to more people should it be successful.

Ethical Issues:

One ethical issue could be that these people have never accessed the internet before, and there is a risk they could expose themselves to dangerous material. It will need to be considered what affect this could have on the people e.g. they could become emotionally distressed if they see harmful images or videos.

Another ethical issue could be that this program could disrupt the lives of the aboriginal tribe. These people may have lived a certain way for a very long time, and the sudden change in their lifestyles via access to the internet could harm their natural way of life.

Technology:

One impact this program could have on technology is the advancement in how groups of people who live in remote areas gain access to technology. This program could provide the infrastructure for other local people or tribes to access technology, such as a basic access to the internet.

Another impact on technology could be that new ideas for future developments of technology or how to train new people to use technology could be identified as part of the program. As the tribe has never accessed a digital device or the internet before, it is a great opportunity to find out what features they would find most useful, or what they think is the best way to learn about how to use the technology.

Legal Issues:

One legal issue that could arise in this situation is that data will need to be collected about the tribe. Therefore, the Data Protection Act will need to be considered. The staff working on the outreach program will need to ensure that all the Data Protection Acts key principles are met. For example, the staff will need to ensure they have the permission of the tribe to hold data about them, and they only collect data that is necessary.

Another legal issue could be that the tribe try to access and spread harmful content over the internet, breaking the Computer Misuse Act. They would likely do this without knowing, however the consequences would still be the same. The outreach team will therefore need to think about how to avoid the tribe misusing the technology.



“Each of these 8-mark questions are worth 10% of the exam paper. Therefore, you want to make sure you get as many marks as possible! Make sure you think about each of the four areas carefully, and make sure you give an answer for each one! You can only get two marks for each section, so if you write two paragraphs on stakeholders for example you won’t get any extra marks”

Open Source vs Proprietary Software

When accessing software, it is categorised into being either **Open Source** or **Proprietary** (also known as ‘off the shelf’).

Open Source Software is when software is released and the programming code (source code) is accessible to all users to edit. It is often free, and users can modify and distribute the software legally.

Proprietary Software is when software is released and the programming code (source code) is not accessible to all users to edit. It often has a cost and users cannot modify and distribute the software legally. This type of software is often owned and sold by a company.

Look at the table below, which outlines some advantages and disadvantages to each:

Open Source	Proprietary
Is often free to download, meaning there is no cost to the user or risk if the software does not do quite what the user wants	Is paid for and can be expensive depending on what the software is or does.
There is often no direct person or group of people who are responsible for updates or bug fixes, meaning bugs may not get fixed for a long time, or even ever	Managed by a group of software engineers who are all trained and knowledgeable. Updates will be rolled out regularly meaning bugs get fixed
There is no direct person or group of people who can deal with any questions or problems you are having. You must work out or solve the problem yourself	There is usually a dedicated customer service team who can answer any questions you have or support you with problems

Past Exam Questions

Answer the questions below, to help you revise what has been covered in 1.6 Ethical, Legal, Cultural and Environmental impacts of Digital Technology.

1. Troy wants a new word processing software. He does not know whether to use open source software or proprietary software.

i. Describe what is meant by open source software [2]

ii. Describe what is meant by proprietary software [2]

ii. Identify and explain two differences between open source and proprietary software [4]

4. A research team wants to analyse how technology usage changes as people grow up. They want to start with 5-year olds and monitor how they use technology until they turn 16.

Discuss the impacts this would have.

You may want to consider the following areas in your answer:

[8]

- Privacy Issues
- Ethical Issues
- Technology
- Legal Issues

Additional Resources

Exam Command Words:

The command words below will be used consistently in all assessment material and resources.

Add: Join something to something else so as to increase the size, number, or amount.

Analyse: Break down in order to bring out the essential elements or structure. To identify parts and relationships, and to interpret information to reach conclusions.

Annotate: Add brief notes to a diagram or graph.

Calculate: Obtain a numerical answer showing the relevant stages in the working.

Compare: Give an account of the similarities and differences between two (or more) items or situations, referring to both (all) of them throughout.

Complete: Provide all the necessary or appropriate parts.

Convert: Change the form, character, or function of something.

Define: Give the precise meaning of a word, phrase, concept or physical quantity.

Describe: Give a detailed account or picture of a situation, event, pattern or process

Design: Produce a plan, simulation or model.

Discuss: Offer a considered and balanced review that includes a range of arguments, factors or hypotheses. Opinions or conclusions should be presented clearly and supported by appropriate evidence.

Draw: Produce (a picture or diagram) by making lines and marks on paper with a pencil, pen, etc.

Evaluate: Assess the implications and limitations; to make judgements about the ideas, works, solutions or methods in relation to selected criteria.

Explain: Give a detailed account including reasons or causes.

Give: Present information which determines the importance of an event or issue. Quite often used to show causation.

How: In what way or manner; by what means.

Identify: Provide an answer from a number of possibilities. Recognise and state briefly a distinguishing factor or feature.

Justify: Give valid reasons or evidence to support an answer or conclusion.

Label: Add title, labels or brief explanation(s) to a diagram or graph.

List: Give a sequence of brief answers with no explanation.

Order: Put the responses into a logical sequence.

Outline: Give a brief account or summary.

Refine: Make more efficient, improve, modify or edit.

Show: Give steps in a derivation or calculation.

Solve: Obtain the answer(s) using algebraic and/or numerical and/or graphical methods.

State: Give a specific name, value or other brief answer without explanation or calculation.

Tick: Mark (an item) with a tick or select (a box) on a form, questionnaire etc. to indicate that something has been chosen.

What: Asking for information specifying something.

Write/Rewrite: Mark (letters, words, or other symbols) on a surface, typically paper, with a pen, pencil, or similar implement/Write (something) again so as to alter or improve it.

Extended Writing Support

Use the below support to help you answer the extended writing questions.

Remember, you must give four paragraphs and cover each of the four areas given to you.

Also remember: **Make your point**, **Explain your point**, **Link back to the question**

What is your point?

Explain your point:

Link back to the question:

Extended Writing Mark Scheme

The below structure shows you how the examiners will mark your answers to the extended writing questions. This is the same across all extended writing questions, however your answers must be relevant to the question asked.

Mark Band 3—High Level (6-8 marks):

The candidate demonstrates a thorough knowledge and understanding of a wide range of considerations in relation to the question; the material is generally accurate and detailed.

The candidate is able to apply their knowledge and understanding directly and consistently to the context provided. Evidence/examples will be explicitly relevant to the explanation. The candidate is able to weigh up both sides of the discussion and includes reference to the impact on all areas showing thorough recognition of influencing factors.

There is a well-developed line of reasoning which is clear and logically structured. The information presented is relevant and substantiated.

Mark Band 2-Mid Level (3-5 marks):

The candidate demonstrates reasonable knowledge and understanding of a range of considerations in relation to the question; the material is generally accurate but at times underdeveloped.

The candidate is able to apply their knowledge and understanding directly to the context provided although one or two opportunities are missed. Evidence/examples are for the most part implicitly relevant to the explanation.

The candidate makes a reasonable attempt to discuss the impact on most areas, showing reasonable recognition of influencing factors. There is a line of reasoning presented with some structure. The information presented is in the most part relevant and supported by some evidence.

Mark Band 1-Low Level (1-2 marks):

The candidate demonstrates a basic knowledge of considerations with limited understanding shown; the material is basic and contains some inaccuracies.

The candidate makes a limited attempt to apply acquired knowledge and understanding to the context provided.

The candidate provides nothing more than an unsupported assertion. The information is basic and communicated in an unstructured way. The information is supported by limited evidence and the relationship to the evidence may not be clear.

0 marks:

No attempt to answer the question or response is not worthy of credit